MedMij Afsprakenstelsel, normenkader

Release 1.5.1

Auteur Project Afsprakenstelsel
Datum 25 februari 2022

Inhoudsopgave

_snippets

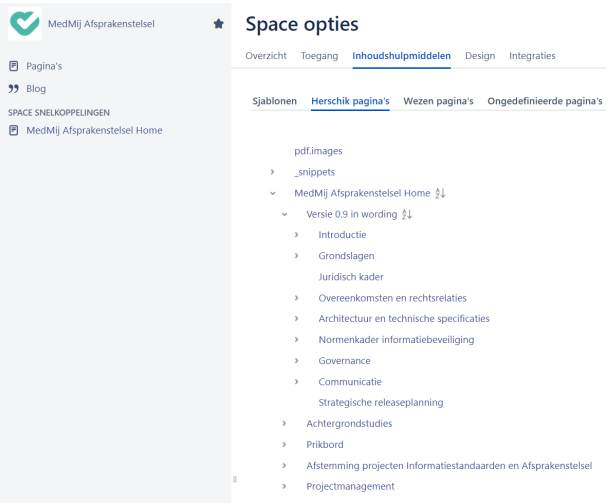
Snippets zijn kleine herbruikbare stukjes tekst die je eenvoudig op een pagina kunt inbedden middels de **Include Page**-macro.

Momenteel zijn er de volgende "snippets".

- snippet.beoordeling.auditor
- snippet.implementatie.niet.voorgeschreven
- snippet.weging.laag
- snippet.weging.midden
- snippet.weging.hoog
- snippet.rollen
- snippet.evidence

> Let op bij het publiceren van het afsprakenstelsel!

Om te voorkomen dat gebruikers de snippets zien, staan ze op een plek staan "buiten het zicht":



Als je het afsprakenstelsel publiceert door de boom te kopiëren naar een andere space, gaan de snippets dus niet mee. De pagina's blijven dan verwijzen naar de snippets in de oorspronkelijke locatie.

Om toch te zorgen dat de snippets mee-gekopieerd worden, en de hyperlinks correct blijven werken, volg onderstaande stappen:

1. Ga naar de menu-optie "herschik pagina's" (https://afsprakenstelsel.medmij.nl/pages/reorderpages.action?key=MA08)
2. Sleep de pagina "_snippets" naar een plek **in** het afsprakenstelsel, bijvoorbeeld onder "Introductie"
3. Kopieer het afsprakenstelsel zoals je gewend was
4. Vanuit de nieuwe locatie, ga je opnieuw naar de menu-optie "herschik pagina's"
5. Sleep de pagina "_ snippets" nu weer **uit** het afsprakenstelsel, bijvoorbeeld boven de "Home"-pagina.
6. Geniet van een afsprakenstelsel met werkende snippets

snippet.beoordeling.auditor

Het afsprakenstelsel schrijft dit niet voor. De auditor kan dit naar eigen inzicht uitvoeren.

snippet.implementatie.niet.voorgeschreven

Deze beheersmaatregel moet zijn opgenomen op de Verklaring van Toepasselijkheid, maar het afsprakenstelsel schrijft (nog) geen nadere invulling voor. Partijen mogen deze naar eigen inzicht invullen.

snippet.weging.laag

LAAG RISICO

MedMij geeft geen specifieke weging aan de implementatie van deze maatregel, hij mag evenwel niet uitgesloten zijn. De auditor of CI bepaalt hoe zwaar deze maatregel weegt in zijn certificatiebeslissing.

snippet.weging.midden

MIDDEN RISICO

MedMij hecht waarde aan de correcte implementatie van deze maatregel. De maatregel moet zijn geïmplementeerd, maar er mag een *kleine non-conformiteit* aanwezig zijn. De auditor moet het verbeterplan hebben goedgekeurd.

snippet.weging.hoog

HOOG

MedMij hecht veel waarde aan de correcte implementatie van deze maatregel. De maatregel moet zijn geïmplementeerd en mogen geen *non-conformiteiten* aanwezig zijn.

snippet.rollen

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

snippet.evidence

Bij de eerste certificering volgens dit normenkader is het aantonen van de opzet voldoende.

MedMij Afsprakenstelsel 1.5.1

Het MedMij Afsprakenstelsel draagt eraan bij dat persoonsgebonden, gevoelige en vertrouwelijke gezondheidsgegevens op een veilige en gebruiksvriendelijke wijze uitgewisseld kunnen worden tussen persoonlijke gezondheidsomgevingen en aanbieders. De uitwisseling geschiedt in twee richtingen; personen kunnen gegevens verzamelen en delen.

MedMij streeft naar het realiseren van interoperabiliteit voor deze uitwisseling. Hiertoe is een afsprakenstelsel ontwikkeld, bestaande uit afspraken op juridisch, organisatorisch, financieel, communicatief, semantisch en technisch gebied, zodat personen en aanbieders op een veilige manier gegevens kunnen uitwisselen. Partijen die deelnemen aan het MedMij Afsprakenstelsel committeren zich aan de afspraken, en kunnen diensten aanbieden op basis van de reeds overeengekomen afspraken.

Het afsprakenstelsel gaat uit van *centraal vertrouwen en decentrale operatie*. Het afsprakenstelsel is een bewust gecreëerde verzameling instituties die waarborgen biedt voor een faire omgang met de belangen van de verschillende stakeholders. Bij de uitwisseling van gegevens via het MedMij-netwerk wordt echter uitgegaan van decentrale technische voorzieningen.

Onderdelen van het afsprakenstelsel

Het MedMij Afsprakenstelsel bestaat uit een samenhangende set afspraken, voorzieningen en ingerichte ontwikkel- en beheerprocessen.

- Partijen die diensten willen bieden aan personen of aanbieders kunnen als deelnemer toetreden tot het afsprakenstelsel in de rol van Dienstverlener persoon of Dienstverlener aanbieder.
- Voordat partijen deelnemer worden in het afsprakenstelsel, doorlopen zij het Toetredingsproces. Op dit proces is het Toetredingsbeleid van toepassing. Bij de start van het proces overlegt de potentiële deelnemer een Zelfverklaring integriteit. Na een eerste controle op enkele formaliteiten maken de kandidaat-deelnemer en de MedMij-beheerorganisatie afspraken over het vervolg van het toetredingsproces door middel van een Intentieverklaring.
- Als het toetredingsproces met goed gevolg is doorlopen en toetreding van de deelnemer het stelselbelang niet schaadt, sluiten de deelnemer en de beheerorganisatie een Deelnemersovereenkomst met elkaar.
- In de Deelnemersovereenkomst is onder meer opgenomen dat partijen zich houden aan de Afsprakenset, een uitgebreide set met rollen en verantwoordelijkheden. Partijen erkennen via de overeenkomst ook de Grondslagen en de Juridische context. Zowel de afsprakenset, de grondslagen als de juridische context van de afsprakenset worden releasematig ontwikkeld, gepubliceerd en in productie genomen.
- De beheerorganisatie onderhoudt een Catalogus die relevant is voor de dienstverlening die via het MedMij-netwerk kan worden aangeboden. De Catalogus definieert welke Gegevensdiensten deelnemers kunnen ontsluiten.
- De governance van het afsprakenstelsel is formeel vastgelegd in de Statuten van de Stichting MedMij , maar ook in een toegankelijker vorm beschreven.
- De toelating van informatiestandaarden tot het MedMij Afsprakenstelsel is onderworpen aan eisen (aan informatiestandaarden) en een uitgewerkte governance (proces en rolverdeling).
- De voor deelnemers relevante beheerprocessen zijn in groter detail uitgewerkt door de beheerorganisatie. De detailuitwerking is geen onderdeel van de afsprakenset omdat die bovenal informatief is; deelnemers worden gebonden via de Operationele processen uit de afsprakenset.
- Aanbieders sluiten op grond van de AVG verplicht een verwerkersovereenkomst met hun dienstverlener(s) aanbieder. MedMij stelt een Modelverwerkersovereenkomst beschikbaar die partijen kunnen gebruiken om passende afspraken met elkaar te maken.

Bindingen

Onderstaande tabel geeft weer hoe partijen formeel gebonden zijn aan de verschillende componenten van het MedMij Afsprakenstelsel.

Gebonden betekent dat een partij een verplichting is aangegaan. *Erkend* betekent dat de partij heeft verklaard dat de component relevante context bij de uitleg van verplichtingen en het overig handelen in het kader van het afsprakenstelsel betreft.

Component	Dienstverlener persoon	Dienstverlener aanbieder	Beheerorganisati
Afsprakenset	Gebonden via deelnemersovereenkomst	Gebonden via deelnemersovereenkomst	Gebonden via deelnemersoveree
Grondslagen	Erkend via deelnemersovereenkomst	Erkend via deelnemersovereenkomst	Erkend via deelnemersoveree
Juridische context	Erkend via deelnemersovereenkomst	Erkend via deelnemersovereenkomst	Erkend via deelnemersoveree
Catalogus	Gebonden via afsprakenset	Gebonden via afsprakenset	Gebonden via afsprakenset
Deelnemersovereenkomst Dienstverlener persoon	Gebonden door overeenkomst	-	Gebonden door overeenkomst
Deelnemersovereenkomst Dienstverlener aanbieder	-	Gebonden door overeenkomst	Gebonden door overeenkomst
Toetredingsbeleid	Gebonden via intentieverklaring	Gebonden via intentieverklaring	Gebonden via intentieverklaring
Toetredingsproces	Gebonden via intentieverklaring	Gebonden via intentieverklaring	Gebonden via intentieverklaring
Zelfverklaring integriteit	Gebonden door ondertekening	Gebonden door ondertekening	-
Intentieverklaring Dienstverlener persoon	Gebonden via overeenkomst (niet in rechte afdwingbaar)	-	Gebonden via overeenkomst (niet in rechte afdwingbaar)
Intentieverklaring Dienstverlener zorgaanbieder	-	Gebonden via overeenkomst (niet in rechte afdwingbaar)	Gebonden via overeenkomst (niet in rechte afdwingbaar)
Governance	Gebonden door statuten	Gebonden door statuten	Gebonden door st
Statuten Stichting MedMij	-	-	Gebonden door burgerlijk recht
Uitwerking beheerprocessen	Gebonden via beleid (afsprakenset)	Gebonden via beleid (afsprakenset)	Gebonden via bele (afsprakenset)

Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener zorgaanbieder	-	Optioneel gebonden door overeenkomst met zorgaanbieder	-

Introductie

Het MedMij Afsprakenstelsel draagt eraan bij dat persoonsgebonden, gevoelige en vertrouwelijke gezondheidsgegevens op een veilige en gebruiksvriendelijke wijze uitgewisseld kunnen worden tussen persoonlijke gezondheidsomgevingen en aanbieders. De uitwisseling geschiedt in twee richtingen; personen kunnen gegevens verzamelen en delen.

MedMij streeft naar het realiseren van interoperabiliteit voor deze uitwisseling. Hiertoe is een afsprakenstelsel ontwikkeld, bestaande uit afspraken op juridisch, organisatorisch, financieel, communicatief, semantisch en technisch gebied, zodat personen en aanbieders op een veilige manier gegevens kunnen uitwisselen. Partijen die deelnemen aan het MedMij Afsprakenstelsel committeren zich aan de afspraken, en kunnen diensten aanbieden op basis van de reeds overeengekomen afspraken.

Het afsprakenstelsel gaat uit van *centraal vertrouwen en decentrale operatie*. Het afsprakenstelsel is een bewust gecreëerde verzameling instituties die waarborgen biedt voor een faire omgang met de belangen van de verschillende stakeholders. Bij de uitwisseling van gegevens via het MedMij-netwerk wordt echter uitgegaan van decentrale technische voorzieningen.

Onderdelen van het afsprakenstelsel

Het MedMij Afsprakenstelsel bestaat uit een samenhangende set afspraken, voorzieningen en ingerichte ontwikkel- en beheerprocessen.

- Partijen die diensten willen bieden aan personen of aanbieders kunnen als deelnemer toetreden tot het afsprakenstelsel in de rol van Dienstverlener persoon of Dienstverlener aanbieder.
- Voordat partijen deelnemer worden in het afsprakenstelsel, doorlopen zij het Toetredingsproces. Op dit proces is het Toetredingsbeleid van toepassing. Bij de start van het proces overlegt de potentiële deelnemer een Zelfverklaring integriteit. Na een eerste controle op enkele formaliteiten maken de kandidaat-deelnemer en de MedMij-beheerorganisatie afspraken over het vervolg van het toetredingsproces door middel van een Intentieverklaring.
- Als het toetredingsproces met goed gevolg is doorlopen en toetreding van de deelnemer het stelselbelang niet schaadt, sluiten de deelnemer en de beheerorganisatie een Deelnemersovereenkomst met elkaar.
- In de Deelnemersovereenkomst is onder meer opgenomen dat partijen zich houden aan de Afsprakenset, een uitgebreide set met rollen en verantwoordelijkheden. Partijen erkennen via de overeenkomst ook de Grondslagen en de Juridische context. Zowel de afsprakenset, de grondslagen als de juridische context van de afsprakenset worden releasematig ontwikkeld, gepubliceerd en in productie genomen.
- De beheerorganisatie onderhoudt een Catalogus die relevant is voor de dienstverlening die via het MedMij-netwerk kan worden aangeboden. De Catalogus definieert welke Gegevensdiensten deelnemers kunnen ontsluiten.
- De governance van het afsprakenstelsel is formeel vastgelegd in de Statuten van de Stichting MedMij , maar ook in een toegankelijker vorm beschreven.
- De toelating van informatiestandaarden tot het MedMij Afsprakenstelsel is onderworpen aan eisen (aan informatiestandaarden) en een uitgewerkte governance (proces en rolverdeling).
- De voor deelnemers relevante beheerprocessen zijn in groter detail uitgewerkt door de beheerorganisatie. De detailuitwerking is geen onderdeel van de afsprakenset omdat die bovenal informatief is; deelnemers worden gebonden via de Operationele processen uit de afsprakenset.
- Aanbieders sluiten op grond van de AVG verplicht een verwerkersovereenkomst met hun dienstverlener(s) aanbieder. MedMij stelt een Modelverwerkersovereenkomst beschikbaar die partijen kunnen gebruiken om passende afspraken met elkaar te maken.

Bindingen

Onderstaande tabel geeft weer hoe partijen formeel gebonden zijn aan de verschillende componenten van het MedMij Afsprakenstelsel.

Gebonden betekent dat een partij een verplichting is aangegaan. *Erkend* betekent dat de partij heeft verklaard dat de component relevante context bij de uitleg van verplichtingen en het overig handelen in het kader van het afsprakenstelsel betreft.

Component	Dienstverlener persoon	Dienstverlener aanbieder	Beheerorganisati
Afsprakenset	Gebonden via deelnemersovereenkomst	Gebonden via deelnemersovereenkomst	Gebonden via deelnemersoveree
Grondslagen	Erkend via deelnemersovereenkomst	Erkend via deelnemersovereenkomst	Erkend via deelnemersoveree
Juridische context	Erkend via deelnemersovereenkomst	Erkend via deelnemersovereenkomst	Erkend via deelnemersoveree
Catalogus	Gebonden via afsprakenset	Gebonden via afsprakenset	Gebonden via afsprakenset
Deelnemersovereenkomst Dienstverlener persoon	Gebonden door overeenkomst	-	Gebonden door overeenkomst
Deelnemersovereenkomst Dienstverlener aanbieder	-	Gebonden door overeenkomst	Gebonden door overeenkomst
Toetredingsbeleid	Gebonden via intentieverklaring	Gebonden via intentieverklaring	Gebonden via intentieverklaring
Toetredingsproces	Gebonden via intentieverklaring	Gebonden via intentieverklaring	Gebonden via intentieverklaring
Zelfverklaring integriteit	Gebonden door ondertekening	Gebonden door ondertekening	-
Intentieverklaring Dienstverlener persoon	Gebonden via overeenkomst (niet in rechte afdwingbaar)	-	Gebonden via overeenkomst (niet in rechte afdwingbaar)
Intentieverklaring Dienstverlener zorgaanbieder	-	Gebonden via overeenkomst (niet in rechte afdwingbaar)	Gebonden via overeenkomst (niet in rechte afdwingbaar)
Governance	Gebonden door statuten	Gebonden door statuten	Gebonden door st
Statuten Stichting MedMij	-	-	Gebonden door burgerlijk recht
Uitwerking beheerprocessen	Gebonden via beleid (afsprakenset)	Gebonden via beleid (afsprakenset)	Gebonden via bel (afsprakenset)

Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener zorgaanbieder	-	Optioneel gebonden door overeenkomst met zorgaanbieder	-

Afsprakenstelsel in de praktijk

Het verhaal van Roos Dalstra

Hallo, ik ben Roos Dalstra, een vrouw van 54 jaar. Leuk dat jullie dit verhaal willen lezen over mijn ervaringen met MedMij, een afsprakenstelsel waar de leverancier van mijn persoonlijke gezondheidsomgeving aan deelneemt, zodat ik met die toepassing op een veilige manier mijn gezondheidsgegevens kan verzamelen bij en delen met zorgaanbieders. Zorgaanbieder is geen woord dat ik zelf gebruik. Ik heb het liever over Marlou en Evelien, mijn huisarts en haar praktijkondersteuner, en Ed, mijn apotheker.

Voor mijn behandeling helpt het enorm om informatie van bijvoorbeeld Ed te krijgen over de medicatie die hij aan me heeft verstrekt. Eerder voelde ik mij onzeker en had ik geen overzicht van de medicijnen die ik moest slikken. Gevoelsmatig had ik er geen grip op. Daarom wil ik mijn ervaringen graag met jullie delen, zodat ook jullie kennis kunnen maken met MedMij.

Een persoonlijke gezondheidsomgeving

Al een aantal jaren heb ik diabetes en sinds kort maak ik gebruik van een persoonlijke gezondheidsomgeving. In mijn geval is dat een combinatie van een persoonlijk gezondheidsplatform en andere apps en apparaten die ik gebruik die op dit platform kunnen aansluiten. Zo heb ik mijn smartwatch, mijn weegschaal en mijn bloedglucosemeter aangesloten en maak ik gebruik van een diabetes-app waarin ik verschillende overzichten kan bekijken. Het persoonlijke gezondheidsplatform zorgt ervoor dat het allemaal mooi samen komt en ik heb een eigen dashboard om het allemaal te beheren. Hierin heb ik bijvoorbeeld geregeld dat mijn diabetesapp gebruik kan maken van de gegevens die ik van de zorgaanbieder heb ontvangen in het platform.

Informatie uitwisselen met mijn huisarts

Ik was laatst in de huisartspraktijk voor controle door Evelien en zat in de wachtkamer te wachten totdat ik aan de beurt was. Mijn oog viel op een poster aan de wand met daarop de boodschap “Wij doen mee MedMij!’ met daaronder de unieke naam van de praktijk die binnen de MedMij-gegevensuitwisseling wordt gehanteerd en die je kan gebruiken om de praktijk te vinden in de persoonlijke gezondheidsomgeving. Van MedMij had ik al gehoord. Mijn zoon Bart heeft me laatst namelijk geholpen om een persoonlijke gezondheidsomgeving te kiezen. “Dat is helemaal van deze tijd!”, had hij gezegd. Daar stond toen ook MedMij bij.

“Mevrouw Dalstra”. Het was Evelien die me kwam ophalen voor de controle. Ik zat nog helemaal met mijn gedachten bij de avond dat ik met Bart een persoonlijke gezondheidsomgeving heb uitgekozen. Ik weet nog dat hij me een app liet zien waarvan ik dacht: “Wat moet ik daar nou mee? Veel te ingewikkeld allemaal.” Hij had toen gezegd: “Mam, geen probleem. Laten we gewoon online kijken welke gezondheidsomgeving bij jou past. Elke aanbieder die zich aan de MedMij-spelregels houdt, kan op een veilige manier gegevens uitwisselen met zorgaanbieders die ook via MedMij kunnen uitwisselen. Er is al aardig wat aanbod.”

We zochten online en vonden een persoonlijke gezondheidsomgeving speciaal voor mensen met diabetes, die ook echt ondersteuning biedt bij de behandeling. “Wat handig!” dacht ik. Hij is trouwens ook eenvoudig in het gebruik, wel zo fijn. Ik ben af en toe echt een kluns met apps. De week daarna heb ik zelf een beetje gespeeld met het dashboard van de omgeving. Dat ging zo makkelijk. Ik heb het voor elkaar gekregen om de bloedwaarden uit mijn bloedglucosemeter in te laden. Echt handig! De overzichten die ik normaal altijd bij Evelien zie, kwamen er zo uitrollen.

Al lopend naar de kamer vroeg ik Evelien wat dat MedMij precies inhoudt. “Wat leuk dat je ernaar vraagt. Daarmee kunnen we alle informatie die we zo gaan vastleggen op een veilige en betrouwbare manier ook met jou delen. Heb je al een eigen gezondheidsomgeving?” reageerde Evelien gelijk heel enthousiast. “Ja, die heb ik laatst uitgezocht met mijn zoon, Bart. Dat is toevallig, nietwaar?” reageerde ik. Evelien lachte naar me. “Wat mooi,” dacht ik, “dan kan ik alles wat we zo bespreken straks even rustig nalezen.” Het stelde me meteen gerust.

Evelien vroeg of ik al informatie had vastgelegd in de omgeving. “Uuh, ja,” stamelde ik en ik greep mijn telefoon om de bloedwaarden te laten zien. “Ik gebruik deze app om mijn bloedwaarden en gewicht zelf bij te houden,” vertelde ik aan Evelien. “Wat goed. De bedoeling is dat je die informatie ook met mij kan gaan delen. Blijf daar dus vooral mee doorgaan.”

Na onze afspraak liep Evelien snel even met me mee. Ze liet me zien hoe ik de praktijk kon vinden in de app van mijn persoonlijke gezondheidsomgeving. Ik moest de app van het platform openen en klikken op ‘Voeg nieuw contact toe’. Daar kon ik de naam invoeren die op de poster in de wachtkamer staat. Ik kreeg de informatie over de praktijk in de app te zien met de vraag of ik de gegevensuitwisseling met de praktijk tot stand wilde brengen. Evelien zei: “Ik moet helaas weer verder, je bent alleen nog niet klaar. De stappen spreken echter voor zich.” Evelien liep weg. Ik sloot de app. Dat doe ik straks wel even rustig als ik thuis ben.

Toen ik weer thuis was, ging ik verder in de app. Ik klikte op de optie om verbinding te maken. Vervolgens kon ik DigiD gebruiken, dat had ik al eens samen met mijn zoon gebruikt voor toeslagen bij de Belastingdienst. Ik voerde mijn gebruikersnaam in om vervolgens een pincode in te voeren. Hierna kreeg ik toegang tot een scherm waarin ik toestemming moest geven voor de gegevensuitwisseling tussen mijn huisarts en mijn persoonlijke gezondheidsomgeving. Ik kreeg te zien dat mijn huisarts toestemming vroeg om laboratoriumwaarden te verstrekken aan de persoonlijke gezondheidsomgeving. Ik gaf toestemming.

De browser op mijn telefoon sloot zich en ik kwam weer terug in de app van mijn gezondheidsomgeving. Ik zag in de contacten dat mijn huisarts was toegevoegd met de status dat ik was verbonden. Ik was gekoppeld met mijn huisarts en klaar om gegevens uit te wisselen.

Informatie uitwisselen met mijn apotheek

Nadat ik mijn huisarts had toegevoegd, ging ik kijken wie ik nog meer kon toevoegen. Na de keuze om een contact toe te voegen, ging ik naar het zoekscherm om te zoeken naar de apotheek van Ed. Nadat ik was ingelogd en toestemming had gegeven, kwam de gegevensuitwisseling gelijk tot stand. En zo kon ik ook het ziekenhuis en mijn tandarts toevoegen. Ik begrijp van het standaard scherm, dat ik steeds te zien krijg om toestemming te geven, dat ik steeds alleen toestemming geef voor de gegevensuitwisseling met mijn persoonlijke gezondheidsomgeving op dat moment. In de gebruiksvoorlichting die de leverancier van de persoonlijke gezondheidsomgeving toonde in een informatiepagina vond ik nog veel meer informatie over MedMij en waar ik goed op moest letten.

De toestemming voor de gegevensuitwisseling tussen mijn persoonlijke gezondheidsomgeving en het apothekerssysteem van Ed was de eerste stap om een overzicht te krijgen van de medicatie die ik via de apotheek heb ontvangen. Een actueel medicatieoverzicht heet dat in de omgeving. Eenmaal akkoord gegeven zag ik de medicatiegegevens binnenkomen in het medicatieoverzicht van de app. Dit overzicht had ik vanaf dat moment altijd beschikbaar binnen de app door hierop in te loggen met mijn vingerafdruk.

Iedere keer als ik medicijnen van een herhaalrecept of van een nieuw recept kreeg, werkte ik mijn medicatieoverzicht bij door de nieuwe gegevens binnen te halen. Toen dat een keer niet goed ging, nam ik contact op met de leverancier van de app via de contactgegevens die ik daarin vond. Deze hielp mij direct verder waardoor ik alsnog de nieuwste gegevens ontving.

Ik vond het zo leuk dat mijn medicatieoverzicht steeds werd bijgewerkt, dat ik het aan Ed vertelde. Hij reageerde gelijk ook heel enthousiast: "Handig hè, om al jouw medicatie-informatie op één plek te hebben?" "Wat ben jij goed op de hoogte," zei ik verbaasd tegen Ed. Hij begon te lachen en zei: "Ja, ik vind het interessant en ik ben vorige week naar een presentatie over dit onderwerp geweest." Hij wees me ook op de gebruikersvoorlichting die standaard wordt geleverd over het uitwisselen van gegevens via MedMij. "Als apotheker heb ik ook voorlichting mee gekregen van de leverancier van mijn informatiesysteem. Daarin staan veel goede tips en achtergronden", zei hij enthousiast.

Voortaan houd ik alles bij met mijn gezondheidsomgeving, ook wat ik wel en niet gebruik aan medicatie. Naast dat ik die informatie kan gaan delen met Evelien en Ed, heb ik er vooral zelf veel baat bij. Ik heb overal en altijd een actueel overzicht van wat ik aan medicatie verstrekt krijg en wat ik gebruik. Zeker in gesprekken met artsen is dat super. Ook de extra mogelijkheden die de omgeving me bieden, helpen me om meer grip te krijgen op mijn eigen gezondheid. Dat geeft me veel vertrouwen.

Afsprakenset

Voor u ligt release 1.5.1 van de afsprakenset van het MedMij Afsprakenstelsel. Release 1.5.1 is de opvolger van release 1.4.1 (zie Changelog).

De afsprakenset draagt bij aan veilige, interoperabele en betrouwbare gegevensuitwisseling tussen persoonlijke gezondheidsomgevingen en informatiesystemen van aanbieders. Deze afspraken moeten partijen voldoende vertrouwen en mogelijkheden geven om de onderlinge gegevensuitwisseling in de praktijk tot stand te brengen. De afsprakenset is preconcurrentieel. De afspraken zijn tot stand gekomen in samenwerking met diverse partijen in de zorg, zoals softwareleveranciers, het ministerie van Volksgezondheid, Welzijn en Sport, Patiëntenfederatie Nederland en vertegenwoordigers van aanbieders, onder andere via werkgroepen op de onderwerpen informatiestandaarden, gegevensuitwisseling /architectuur, juridisch en governance. Partijen die deelnemen aan het MedMij Afsprakenstelsel committeren zich aan de afspraken.

Het is mogelijk om beoogd deelname aan het afsprakenstelsel kenbaar te maken middels een aanmelding tot kandidaat-deelnemer. Zie voor meer informatie hierover https://www.medmij.nl/leveranciers/.

Leeswijzer

Wet- en regelgeving vormen de belangrijkste kaders voor de afsprakenset. De set beschrijft alleen dat wat nog niet in wet- en regelgeving is vastgelegd en wat nodig is voor het vertrouwen en de interoperabiliteit van deelnemers in de onderlinge gegevensuitwisseling.

De documentatie van de afsprakenset is als volgt opgebouwd:

- **Releaseinfo:** Het hoofdstuk biedt meta-informatie over deze release van de afsprakenset.
- **Grondslagen**: Een beschrijving van de achtergrond, criteria aan, principes voor, opzet van en begrippenlijst binnen het afsprakenstelsel.
- **Juridische context**: Een uitwerking van de juridische analyses.
- **Architectuur en technische specificaties:** De architectuurbeschrijving geeft een overzicht van de vereisten aan en vormgeving van de gegevensuitwisseling via MedMij. Dit is vertaald in technische specificaties die deelnemers, aangesloten op het MedMij-netwerk, dienen te implementeren om te voldoen aan de afspraken.
- **Normenkader informatiebeveiliging:** Het Normenkader informatiebeveiliging beschrijft de maatregelen die deelnemers minimaal dienen te treffen op het gebied van privacy en informatiebeveiliging. Deze maatregelen verminderen mogelijke risico's en komen voort uit een risicoanalyse die jaarlijks stelselbreed wordt uitgevoerd.
- **Beleid:** Het beleid gaat in op de vraag hoe Stichting MedMij omgaat met een aantal belangrijke besturingsthema's en vormt de basis voor de Operationele processen. Het beleid is richtinggevend voor het optreden van Stichting MedMij en de uitvoeringsorganisaties. Het bevat tevens verantwoordelijkheden voor deelnemers.
- **Operationele processen:** Een beschrijving van belangrijkste de operationele beheerprocessen die deelnemers raken.
- **Communicatie:** Het onderdeel communicatie bevat richtlijnen voor de communicatie over MedMij vanuit de deelnemers. Het bestaat uit afspraken over het gebruik van het merk MedMij, verplichte gebruikersvoorlichting en de opzet van een verplicht te gebruiken toestemmings- en bevestigingsverklaring.
- **Managementinformatie:** Managementinformatie beschrijft de sturingsinformatie die deelnemers periodiek dienen aan te leveren bij de beheerorganisatie.

Alle lezers wordt aangeraden om, alvorens de afsprakenset te bestuderen, eerst kennis te nemen van de stelselbrede Introductie en Afsprakenstelsel in de praktijk (release-onafhankelijk) en daarna van de context van voorliggende afsprakenset (Grondslagen en het Juridisch kader). Deze drie delen samen vormen een goed beeld van de achtergrond bij en de reikwijdte van het afsprakenstelsel. De Architectuur en technische specificaties, het Normenkader informatiebeveiliging, het Beleid, de Operationele processen, de afspraken rond Communicatie en Managementinformatie beschrijven vervolgens per onderwerp de verschillende afspraken.

Releaseinfo

In deze sectie is meta-informatie opgenomen over de release van de afsprakenset. De release- en versiebeschrijving duidt de positionering en status van deze publicatie. Wijzigingen ten opzichte van eerder gepubliceerde versies (en een historisch overzicht van wijzigingen) zijn opgesomd in de changelog.

Lezers met suggesties voor toekomstige releases kunnen gebruik maken van de hun ter beschikking staande communicatiekanalen met MedMij, of via info@medmij.nl.

Release- en versiebeschrijving

De releasebeschrijving beschrijft de belangrijkste kenmerken van de release. De versie betreft de versie van de release en duidt aan in welk stadium van ontwikkeling of besluitvorming de release zich bevindt. Een release die is vastgesteld door de Stichting MedMij heeft altijd versie 1.0. Hogere versienummers zijn alleen mogelijk als er documentatiecorrecties worden doorgevoerd. Inhoudelijke wijzigingen op een al vastgestelde release leiden altijd tot een nieuwe release. In het Change- en releasebeleid is beschreven hoe releases worden genummerd.

Release	1.5.1
Versie	1.0: Versie vastgesteld door het bestuur en de eigenaarsraad van Stichting MedMij.
Doel	Het bieden van de formele basis voor de eerste productiefase van MedMij, waarin het MedMij-netwerk operationeel zal zijn en dienstverlening aan de gebruikers plaatsvindt. Deelnemers sluiten een deelnemersovereenkomst af met de beheerorganisatie en committeren zich aan de afspraken.
Doelgroep	• potentiële *Deelnemers* (*Dienstverleners persoon* en *Dienstverleners zorgaanbieder*) • *Deelnemers* • alle onderdelen van de MedMij-organisatie (Stichting MedMij, programma MedMij, MedMij Beheer) • andere geïnteresseerden in het MedMij Afsprakenstelsel
Totstandkoming	De ontwikkeling van release 1.4.1 tot release 1.5.1 is uitgevoerd onder leiding van de MedMij-beheerorganisatie, in samenwerking met de Deelnemersraad en de Eigenaarsraad van MedMij, de Stichting MedMij en een keur aan andere betrokkenen bij MedMij.
Inwerkingtreding	Per datum van publicatie: 30 oktober 2021
Operationeel toepassingsgebied	• Allen die op 30 april 2022 *Deelnemer* aan MedMij zijn. Deze *Deelnemers* zijn gehouden release 1.5.1 te implementeren, zonder dat dit evenwel een heracceptatie vereist. • Allen die na 30 oktober 2021 zullen starten met een MedMij-acceptatie. Die acceptatie zal conform Testbeleid uitgevoerd worden tegen versie 1.4.1 of versie 1.5.1 van het Afsprakenstelsel. • De MedMij-beheerorganisatie.
Status	Afsprakenset geformaliseerd via vaststelling door Stichting MedMij.
Functionele scope	De functionele scope van release 1.5.1 ten opzichte van release 1.4.1 is niet gewijzigd. Voor overige wijzigingen zie Changelog release 1.5
Licentie	Creative Commons: Naamsvermelding-GeenAfgeleideWerken 4.0 Internationaal (CC BY-ND 4.0). 

Changelog

De changelog beschrijft de wijzigingen die achtereenvolgens zijn doorgevoerd bij releases van het MedMij Afsprakenstelsel.

Changelog release 1.5

Op de pagina Changelog release 1.5.0 zijn de changes opgenomen van release 1.5.1 ten opzichte van 1.4.1.

Changelog release 1.5.0

Hieronder vind je een overzicht van de grootste wijzigingen in het afsprakenstelsel ten opzichte van release 1.4.1 en een grove schatting van de impact die de wijziging heeft op de deelnemers.

Verplichte wijzigingen	Impact DVP	Impact DVZA
Om de gebruikersvriendelijkheid op een hoger niveau te krijgen, is het mogelijk gemaakt om in één handeling voor meerdere gegevensdiensten autorisatie te verlenen. In de huidige vorm zitten hier wel beperkingen aan. Autorisatie kan gegeven worden voor alle gegevensdiensten die namens een Aanbieder worden aangeboden door een Dienstverlener Aanbieder. Indien gebruik wordt gemaakt van deze optie, moeten de verschillende gegevensdiensten worden meegegeven in de scope van het verzoek. Voorheen mocht hier maar één gegevensdienst worden opgegeven.	Optioneel	Verplicht
De normen A.18.2.3 (1) en A.18.2.3 (2) zijn gewijzigd. De eisen te aanzien van een penetratietest zijn specifieker benoemd. Daarnaast hoeft te test niet altijd meer als whitebox test uitgevoerd te worden, maar kan een greybox test ook volstaan.	Verplicht	Verplicht
De Dienstverlener persoon is verplicht de gehele PGO te beveiligen met Multi Factor Authentication, waarbij de tweede factor bij voorkeur sterker is dan het gebruik van SMS.	Verplicht	Geen
In de Authorization en Token requests moet de `redirect_uri` URL-encoded zijn.	Verplicht	Verplicht
In het Authorization request moet de state parameter voldoen aan de nieuw gestelde eisen. Voorheen was er geen beperking betreffende de lengte.	Verplicht	Verplicht

Optionele wijzigingen	Impact DVP	Impact DVZA
Vrijwillige vertegenwoordiging is als extensie toegevoegd. Als dit door Deelnemers geïmplementeerd wordt, kan een Persoon (Vertegenwoordigde) zich laten vertegenwoordigen door een andere partij / Persoon (Vertegenwoordiger). Voor beide rollen (Dienstverlener persoon en Dienstverlener aanbieder) is het optioneel Vertegenwoordiging te implementeren. Daarom is een aantal uitzonderingen en verantwoordelijkheden gedefinieerd, zodat vermenging van gezondheidsgegevens zo veel als mogelijk wordt voorkomen.	Optioneel	Optioneel

Overige wijzigingen	Impact DVP	Impact DVZA
Herstructurering van 'Architectuur en technische specificaties' Dit onderdeel van het afsprakenstelsel is flink onder handen genomen om de leesbaarheid en bruikbaarheid voor deelnemers te vergroten. Wijzigingen die zijn doorgevoerd:	Geen	Geen

- Het afsprakenstelsel is opgedeeld in de MedMij Core en MedMij Extensies. De MedMij Core bevat die onderwerpen die essentieel zijn voor het in de regie stellen van Personen over de eigen gezondheidsgegevens. MedMij Extensies vormen een uitbreiding op de Core.
  - De functies *Verzamelen* en *Delen* zijn onderdeel van de MedMij Core. Daarentegen zijn de functies *Abonneren* en *Notificeren* onderdeel van een Extensie, namelijk Extensie Abonneren.
- De structuur van de onderwerpen is aangepast naar Rollen, Functies en gegevens, Verantwoordelijkheden.
- De focus van MedMij is breder dan alleen zorg. Daarom wordt in de MedMij Core en MedMij Extensies niet meer gesproken over zorg, maar is dit als een los domein toegevoegd (zie Zorg). Hiervoor is een aantal wijzigingen doorgevoerd in het rollenmodel van de MedMij Core en MedMij Extensies, namelijk:
  - *Zorggebruiker* → *Persoon*
  - *Zorgaanbieder* → *Aanbieder*
  - *Dienstverlener zorgaanbieder* → *Dienstverlener aanbieder*
- Het rollenmodel is aangepast:
  - De architectuur van het afsprakenstelsel is nu gebaseerd op de drie basislagen van enterprise architectuur, namelijk Business, Applicatie en Technologie. De vierde laag, oftewel de datalaag, wordt gevormd door de afspraken betreffende de gegevensdiensten. De laag Juridica is vervallen in de beschrijvingen, een aantal rollen is overgenomen in de businesslaag
  - Op de businesslaag is een aantal wijzigingen doorgevoerd:
    - *Stichting MedMij* is generiek beschreven als *Eigenaar MedMij*.
    - De rollen *Uitgever*, *Bron* en *Lezer* zijn verwijderd. In plaats hiervan wordt gewerkt met de bovenliggende rollen, namelijk *Dienstverlener persoon* en *Dienstverlener aanbieder*. De rollen *Uitgever*, *Bron* en *Lezer* zorgden voor discussie en onduidelijkheid. Door deze uit het afsprakenstelsel te halen is getracht de leesbaarheid en bruikbaarheid te verhogen.
    - De verantwoordelijkheden uit de businesslaag (voorheen Proces en Informatie) zijn met een gele achtergrond weergegeven. De verantwoordelijkheden uit de applicatielaag hebben een blauw achtergrond en voor de technologielaag is groen gebruikt.
  - Op de applicatielaag is een aantal wijzigingen doorgevoerd:
    - *PGO Presenter, PGO User Agent, OAuth User Agent* en *Authentication User Agent* zijn samengevoegd tot *User Agent*. De scheiding van deze twee rollen leverde onduidelijkheid bij Deelnemers en de meerwaarde van de scheiding was nihil.
    - *PGO Server* is hernoemd naar *DVP Server*. Hoewel DVP en PGO nauw gekoppeld zijn, richt MedMij zich op de DVP-rol en niet op de gehele PGO.
  - Op de technologielaag is een aantal wijzigingen doorgevoerd:
    - Omdat de rol van *Internet* nergens duidelijk als rol beschreven wordt, is besloten deze niet meer als rol terug te laten komen. Uit verschillende verantwoordelijkheden is te herleiden is dat *Internet* het achterliggende netwerk is
    - In plaats van *MedMij Stelselnode*, *PGO Node* en *ZA Node* is gekozen voor een opdeling tussen *Backchannel Node* en *Frontchannel Node*, om zo meer duidelijkheid te kunnen geven over de verschillen tussen backchannel en frontchannel.
    - *PKIoverheid TSP* wordt niet meer als rol getoond in het rollenmodel. De reden hiervoor is dat MedMij gebruikmaakt van het stelsel van PKIoverheid, maar dat PKIoverheid zelf als partij geen rol heeft in het afsprakenstelsel. In de verantwoordelijkheden wordt wel verwezen naar PKIoverheid en staat beschreven hoe de certificaten gebruikt moeten worden.

• Alle verantwoordelijkheden hebben een unieke code gekregen, waarmee eenvoudiger gerefereerd kan worden aan deze verantwoordelijkheden. De mapping van 1.4.0 naar 1.5.0 is in deze changelog te vinden.		

Omdat Zorg het enige domein is dat op dit moment door het afsprakenstelsel ondersteund wordt, is een aantal onderdelen van het afspraken nog niet herzien. Dit moet uitgevoerd worden zodra een nieuw domein wordt toegevoegd. Het gaat hierbij voornamelijk om juridische onderdelen:
 	
• Juridische context
  • Juridisch kader
  • Overeenkomsten en rechtsrelaties
  • Toelichting verwerkingsverantwoordelijkheid
• Informatiemodellen
  • Metamodel
  • Logische modellen
  • XML-schema's
  • XML-bestanden voor lijsten
• Communicatie
  • Toestemmingsverklaring
  • Toestemmingsverklaring Abonneren
  • Bevestigingsverklaring
  • Beëindigingsverklaring Abonnement
• Deelnemersovereenkomsten
  • Deelnemersovereenkomst Dienstverlener persoon
  • Deelnemersovereenkomst Dienstverlener aanbieder
• Toetreding
  • Toetredingsbeleid
  • Intentieverklaringen
  • Intentieverklaring Dienstverlener persoon
  • Intentieverklaring Dienstverlener zorgaanbieder
• Modelverwerkersovereenkomst
	Geen	Geen

Het publiceren van gegevensdiensten wordt zoveel als mogelijk gecombineerd met de release van een nieuwe versie van het afsprakenstelsel.	Geen	Geen
De HTML en CSS-bestanden geven een indicatie over wat de schermen moeten tonen. Beschreven is nu dat het niet verplicht is deze HTML en CSS te volgen.	Geen	Geen

Correcties op release 1.5.0

Op deze pagina worden alle correcties, voorziene en doorgevoerde, bijgehouden op deze release van het MedMij Afsprakenstelsel. Bij correcties gaat het om aanpassingen die de inhoudelijke strekking van de tekst van het MedMij Afsprakenstelsel niet raken. Voorbeelden zijn:

- gebroken of foute verwijzingen
- fouten in terminologie
- weggevallen passages
- taalfouten.

Om te voorkomen dat lezers van het MedMij Afsprakenstelsel voortdurend een lijst van errata zouden moeten raadplegen, worden de correcties doorgevoerd in de hoofdtekst. Onderstaande tabel geldt daarbij als vastlegging van de correctiegeschiedenis.

Nr	Pagina('s)	Correctie(s)	Reden	Aangepast op

150001	Normenkader informatiebeveiliging	Document aangepast en de link naar de download aangepast. Het document verwees naar versie 1.3.0
		
		• Versienummer op de laatste pagina aangepast naar 1.5.0
		• Normen gelijkgetrokken
		  • 9.4.1
		  • 18.2.3(1)
		  • 18.2.3(2)
			Correctie	11-feb-2022

Mapping van 1.4.0 naar 1.5.0

Plaats in 1.4.0			Code in 1.5.0	Uitleg
Processen en informatie	Rollen	1	-	Er is geen rol Uitgever meer, waarmee deze verantwoordelijkheid kwam te vervallen.
		2	-	Er is geen rol Bron of Lezer meer, waarmee deze verantwoordelijkheid kwam te vervallen.
		3	core.rollen.100	
		4	dmn.zorg.rollen.100	Omdat het over de rol Zorggebruiker gaat, is deze verplaatst naar Domein Zorg.
	Verantwoordelijkheden	1a	core.dossier.100	
		1b	core.dossier.101	
		1c	core.dossier.102	
		2a	core.dossier.103	
		2b	core.dossier.104	
		3a	ext.abo.abonneren.100	Abonneren valt niet onder de functies van de MedMij Core, waardoor deze verplaatst is naar de extensie Gegevensuitwisseling.
		3b	ext.abo.abonneren.101	
		3c	ext.abo.abonneren.102	
		3d	ext.abo.abonneren.103	
		3e	ext.abo.abonneren.104	
		3f	ext.abo.notificeren.103	Notificeren valt niet onder de functies van de MedMij Core, waardoor deze verplaatst is naar de extensie Gegevensuitwisseling.
		3g	ext.abo.notificeren.104	
		3h	ext.abo.notificeren.105	

3i	ext.abo.abonneren.105	Abonneren valt niet onder de functies van de MedMij Core, waardoor deze verplaatst is naar de extensie Gegevensuitwisseling.
4	core.gegevensdiensten.100	
5	core.gegevensdiensten.101	
6	core.gegevensdiensten.102	
7a	core.gegevensdiensten.103	
7b	core.gegevensdiensten.104	
8a	core.autorisatie.100	
8b	core.autorisatie.101	
8c	ext.abo.autorisatie.100	Abonneren valt niet onder de functies van de MedMij Core, waardoor deze verplaatst is naar de extensie Gegevensuitwisseling.
9	core.authenticatie.100	
10	core.alst.100	
11	core.lijsten.100	
12	core.alst.101	
13	core.alst.102	
14a	core.ocl.100	
14b	core.ocl.101	
15	core.ocl.102	
16	core.gnl.100	
17	core.gnl.101	
18	core.whl.100	

		19a	core.logging.100	
		19b	ext.abo.logging.100	Abonneren valt niet onder de functies van de MedMij Core, waardoor deze verplaatst is naar de extensie Gegevensuitwisseling.
		19c	core.logging.101	
		20	core.algemeen.200	
		21a	core.logging.102	
		21b	core.logging.103	
		21c	core.logging.104	
		21d	core.logging.105	
	Beschikbaarheids- en ontvankelijkheidsvoorwaarde	1a	dmn.zorg.besont.100	Omdat het over de rol Zorgaanbieder gaat, is deze verplaatst naar Domein Zorg.
		1b	dmn.zorg.besont.101	
		1c	dmn.zorg.besont.102	
		1d	dmn.zorg.besont.103	
		2	dmn.zorg.besont.104	
		3	-	Dit is verplaatst naar de inleidende tekst. De beschrijving vormde geen verantwoordelijkheid.
Applicatie	Rollen	1a	core.rollen.200	
		1b	ext.abo.rollen.200	
		2a	core.rollen.201 & core.rollen.202 & ext.abo.rollen.201	De verantwoordelijkheid is opgesplitst, om de leesbaarheid te verhogen. Daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de Subscription Server.
		2b	ext.abo.rollen.202	Abonneren valt niet onder de functies van de MedMij Core, waardoor deze verplaatst is naar de extensie Gegevensuitwisseling.
		2c	ext.abo.rollen.203	
		3	core.rollen.203	

		4	core.rollen.204	
		5	core.rollen.205	
		6	core.rollen.206 & ext.abo.rollen.204	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de Subscription Server.
		7	core.rollen.207 & ext.abo.rollen.205	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de Subscription Server.
		8	-	Dit is verplaatst naar de Begrippenlijst. De beschrijving vormde geen verantwoordelijkheid.
	Verantwoordelijkheden	1a	-	Implementatie staat uitgewerkt bij Verzamelen.
		1b	-	Implementatie staat uitgewerkt bij Delen.
		1c	-	Implementatie staat uitgewerkt bij de functies.
		2	core. gegevensdiensten. 200 & ext.abo. autorisatie.200	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de functie Abonneren.
		3	core.autorisatie. 200	
		4	core.autorisatie. 201	
		5	core.autorisatie. 202	
		6	core.autorisatie. 203	
		7	core.autorisatie. 204	

8a	core.autorisatie.205	
8b	core.autorisatie.206	
8c	core.autorisatie.207	
8d	core.autorisatie.208	
8e	core.autorisatie.209	
9	core.autorisatie.210	
10a	core.alst.200	
10b	core.alst.201	
10c	core.alst.202	
11a	core.ocl.200	
11b	core.ocl.201	
11c	core.ocl.202	
12a	core.gnl.200	
12b	core.gnl.201	
12c	core.gnl.202	
13	core.beveiliging.200	
14	core.beveiliging.201	
15	core.beveiliging.202	
16	core.beveiliging.203	
17	core.beveiliging.204	
18	core.beveiliging.205	
19a	core.logging.200	
19b	core.logging.201	

Interfaces	1a	core.adressering.200 & ext.abo.adressering.200	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de rol Subscription Server.
	1b	core.adressering.201	
	2a	core.adressering.202 & ext.abo.adressering.201	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de Subscription en Notification interfaces.
	2b	core.adressering.203 & ext.abo.adressering.202	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de Subscription request.
	2c	ext.abo.adressering.203	Subscription notification en resource notification vallen niet onder de functies van de MedMij Core, waardoor deze verplaatst is naar de extensie Gegevensuitwisseling.
	3	core.adressering.204	
User interface (Autorisatieserver)	1	core.usrint.100 & ext.abo.usrint.100	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de functie abonneren.
	2	core.usrint.101 & ext.abo.usrint.101	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de functie abonneren.
	2a	core.usrint.102	

	2b	core.usrint.103	
	2c	ext.abo.usrint.102	De functie Abonneren valt niet onder de functies van de MedMij Core, waardoor deze verplaatst is naar de extensie Gegevensuitwisseling.
Authorization interface	1a	core.authint.200 & ext.abo.authint. 200	De scope subscribe valt niet onder de functies van de MedMij Core, waardoor deze verplaatst is naar de extensie Gegevensuitwisseling.
	1b	core.authint.201	
	2a	core.authint.202	
	2b	core.authint.203 & ext.abo.authint. 201	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de scope subscribe.
	3	core.authint.204	
	4	core.authint.205 & ext.abo.authint. 202	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de functie Abonneren.
	5	core.authint.206	
	6	core.authint.207 & ext.abo.authint. 203	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de functie Abonneren.
Token interface	1	core.tknint.200	
	2	core.tknint.201 & ext.abo.tknint.200	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de functie Abonneren.
	3a	core.tknint.202	

		3b	core.tknint.203	
		3c	core.tknint.204	
		4	core.tknint.205	
		5	core.tknint.206 & ext.abo.tknint.201	De verantwoordelijkheid geldt ook voor de functie Abonneren.
		6	core.tknint.207 & ext.abo.tknint.202	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de functie Abonneren.
	Resource interface	1a	core.rscint.200	
		1b	core.rscint.201	
		2	core.rscint.202	
		3	core.rscint.203	
		4	core.rscint.204	
	Subscription interface	1a	ext.abo.subint.200	De Subscription Interface valt niet onder de functies van de MedMij Core, waardoor deze verplaatst is naar de extensie Gegevensuitwisseling.
		1b	ext.abo.subint.201	
		1c	ext.abo.subint.202	
		2a	ext.abo.subint.203	
		2b	ext.abo.subint.204	
		3a	ext.abo.subint.205	
		3b	ext.abo.subint.206	
		3c	ext.abo.subint.207	
		4a	ext.abo.subint.208	
		4b	ext.abo.subint.209	
		4c	ext.abo.subint.210	
		5a	ext.abo.subint.211	
		5b	ext.abo.subint.212	
		5c	ext.abo.subint.213	
		6	ext.abo.subint.214	
		7	ext.abo.subint.215	

	8	ext.abo.subint.216	
Subscription notification interface	1a	ext.abo.subnotint.200	De Subscription Notification Interface valt niet onder de functies van de MedMij Core, waardoor deze verplaatst is naar de extensie Gegevensuitwisseling.
	1b	ext.abo.subnotint.201	
	1c	ext.abo.subnotint.202	
	1d	ext.abo.subnotint.203	
	2	ext.abo.subnotint.204	
	3	ext.abo.subnotint.205	
	4	ext.abo.subnotint.206	
	5	ext.abo.subnotint.207	
Resource notification interface	1a	ext.abo.rscnotint.200	De Resource Notification Interface valt niet onder de functies van de MedMij Core, waardoor deze verplaatst is naar de extensie Gegevensuitwisseling.
	1b	ext.abo.rscnotint.201	
	1c	ext.abo.rscnotint.202	
	1d	ext.abo.rscnotint.203	
	2	ext.abo.rscnotint.204	
	3	ext.abo.rscnotint.205	
	4a	ext.abo.rscnotint.206	
	4b	ext.abo.rscnotint.207	
	5	ext.abo.rscnotint.208	
GNL-, OCL- en ZAL-interface	1	core.lijsten.300	
	2	core.lijsten.301	
	3	core.lijsten.302	

		4	core.lijsten.303	
Netwerk	Rollen	1	core.rollen.300	
		2	core.rollen.301 & ext.abo.rollen.300	De verantwoordelijkheid is opgesplitst. Een deel is in de MedMij Core geplaatst, daarnaast is in de extensie Gegevensuitwisseling een uitbreiding geplaatst, gericht op de rol Subscription Server.
		3	-	Hoewel PKIoverheid nog steeds gebruikt moet worden voor beveiliging, is de rol verwijderd uit het rollenmodel.
	Verantwoordelijkheden	1a	core.tls.300	
		1b	core.tls.301	
		1c	core.tls.302	
		1d	core.tls.303	
		1e	core.tls.304	
		1f	core.tls.305	
		2	core.tls.306	
		3	core.tls.307	
		4	-	De verantwoordelijkheid staat in de andere verantwoordelijkheden beschreven en was dus dubbel.
		5	core.tls.308	
		6a	core.tls.309	
		6b	core.tls.310	
		6c	core.tls.311	
		6d	core.tls.312	
		6e	core.tls.313	
		7	core.whl.300	
		8	core.whl.301	
		9	core.whl.302	
		10	core.whl.303	
		11	core.whl.304	

		12	core.whl.305	
		13	core.whl.306	
		14a	core.whl.307	
		14b	core.whl.308	
		15	core.whl.309	
		16	core.dns.300	
		17	core.dns.301	
		18	core.ocl.300	
	WHL-Interface	1	core.lijsten.300	
		2	core.lijsten.301	
		3	core.lijsten.302	
		4	core.lijsten.303	

Changelog release 1.5.1

Hieronder volgt een overzicht van de grootste wijzigingen in het Afsprakenstelsel ten opzichte van release 1.5.1 en een grove schatting van de impact die de wijziging heeft op de deelnemers.

Verplichte wijzigingen	Impact DVP	Impact DVZA

Optionele wijzigingen	Impact DVP	Impact DVZA

Overige wijzigingen	Impact DVP	Impact DVZA
Wijzigingen PKIoverheid De wijzigingen vanuit RFC0065 (Patch), AF-1349 Gebruik publieke certificaten in afsprakenstelsel 1.5 zijn doorgevoerd. Voor partijen die op 25-02-2022 al deelnemer waren van MedMij heeft dit niet direct impact. De wijzigingen gelden wel direct voor nieuwe deelnemers. Bestaande deelnemers moeten voor 04-12-2022 voldoen aan de nieuwe eisen.	Geen	Geen

Correcties op release 1.5.1

Op deze pagina worden alle correcties, voorziene en doorgevoerde, bijgehouden op deze release van het MedMij Afsprakenstelsel. Bij correcties gaat het om aanpassingen die de inhoudelijke strekking van de tekst van het MedMij Afsprakenstelsel niet raken. Voorbeelden zijn:

- gebroken of foute verwijzingen
- fouten in terminologie
- weggevallen passages
- taalfouten.

Om te voorkomen dat lezers van het MedMij Afsprakenstelsel voortdurend een lijst van errata zouden moeten raadplegen, worden de correcties doorgevoerd in de hoofdtekst. Onderstaande tabel geldt daarbij als vastlegging van de correctiegeschiedenis.

Nr	Pagina('s)	Correctie(s)	Reden	Aangepast op
151001	Verantwoordelijkheden, Core Opvragen Gegevensdienstnamenlijst	Verschillende foutieve links verbeterd en typefouten aangepast	Correctie	25-feb-2022

Changelog release 1.4

Op de pagina Changelog release 1.4.0 zijn de changes opgenomen van release 1.4.0 ten opzichte van 1.3.0.

Changelog release 1.4.0

Hieronder volgt een overzicht van de grootste wijzigingen in het Afsprakenstelsel ten opzichte van release 1.2.0 en een grove schatting van de impact die de wijziging heeft op de deelnemers.

Verplichte wijzigingen	Impact DVP	Impact DVZA
Verwijzing naar ICT-beveiligingsrichtlijnen 2.1 van NCSC (Netwerk) Op de pagina Netwerk bij 'TLS en certificaten' wordt vanaf deze release verwezen naar versie 2.1 van de ICT-beveiligingsrichtlijnen van NCSC. De regels rondom het gebruik van deze richtlijnen is uitgebreid. Deze wijzigingen beschrijven dat: • alle deelnemers TLS 1.2 moeten ondersteunen. • alle deelnemers TLS 1.3 moeten ondersteunen, indien redelijkerwijs mogelijk. • bij de TLS-handshake de hoogste toegestane TLS-versie gekozen moet worden die beide partijen ondersteunen.	Midden	Midden
Knop 'annuleren' op landings- en annuleringspagina (Landingspagina & Annuleringspagina) Op zowel de landingspagina als de annuleringspagina, die de DVZA toont namens de zorgaanbieder, is een knop "annuleren" toegevoegd, waarmee de gebruiker kan terugkeren naar de PGO zonder geauthentiseerd te zijn. Dit resulteert in uitzonderingssituatie 2 op het Authorization Interface.	Klein	Klein
Aanscherping Uitzonderingen OAuth (Resource interface & Subscription interface) In de specificaties van de Resource en Subscription Interface is de juiste toepassing van de OAuth standaard in uitzonderingssituaties beschreven. Deze moeten worden toegepast.	Midden	Midden

Optionele wijzigingen	Impact DVP	Impact DVZA
Validaties op de Token interface (Applicatie) Regel 8e is toegevoegd aan de pagina Applicatie. Er wordt verwezen naar een controle van het gebruikte certificaat bij de aanroep van de Token Interface, zoals beschreven in IETF RFC 8705. In deze release van het afsprakenstelsel wordt deze validatie als optioneel beschouwd voor de DVZA's. De DVP's moeten informatie doorgeven betreffende de credentials van het te gebruiken certificaat.	Klein	Midden

Addendum aanbieder zonder behandelrelatie Het MedMij afsprakenstelsel ondersteunt op het moment enkel uitwisseling tussen zorggebruikers en zorgaanbieders wanneer de zorggebruiker met de betreffende zorgaanbieder een behandelrelatie in de zin van de WGBO heeft (gehad). Er zijn echter ook relevante gezondheidsgegevens over de zorggebruiker beschikbaar in andere domeinen. Een voorbeeld hiervan is het publieke gezondheidsdomein (Wet publieke gezondheid), waar onder meer informatie bekend is over welke vaccinaties zijn gegeven in het kader van het rijksvaccinatieprogramma en Covid-19. Ook bij de uitvoering van de Wet langdurige zorg zijn er relevante gegevens bekend bij bijvoorbeeld het CIZ en bij zorgkantoren. Dit addendum maakt het mogelijk om ook deze gezondheidsgegevens te kunnen uitwisselen met het persoonsdomein door *Aanbieders* zonder behandelrelatie te ondersteunen en beschrijft de wijzigingen in verantwoordelijkheden en implementatie die een DVZA moet doorvoeren. Een aanbieder zonder behandelrelatie mag enkel op het MedMij netwerk diensten aanbieden na uitdrukkelijke toestemming van stichting MedMij.	Geen	Midden

Overige wijzigingen	Impact DVP	Impact DVZA
Leesbaarheid afsprakenstelsel De opmaak van veel pagina's is gewijzigd. De toelichtingen, die in zichtbare infoblokken stonden, zijn opnieuw doorgenomen. De inhoudt van deze blokken is: • of als normale tekst in een hoofdstuk geplaatst, • of als toelichting in een te openen box geplaatst, daar waar de toelichting naar verwees, • of als extra regel toegevoegd aan de verantwoordelijkheden, • of verwijderd, als de inhoud geen meerwaarde had.	Geen	Geen
Verwijzing naar RFC 8705 (Token interface) In de beschrijving van de token interface wordt bij het attribuut 'client_id' verwezen naar de geldende versie van IETF RFC 8705, met betrekking tot Mutual TLS Client Authentication. Tevens is de tekst aangepast, zodat direct duidelijk is dat het gebruik van client_id verplicht is.	Geen	Geen
Beschrijving certificaatwissel verwijderd De teksten betreffende de wissel van PKIoverheid certificaten is verwijderd. In release 1.3.0 is benoemd hoe om te gaan met G3 certificaten. Omdat de certificatenwissel volledig is doorgevoerd, kon dit informatieblok volledig worden verwijderd.	Geen	Geen
Beschrijving attribuut state aangepast (Authorization interface) De beschrijving van het attribuut state van de Authorization Interface is versimpeld. Er wordt alleen nog verwezen naar sectie 4.1.1. van RFC 6749. Voorheen werd ook aangegeven dat de waarde geen URI mag bevatten. Omdat de waarde volgens RFC 6749 'OPAQUE' moet zijn, was de tweede regel overbodig.	Geen	Geen

Correcties bij de changelog geplaatsts De pagina voor correcties op de release van het afsprakenstelsel is verplaatst naar de Changelog, onder de pagina voor diezelfde release. Hiermee is er een duidelijke koppeling tussen Changelog van een release en de bij die release behorende correcties.	Geen	Geen
Nieuwe tekst 'Achtergrond' (Achtergrond) De pagina 'Achtergrond' is voorzien van een nieuwe tekst, die beter aansluit bij de huidige situatie van het afsprakenstelsel.	Geen	geen

Correcties op release 1.4.0

Met deze pagina worden alle correcties, voorziene en doorgevoerde, bijgehouden op deze release van het MedMij Afsprakenstelsel. Bij correcties gaat het om aanpassingen die de inhoudelijke strekking van de tekst van het MedMij Afsprakenstelsel niet raken. Voorbeelden zijn:

- gebroken of foute verwijzingen;
- fouten in terminologie;
- weggevallen passages;
- taalfouten.

Om te voorkomen dat lezers van het MedMij Afsprakenstelsel voortdurend een lijst van errata zouden moeten raadplegen, worden de correcties doorgevoerd in de hoofdtekst. Onderstaande tabel geldt daarbij als vastlegging van de correctiegeschiedenis.

Nr	Pagina('s)	Correctie(s)	Reden	Aangepast op
140001	Toelichting verwerkingsverantwoordelijkheid	Gebroken link naar Juridisch kader hersteld.	Correctie	20210506
140002	Overeenkomsten en rechtsrelaties	Gebroken links naar Modelverwerkersovereenkomst hersteld	Correctie	20210614
140003	Resource interface	Correctie: Flow mag worden voortgezet bij uitzondering 6	Correctie	20210709
140004	Authorization interface	Correctie: Tabel inhoud verschoven, nu gecorrigeerd	Correctie	20210712
140005	Functie Server Authentication	Correctie: Uitzondering met betrekking tot het gebruik van EV-certificaten voor M2M toepassingen toegevoegd aan regel 6d.	Correctie	20210715
140006	XML-schema's	Correctie: Definitie van Zorgaanbiedernaam in scheme portabiliteitsrapportage bijgewerkt.	Correctie	20210720

Changelog release 1.3

Op de pagina Changelog release 1.3.0 zijn de changes opgenomen van release 1.3.0 ten opzichte van 1.2.0.

Changelog release 1.3.0

Hieronder volgt een overzicht van de grootste wijzigingen in het Afsprakenstelsel ten opzichte van release 1.2.0 en een grove schatting van de impact die de wijziging heeft op de deelnemers.

Changes die interoperabiliteit direct raken	Impact DVP	Impact DVZA
Extra controles door Authorization interface - De *Autorisatieserver* dient voortaan een controle op de redirect url tegen waarde in de OCL uit te voeren. DVP's zullen een redirect url moeten opvoeren.	Klein: opvoeren endpoint	Klein
Extra uitzondering Token interface - Niet langer toegestaan om uitzondering met betrekking tot beschikbaarheids- of ontvankelijkheidsvoorwaarde op Token Interface te geven. De desbetreffende uitzonderingssituatie is verwijderd.	Mogelijk (zeer klein)	Klein
Extra controles Token interface - Zowel DVP als DVZA moeten extra controles uitvoeren op dit koppelvlak om onveiligheden in OAuth2 te mitigeren	Klein	Klein
Logging eisen zijn aangepast - Logging gebeurt nu op basis van een door DVP verstrekt ID op het Resource interface	Klein	Klein
Changes optionele functionaliteit die interoperabiliteit raken		
De Subscription interface is herzien - Belangrijkste wijziging zijn dat de de verantwoordelijkheden rond Abonnement zijn aangepast en de Subscription interface nu restful is uitgewerkt	Groot	Groot
Overige significante changes		
Verduidelijking communicatie Zorgaanbieder - Zorggebruiker - In de usecases (implementaties) van UCI Verzamelen, UCI Delen en UCI Abonneren zijn nieuwe schermen opgenomen om duidelijk te maken wanneer de *Zorgebruiker* met de *Zorgaanbieder* interacteert. Bestaande schermen bevatten een beperkte wijziging.	Geen	Midden
De MedMij Catalogus is vernieuwd, Register van Informatiestandaarden is vervallen - Het *Register van Informatiestandaarden* is vervallen, voortaan worden *Informatiestandaarden* niet meer zelfstandig toegelaten maar worden de eisen waaraan een systeemrol/*Informatiestandaard* moet voldoen meegewogen bij het samenstellen van een specifieke *Gegevensdienst*. De *Catalogus* is uitgebreid om de relevante onderdelen van het *Register van Informatiestandaarden* over te kunnen nemen. Tegelijkertijd is die geoptimaliseerd zodat die alleen relevante en heldere concepten bevat. De *Catalogus* wordt beschikbaar gesteld als XML-bestand en een automatische vertaling naar een gebruiksvriendelijke versie. Het Gegevensdienstenbeleid reflecteert de vereenvoudiging.	Geen	Geen

Relatie tussen Gegevensdiensten en Interfaceversies is geëxpliciteerd - In de *Catalogus* wordt aangegeven met welke *Interfaceversies* een *Gegevensdienst* mag worden gebruikt.	Geen	Geen
Het Testbeleid is verhelderd - Belangrijkste verheldering is dat de erkenning op een *Systeemrol* een onbeperkte geldigheidsduur heeft.	Geen	Geen
Encryptie opslag persoonsgegevens in het persoonsdomein - Er is meer keuzevrijheid in de vorm van toegepaste encryptie waardoor het ook wordt toegestaan om persoonsgebonden encryptie toe te passen.	Meer vrijheid	Geen
De Overeenkomsten en rechtsrelaties die spelen in de context van MedMij zijn verduidelijkt	Geen	Geen
Openbare publicatie Zorgaanbieder - Gegevensdienst combinaties - MedMij zal een publiek toegankelijke Zorgaanbiederskoppellijst publiceren.	Geen	Procesmatig: Verklaring van zorgaanbieder is aangepast (Operationele processen)
De DVP moet een nieuwe indicator in de Managementinformatie opleveren - De nieuwe indicator is een vereiste indicator voor subsidieregelingen vanuit VWS.	Midden	Mogelijk (zeer klein)

Correcties op release 1.3.0

Met deze pagina worden alle correcties, voorziene en doorgevoerde, bijgehouden op deze release van het MedMij Afsprakenstelsel. Bij correcties gaat het om aanpassingen die de inhoudelijke strekking van de tekst van het MedMij Afsprakenstelsel niet raken. Voorbeelden zijn:

- gebroken of foute verwijzingen;
- fouten in terminologie;
- weggevallen passages;
- taalfouten.

Om te voorkomen dat lezers van het MedMij Afsprakenstelsel voortdurend een lijst van errata zouden moeten raadplegen, worden de correcties doorgevoerd in de hoofdtekst. Onderstaande tabel geldt daarbij als vastlegging van de correctiegeschiedenis.

Nr	Pagina('s)	Correctie(s)	Reden	Aangepast op
1.3.0-1	Resource notification interface	Stap 1c gecorrigeerd	Verkeerde merge	5 november 2020
1.3.0-2	Subscription notification interface	Stap 1c gecorrigeerd	Verkeerde merge	5 november 2020
1.3.0-3	Authorization interface	Scope toelichting over duur met waarde 0 gecorrigeerd.	Typo's en redactiewerk	5 november 2020
1.3.0-4	Netwerk	Ondersteuning G3 certificaten tot 31 december 2020	Correctie	11 november 2020
1.3.0-5	Token interface	Uitzondering Token interface 2 verwijderd (conform RFC0015 Uitzondering Token interface 2)	Typo's en redactiewerk	12 november 2020
1.3.0-6	Changelog release 1.3.0	RFC0015/token interface wijziging gecorrigeerd (conform RFC0015 Uitzondering Token interface 2)	Typo's en redactiewerk	12 november 2020
1.3.0-7	Token interface	RFC0014 Extra controles door Authorization Interface correctie toegepast	Typo's en redactiewerk	12 november 2020
1.3.0-8	Changelog release 1.3.0	Extra controle RFC0014 Extra controles door Authorization Interface toegevoegd	Typo's en redactiewerk	12 november 2020
1.3.0-9	XML-schema's	Schema OCL aangepast ivm backwards compatibility (redirect_url niet verplicht voor 1.2.0 entries)	Correctie	13 november 2020
1.3.0-10	A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	Correctie op RFC0013 Meer mogelijkheden voor encryptie toestaan doorgevoerd.	Correctie	16 november 2020

1.3.0-11	Normenkader informatiebeveiliging	Verouderde versie changelog normenkader vervangen door nieuwe.	Correctie	16 november 2020
1.3.0-12	Aanvullende auditverklaring en onderbouwende rapportage	Verwijzing naar correcte versie afsprakenstelsel	Typo's en redactiewerk	16 november 2020
1.3.0-13	Normenkader informatiebeveiliging	Word download van normenkader vervangen door nieuwe versie	Typo's en redactiewerk	16 november 2020
1.3.0-14	Resource interface	Correctie bij uitzondering 3: treedt op als uitzonder 1 én 2 niet van toepassing zijn	Correctie	27 november 2020
1.3.0-15	Interfaces lijsten	Parameter in uri's vervangen naar 1.3.0	Correctie	2 december 2020
1.3.0-16	XML-schema's	Voorbeelden bijgewerkt met tijdzone in tijdstempels	Correctie	12 december 2020
1.3.0-17	Statuten Stichting MedMij	Link naar statuten hersteld	Typo's en redactiewerk	23 januari 2021

Changelog release 1.2

Changelog release 1.2.0

Release 1.2.0 zal enkele veranderingen omvatten waarvoor *Dienstverleners persoon* en/of *Dienstverleners zorgaanbieder* hun oplossingen (zeker of eventueel) zullen moeten aanpassen om compatibel te blijven (backwards-incompatible changes). Het gaat om wijzigingen voor zowel *Dienstverleners zorgaanbieder* als *Dienstverleners persoon*.

- **Abonneren en notificeren** — Het MedMij Afsprakenstelsel gaat het abonneren op notificaties over *Gegevensdiensten* (voor *Verzamelen)* mogelijk maken. Er zijn twee nieuwe use cases met bijbehorende use case-implementaties: *Abonneren* en *Notificeren*. Er zijn drie nieuwe interfaces: het subscription interface, het resource notification interface en het subscription notification interface. De schema's van de *Zorgaanbiederslijst* en de *OAuthclientlist* zijn hierop aangepast. De functionaliteit is optioneel: *Deelnemers* die er geen gebruik van wensen te maken, kunnen zich beperken tot het kunnen verwerken van de nieuw gestructureerde lijsten.
- **Versionering van interfaces** — Alle interfaces krijgen een versie, behorend bij de versie van het MedMij Afsprakenstelsel waarin zij zijn gedefinieerd. Dat maakt het mogelijk om meerdere versies van hetzelfde interface naast elkaar actief te laten zijn op het MedMij-netwerk, bijvoorbeeld in overgangsperiodes naar een nieuwe release van het MedMij Afsprakenstelsel. Het betekent o.a. dat *Dienstverleners zorgaanbieder* (actieve) versienummers gaan opgeven voor in de *Zorgaanbiederslijst* en *Dienstverleners persoon* voor in de *OAuthclientlist.*
- **Zorgaanbiedersnamen** — De maximale lengte van de *Zorgaanbiedersnaam* is vergroot; daarnaast is er een verplichting voor de *Dienstverlener zorgaanbieder* toegevoegd om bij toevoeging aan de *Zorgaanbiederslijst* een verklaring van de *Zorgaanbieder* over het opvoeren van een *Zorgaanbiedersnaam* te kunnen overleggen.
- **Portabiliteit tussen PGO's** — *Dienstverleners persoon* moeten de nieuwe *UC Portabiliteitsrapport* ondersteunen. Voor deze exportfunctionaliteit is een XML-schema opgenomen.
- **Beheerrapport** — Beheerrapportages moeten door alle *Deelnemers* gaan worden aangeleverd. Voor deze rapportages is een XML-schema opgenomen in het MedMij Afsprakenstelsel.
- **Structuur *Zorgaanbiederslijst* en *OAuthclientlist*** — Er komen nieuwe versies van de XML-schema's van de *Zorgaanbiederslijst* en de *OAuthclientlist,* om versionering van interfaces mogelijk te maken, en om abonneren en notificeren mogelijk te maken. Voorts moet in de Zorgaanbiederslijst gebruik gemaakt gaan worden van base-URLs, waar de Dienstverlener zorgaanbieder zijn Resource Server daarmee heeft geconfigureerd.
- **Verplichting client_id in het token request** — Het `client_id` wordt een verplichte parameter in het token request. Deze verandering is al in release 1.1.2 voorbereid door *Dienstverleners zorgaanbieder*; zij accepteren sindsdien token request met én zonder `client_id`. In release 1.2.0 worden de twee laatste stappen gezet: *Dienstverleners persoon* nemen de `client_id` op in het token request, terwijl *Dienstverleners zorgaanbieder* token requests zonder `client_id` gaan weigeren.
- **Controle op ingetrokken certificaten** — De eisen aan het controleren op ingetrokken certificaten zijn verruimd; CRL en OCSP Stapling behoren nu ook tot de mogelijkheden.

Verder zijn de volgende belangrijke veranderingen in het MedMij Afsprakenstelsel aangebracht.

- **Releasebeleid** — MedMij gaat een dakpansgewijs releasebeleid voeren, waarin steeds twee releases tegelijk actief zijn op het MedMij-netwerk: een verplichte en een al gepubliceerde opvolger daarvan. Operationele processen, testbeleid en het beleid inzake gecontroleerde livegangen zijn hierop aangepast.
- **Ruimte voor andere authenticatiemiddelen dan DigiD** — Het MedMij Afsprakenstelsel gaat meer verantwoordelijkheid bij de *Zorgaanbieder* neerleggen, maar dus ook meer ruimte aan de *Zorgaanbieder* geven, om andere authenticatiemiddelen dan enkel DigiD te gebruiken.
- **Coördinatie, regie en uitwisseling** — In de architectuur van het MedMij Afsprakenstelsel worden drie hoofdfuncties van elkaar onderscheiden — *Regie, Uitwisseling* en *Coördinatie* — die gezamenlijk al het gedrag op de Processen-en-Informatie- en op de Applicatie-laag omvatten. Aan deze scheiding

worden acht architectuurbeginselen verbonden, die richting geven aan de ontwikkeling van het MedMij Architectuur in de toekomst. Zo kunnen *Deelnemers* beter anticiperen op die ontwikkeling met de architectuurkeuzes in hun implementaties.

- **Twee-factor-authenticatie** — De eisen aan *Dienstverleners persoon* inzake twee-factor-authenticatie zijn geëxpliciteerd.

Changelog release 1.1

Changelog release 1.1 bevat de changelogs voor de (tussen)versies van release 1.1.

Changelog release 1.1.2

Release 1.1.2 omvat enkele veranderingen waarvoor *Dienstverleners persoon* en/of *Dienstverleners zorgaanbieder* hun oplossingen (zeker of eventueel) zullen moeten aanpassen om compatibel te blijven (backwards-incompatible changes). Het gaat allereerst om twee zekere wijzigingen voor *Dienstverleners zorgaanbieder*.

- De *Authorization Server* gaat controleren of een *Client* wel erkend is op de *Gegevensdienst* waarvoor hij een authorization request doet. Daartoe wordt de *OAuthclientlist* uitgebreid met, per *OAuthclient*, de *Gegevensdiensten* waarop deze erkend is. Het XML-schema van de *OAuthclientlist* wordt dus aangepast. Gedurende de beperkte invoeringsperiode zijn de huidige en de nieuwe *OAuthclientlist* beide beschikbaar. Deze wijziging gaat ook de mogelijkheid bieden voor zogenoemde gecontroleerde livegangen.
- In release 1.1.2 gaan *Authorization Servers* ook access token requests accepteren met een `client_id`. Indien aanwezig gaan zij die ook controleren. In release 1.1.1 was de `client_id` verplicht afwezig in de access token request. Deze stap is een voorbereiding op de uiteindelijke verplichtstelling, in een volgende release, van de `client_id` in de access token request.

Verder is er één eventuele backwards-incompatible wijziging voor *Dienstverleners persoon*.

- Ter bestrijding van de "open redirector" kwetsbaarheid wordt het verboden om URI's in de state-parameter op te nemen. *Dienstverleners persoon* die dat eventueel wel hadden gedaan zullen deze moeten verwijderen.

Daarnaast zijn er vijf backwards-incompatible wijzigingen, één zekere en vier eventuele, voor zowel *Dienstverleners persoon* als *Dienstverleners zorgaanbieder*.

- De interfaces voor het ophalen van de *Gegevensdienstnamenlijst*, *OAuthclientlist*, *Whitelist* en *Zorgaanbiederslijst* zullen geversioneerd worden. Hiermee wordt de invoering van wijzigingen in de XML-schema's van die lijsten vereenvoudigd, omdat tijdens migraties meerdere interfaces (en dus XML-schema's) naast elkaar in gebruik kunnen zijn. De bovenstaande wijziging inzake de *OAuthclientlist* geldt als eerste voorbeeld. Aan de bevraging van de lijsten zal een query-parameter met een releasenummer toegevoegd worden.
- De `state`-parameter is verplicht in de authorization request. Dat is in release 1.1.1 ook al zo, maar stond niet helder in de tekst verwoord. Omdat we ermee rekening houden dat daardoor de `state`-parameter niet overal is opgenomen, zien we het als een change. De kans is evenwel groot dat deze zeer beperkt tot geen aanpassingen gaat vragen.
- Als in de authorization request een ongeldige `redirect_uri` wordt meegegeven is dat niet alleen een fout, maar moet deze fout bovendien niet via die ongeldige `redirect_uri` worden teruggemeld, maar direct aan de eindgebruiker. Dit stond nog niet vermeld in release 1.1.1, maar is desondanks bij menige *Deelnemer* al wel zo geïmplementeerd. We verwachten ook hier daarom beperkte wijzigingen.
- In release 1.1.2 wordt voor alle `htpps`-verbindingen de daarvoor door IANA aangewezen poort (443) verplicht. In release 1.1.1 bestonden nog mogelijkheden om andere poortnummers te kiezen, ook bijvoorbeeld voor de endpointadressen in de *Zorgaanbiederslijst*, hoewel daarvan amper of geheel geen gebruik is gemaakt. Waar in release 1.1.2 in de *Zorgaanbiederslijst* nog poortnummers voorkomen, zal dat altijd het IANA-poortnummer zijn.
- In april van dit jaar heeft het NCSC een nieuwe versie van haar TLS-richtlijnen gepubliceerd. Het MedMij Afsprakenstelsel volgt deze. *Deelnemers* kunnen er nu voor kiezen ook TLS 1.3 te implementeren, maar alleen als ook TLS 1.2 nog wordt geboden. Tot zover is deze change backwards-compatible. Sommige TLS-algoritmen hebben in de nieuwe TLS-richtlijnen echter hun classificatie "goed" verloren. Mochten *Deelnemers* deze in gebruik hebben, moeten zij worden afgevoerd.

Verder zal release 1.1.2 een hoeveelheid veranderingen omvatten die geen aanpassingen vereisen van de oplossingen van *Dienstverleners persoon* en *Dienstverleners zorgaanbieder* (backwards-compatible changes). Het gaat om de volgende.

- Het gaat mogelijk worden dat een groep van (minstens één) *Dienstverleners persoon* en (minstens één) *Dienstverleners Zorgaanbieder* zich tijdelijk organiseren in een zogenoemde 'gecontroleerde livegang'. *Dienstverleners zorgaanbieder* betrekken een afgebakende groep *Zorgaanbieders*, hun klanten. *Dienstverleners persoon* kunnen naar keuze een afgebakende groep *Personen* daarbij organiseren. Elke gecontroleerde livegang gaat om één geldige *Gegevensdienst*, die in de *Catalogus* staat. In een gecontroleerde livegang kan het aanbieden van die *Gegevensdienst* door de genoemde *Zorgaanbieders* beproefd worden op het live MedMij-netwerk, gedurende een korte periode, zodanig dat alleen de deelnemende *Dienstverleners persoon* deze *Gegevensdienst* ook van deze *Zorgaanbieders* kunnen afnemen. Het doel is dat daarna de betreffende Zorgaanbieders volledig live gaan op die *Gegevensdienst*. Gecontroleerde livegangen worden mogelijk gemaakt zonder enige technische of functionele ingreep, maar enkel door een administratieve ingreep, namelijk door een tijdelijke administratieve kopie te maken van de betreffende *Gegevensdienst*.
- In release 1.1.2 wordt naast het SAML-koppelvlak ook het CGI-koppelvlak van DigiD toegestaan, onder de kanttekening dat voor DigiD het SAML-koppelvlak de toekomstvast keuze is.
- Op drie punten is de beschrijving van de flow aan het eind van *UCI Verzamelen* en *UCI Delen* verbeterd: het is mogelijk om onmiddellijk na ontvangst van een access token tot gebruikersinteractie over te gaan, na optreden van een uitzondering hoeft de herhaling niet onderbroken te worden en er kan sprake zijn van herhaalde resource requests in meer situaties dan oorspronkelijk vermeld.
- De ordening van de verantwoordelijkheden op de Applicatie-laag heeft een ingrijpend nieuwe opzet gekregen, langs de lijnen van interfaces. Dit verbetert het overzicht en opent de mogelijkheid voor versionering van interfaces in de toekomst. Tegelijkertijd zijn de adresseringsverantwoordelijkheden verhelderd.
- In het normenkader:
    - is het toetsingskader nu in de hoofdtekst opgenomen, in plaats van in bijgevoegde documenten. Dat geldt ook voor de aanvullende auditverklaring, die in de hoofdtekst gegenereerd kan worden;
    - zijn drie normen toegevoegd en hebben drie normen toevoegingen gekregen. Bestaande aanvullende auditverklaringen blijven echter van kracht;
    - zijn enkele normen (door opdeling of samenvoeging) herordend;
    - is de tekst van enkele normen verduidelijkt;
- De beschrijving van de (limitatief) toegestane informatie-inhoud van het access token is verbeterd. Toegelicht is bovendien dat, en waarom, OpenID Connect niet wordt toegepast op het koppelvlak van *UCI Verzamelen* en *UCI Delen*.
- Toegelicht is dat, en waarom, OCSP Stapling vooralsnog niet wordt toegepast.
- Toegelicht is wat met een "full" redirect_uri wordt bedoeld.
- Een keur aan kleinere tekstuele verbeteringen is doorgevoerd.

Release 1.1.2 wordt op 4 oktober 2019 gepubliceerd. Deelnemers worden geacht de op hen betrekking hebbende wijzigingen door te voeren, niet eerder dan na publicatie en niet later dan op 31 december 2019.

Dienstverleners Zorgaanbieder dragen zelf de verantwoordelijkheid om, wanneer zij eerder dan 31 december 2019 deelnemen aan een gecontroleerde livegang, tijdig de eerste hierboven genoemde wijziging te hebben doorgevoerd: controle van authorization request op basis van nieuwe *OAuthclientlist.* Zo lopen zijzelf en de andere partijen in die gecontroleerde livegang niet het risico onbedoelde *PGO Servers* toegang tot de (kopie-) *Gegevensdienst* van de gecontroleerde livegang te geven.

Changelog release 1.1.1

De belangrijkste wijzigingen in deze release zijn:

Architectuur en technische specificaties

- Opgenomen op de Netwerk-pagina dat de *Whitelist*-controle, onder bepaalde condities, ook na afronding van de TLS-handshake mag worden uitgevoerd.
- Pagina met toelichtingen afsprakenset release 1.1 verwerkt in hoofdtekst Architectuur en technische specificaties:
  - Applicatierollen en hun getalsverhoudingen;
  - Bedoeling van de beschikbaarheids- en de ontvankelijkheidstoets.
  - Eisen van DigiD inzake uitloggen.
  - G2- en G3-certificaten van PKIoverheid.
- Toelichting op betekenis start- en einddatum van een *Gegevensdienst* toegevoegd (Metamodel).
- Verschillende kleine aanpassingen doorgevoerd in het Metamodel:
  - Samenstelling van de gegevensdienstnaam nader gedefinieerd.
  - Attribuut 'Vervangt' toegevoegd aan klasse Gegevensdienst.
- Beschikbaarheid- en ontvankelijkheidstoets opnieuw geformuleerd als beschikbaarheids- en ontvankelijkheidsvoorwaarde. Moment van van kracht worden gerelativeerd: tussen een vroegste en laatste moment.
- Nieuwe element (OAuth scope) mogelijk gemaakt als inhoud van access token. Custom HTTP header `medmijscope:` verwijderd.

> **Structuurwijzigingen catalogus n.a.v. release 1.1.1**
>
> De *Catalogus* is geen onderdeel van de afsprakenset en kent haar eigen releasecyclus. Bovenstaande wijzigingen hebben echter wel op de volgende manier impact op de structuur van de *Catalogus*:
>
> - Patchnummers verwijderd uit *Gegevensdienstnaam* en *Systeemrolcodes*.
> - Kolom 'Vervangt' toegevoegd om opvolging van gegevensdiensten te kunnen aangeven.
>
> De wijzigingen zijn ondertussen doorgevoerd.

Normenkader informatiebeveiliging

Op basis van terugkoppeling uit eerste lopende audittrajecten is verduidelijking aangebracht in het normenkader:

- Eis aan het certificaat over de scope is geschrapt. De beoordeling van de MedMij scope wordt duidelijk uit de beoordeling van het normenkader.
- Toegevoegd dat verwacht wordt dat dezelfde eisen gesteld worden aan de uitvoerend auditor door de CBI als voor de afgifte van het NEN 7510 certificaat.
- In Beoordelingskader verduidelijking aangebracht in de auditmethode op diverse normen. Op basis hiervan zijn tevens enkele normen tekstueel verduidelijkt.
- Norm A.12.3.1 Back-up van informatie: toegevoegd dat deze ook voor de *Dienstverleners zorgaanbieder* geldt.
- Norm A.9.4.1 Beperking toegang tot informatie: aangegeven dat deze alleen voor de *Dienstverlener persoon* geldt.
- Rapportageformat auditverklaring: versie afsprakenstelsel aangepast.

Beleid

- Gegevensdienstenbeleid: tekst onder kopje 'Mutaties van gegevensdiensten' aangepast.
- OAuthclient-namenbeleid: eis "dat de naam in het verleden niet door een andere *Dienstverlener persoon* gebruikt mag zijn" verwijderd.
- Verwijzing naar uitvoeringsorganisatie consequent vervangen naar Stichting MedMij. Onderscheid is voor het afsprakenstelsel niet relevant.

Communicatie

- Toestemmings- en bevestigingsscherm: verduidelijkt dat de HTML- en CSS-bestanden enkel de tekst en vormgeving beschrijven. De *Dienstverlener zorgaanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina.

Changelog release 1.1 versie 1.0

De versie van release 1.1 zoals vastgesteld door bestuur en eigenaarsraad van Stichting MedMij. De wijzigingen ten opzichte van versie 0.9 zijn:

- Normenkader informatiebeveiliging: rapportageformat en beoordelingskader normenkader toegevoegd.
- Toelichting AVG-normen: links naar formats gegevensbeschermingseffectbeoordelingen toegevoegd.
- Pagina known issues niet meer opgenomen: in overleg met de governancestructuur MedMij Afsprakenstelsel wordt prioriteitstelling bepaald.

Changelog release 1.1 versie 0.9

> **Afsprakenset versus afsprakenstelsel**
>
> Met ingang van deze versie is een duidelijker onderscheid gemaakt tussen de verschillende onderdelen van het afsprakenstelsel. Het totaaloverzicht is te vinden bij de Introductie op het afsprakenstelsel. Deze changelog behandelt enkel de wijzigingen in de afsprakens*et*. Wijzigingen in de overige onderdelen van het stelsel, zoals de deelnemersovereenkomsten en de catalogus, vinden niet releasematig plaats en zijn daarmee geen onderdeel meer van de changelog.

De belangrijkste wijzigingen in deze versie zijn:

Grondslagen

- Definitie van Zorgaanbieder aangescherpt.
- Principe toegevoegd: "Aan de persoonlijke gezondheidsomgeving zelf worden eisen gesteld." (ter vervanging van Principe 8)
- Principe toegevoegd: "Afspraken worden aantoonbaar nageleefd en gehandhaafd."
- Principe toegevoegd: "Het afsprakenstelsel snijdt het gebruik van normen en standaarden op eigen maat."

Juridische context

- De juridische context bestaat nu uit diverse toelichting op de juridische context van handelen door deelnemers aan het MedMij Afsprakenstelsel. Op de beginpagina is beschreven waar die toelichting, en daarmee met name advisering en ondersteuning aan deelnemers, uit bestaat.
- Er is een pagina toegevoegd met verantwoordelijkheden en normen vanuit de AVG. Deelnemers hierin ondersteund met informatie over verplichtingen die zij zelfstandig dienen te implementeren conform deze wetgeving en waarvan MedMij het belangrijk vindt dat deelnemers deze kennen. Dit was tevens een aanbeveling in de uitgevoerde PIA.
- In het juridisch kader zijn beschrijvingen van wet- en regelgeving geüpdatet. Tevens zijn bevindingen uit de PIA verwerkt, met name tekstueel.

Deelnemersovereenkomsten

- De onderwerpen waar de overeenkomst op toeziet zijn geüpdatet naar aanleiding van de laatste wijzigingen in deze release.
- Artikelen onder 5 met betrekking tot doel van de gegevensverwerking zijn aangepast naar de scope van het MedMij Afsprakenstelsel.
- De overeenkomst is meer wederkerig gemaakt tussen deelnemers en de stichting.
- Enkele definities zijn aangescherpt.
- Verwerking van aanbevelingen vanuit een uitgevoerde PIA, met name tekstueel.

Model verwerkersovereenkomst

- Eis verscherpt dat verwerking van data in de EU en conform EU wetgeving moet plaatsvinden door verwerkers in artikel 3.10 en 6.2.

Architectuur en technische specificaties

Laagoverstijgend

- Verduidelijkt dat een hostname altijd een fully qualified domain name is en dat wildcards niet zijn toegestaan op de whitelist.

Applicatie

- Verplicht gebruik GET-methode bij authorization request toegevoegd.
- Gebruik UUID vervangen door generieke eisen aan de tokens. (UUID mag niet meer gebruikt worden als enkel ID van het token.)
- Verplicht gebruik Authorization Request Header Field toegevoegd.
- Maximale duur gebruik lijsten voorgeschreven in situatie dat MedMij Registratie onbereikbaar is.
- Technische adressering MedMij Registratie toegevoegd.
- Toelichting op relatie tussen Authorization Server en Resource Server verduidelijkt.
- Verantwoordelijkheid voor afwezigheid van BSN's in de content van gegevensdiensten verwijderd.
- AuthorizationEndpoint hoeft niet meer aan één Zorgaanbieder gekoppeld te zijn. Zorgaanbiedernaam en Gegevensdienst moeten worden meegegeven in de scope-parameter van het OAuth-request.
- ResourceEndpoint hoeft niet meer aan één zorgaanbieder gekoppeld te zijn. De Zorgaanbiedernaam en Gegevensdienst moeten worden meegegeven in een custom-HTTP-header.

Netwerk

- ZA Node gekoppeld aan één deelnemer.

Informatiemodellen

- Informatiemodellen opnieuw geordend.
  - Scheiding aangebracht tussen conceptueel model en logische modellen. Logische modellen geïntroduceerd.
  - Relatie tussen conceptueel model en logische modellen enerzijds en XML-schema's anderzijds aangescherpt (resulterend in enkele wijzigingen in de schema's en de toelichting erop).
- Diverse modelmatige verbeteringen, waarvan de belangrijkste zijn:
  - Stringtypes vervangen door basisklassen.
  - Transactie vervangen door Systeemrol als primaire component van Transactieverzameling.
  - Gegevensdienst gekoppeld aan één use case.
  - Informatiestandaard toegevoegd.
  - Geldigheidsperiode aan Gegevensdienst toegevoegd.
  - Identificerende naam van gebruiksvriendelijke naam voor Gegevensdienst onderscheiden.
  - Afhankelijkheid tussen Gegevensdiensten mogelijk gemaakt.

Normenkader informatiebeveiliging

- Op basis van een consultatie met auditors op versie 0.8 zijn enkele normen verder verduidelijkt of voorzien van een link naar ondersteunende documentatie.
- De toelichting is verplaatst naar het privacy- en informatiebeveiligingsbeleid.

Beleid

- Dienstverleningsoverdrachtsbeleid toegevoegd.
- Beschrijving van de mogelijke mutaties van gegevensdiensten toegevoegd in het Gegevensdienstenbeleid.
- Informatieclassificatiebeleid toegevoegd.
- Performancebeleid toegevoegd.
- Beschrijving van de jaarlijkse stelselbrede risico-analyse onder privacy- en informatiebeveiligingsbeleid toegevoegd.
- Change en releasebeleid aangescherpt.
- Gegevensdienstenbeleid aangescherpt.
- Kwalificatie- en acceptatiebeleid vervangen door testbeleid.
- In OAuthclient-namenbeleid opgenomen dat OAuthclient-naam gelijk moet zijn aan een handelsnaam van de Dienstverlener persoon in het handelsregister.

- Aan het privacy- en informatiebeveiligingsbeleid is een pagina toegevoegd met achtergrond over de risicoanalyse die mede bepalend is voor diverse maatregelen op het gebied van informatiebeveiliging in het MedMij Afsprakenstelsel, zoals in de architectuur en technische specificaties of het aanvullend normenkader.

Operationele processen

- Proces erkenning als aanbieder van gegevensdienst toegevoegd.
- Proces beheren technische kwetsbaarheden toegevoegd.

Communicatie

- Paragraaf 'Uitingsvormen van het merk' gewijzigd.

Managementinformatie

- Afspraak over aanleveren managementinformatie over performance resource server door Dienstverlener zorgaanbieder verwijderd.

Changelog release 1.1 versie 0.8

De belangrijkste wijzigingen in deze versie zijn:

Grondslagen

- Aangepast: Doelstelling 7 verfijnd.
- Toegevoegd: Principes "Uitwisseling is een keuze", "Het MedMij-netwerk is gebruiksrechten-neutraal" en "De burger regisseert zijn eigen gezondheidsinformatie als uitgever".
- Toegevoegd: Deelnemers behandelen elkaar onderling gelijk (bij principes).
- Toegevoegd: Vrij verkeer over het MedMij-netwerk (deelnemers brengen elkaar geen kosten in rekening) (bij principes).

Juridisch kader

- Toegevoegd: Wet gelijke behandeling op grond van handicap en chronische ziekte (wgbh/cz) toegevoegd als belangrijk kader voor leveranciers om toegankelijke toepassingen te realiseren.
- Toegevoegd: Verdere verduidelijking zienswijze van MedMij op de verwerkingsverantwoordelijkheden in het stelsel als toelichting op de AVG, evenals een aparte pagina bij het juridisch kader.
- Toegevoegd: Aanvullingen op de toelichting inzake de AVG en WGBO bezien vanuit de nieuwe UC Delen.

Overeenkomsten en rechtsrelaties

- Gewijzigd: Bètaovereenkomsten gelden niet meer, er zijn Deelnemersovereenkomsten voor productiesituatie teruggekomen.
- Toegevoegd: In de Deelnemersovereenkomsten: een bepaling over de operationele processen en samenwerkingsafspraken en een bepaling over het niet rekenen van onderlinge vergoedingen voor gegevensuitwisseling.
- Toegevoegd: Zelfverklaring integriteit.
- Toegevoegd: In de Modelverwerkersovereenkomst is rekening gehouden met de verwerkingsverantwoordelijkheden die voortkomen uit UC Delen.

Architectuur en technische specificaties

Correctie

- Aangepast: De positie van 'controleer beschikbaarheid' in de UC en UCI Verzamelen in lijn gebracht met de tekst.

Doorontwikkeling

- Aangepast: Catalogus losgekoppeld van afsprakenset en verwijzing opgenomen.
- Aangepast: De stelselnode wordt niet opgenomen op de whitelist.
- Aangepast: Altijd 'goede' (volgens NCSC) TLS-versies en -algoritmen voor front-channelverkeer vereist.
- Aangepast: Verwijzing naar NEN7513:2018 (specifieke versie) ingevoegd, en verantwoordelijkheid over logging aangepast zodat de positie van NEN7513 duidelijker is
- Toegevoegd: Gegevensdienstnamenlijst (use case, use case-implementatie, relatie met overige use cases).
- Toegevoegd: Service levels van MedMij Registratie, de Authorization Server en de Resource Server.
- Toegevoegd: Verantwoordelijkheid om gebruik te maken van DNSSEC.
- Toegevoegd: Verantwoordelijkheid om voldoende onvoorspelbaarheid van UUID's te waarborgen.
- Toegevoegd: Verantwoordelijkheid dat als OCSP-responder onbereikbaar is, TLS-sessie niet tot stand komt.

- Toegevoegd: Use case en use case-implementatie Delen.
- Toegevoegd: De 'scheme' bij adressering moet altijd uit kleine letters bestaan.
- Toegevoegd: Verantwoordelijkheid voor beheerorganisatie om historie van lijsten te bewaren.
- Toegevoegd: Aantekenen Bron en Gegevensdienst door Uitgever bij verzamelde gegevens.
- Toegevoegd: Eisen aan de syntax van de hostname.
- Toegevoegd: Uitzonderingssituatie: na authenticatie constateert dienstverlener zorgaanbieder dat persoon jonger is dan 16 jaar.
- Toegevoegd: Verantwoordelijkheid voor deelnemers om elkaar onderling gelijk te behandelen.

Verduidelijking

- Aangepast: Beschrijving van de wijze waarop de whitelistcontrole plaats moet vinden bij inkomend en uitgaand verkeer.
- Aangepast: Netwerk-laag is opnieuw beschreven. Relatie tussen Netwerk en Applicatie-laag is opnieuw vormgegeven.
- Aangepast: De te nemen beveiligingsmaatregelen uit RFC6819 zijn toegankelijk en specifiek vermeld.
- Aangepast: Rol PGO User Agent is gesplitst in PGO User Agent en PGO Presenter.
- Toegevoegd: Verantwoordelijkheid om nog korte tijd bereikbaar te zijn na uitfasering van de ZorgaanbiederGegevensdienst in de ZAL.
- Toegevoegd: Eis van betekenisloosheid van tokens in het MedMij-netwerk.
- Toegevoegd: Hanteren two-way TLS-handshake voor back-channelverkeer.
- Toegevoegd: Verantwoordelijkheid voor beheerorganisatie om geen verlopen entries in ZAL te publiceren.
- Toegevoegd: Hostname mag voorkomen als CN of als SAN.

XML-schema's

- Aangepast: Modellering van het complexType MedMijNode in lijn gebracht met het metamodel.
- Toegevoegd: Gegevensdienstnamenlijst (XSD en XML-voorbeeldbestand).
- Toegevoegd: Eisen aan de XML-lijsten.

Normenkader informatiebeveiliging

- Gewijzigd: bij alle normen een rationale toegevoegd en de weging voor de auditor verwijderd.
- Gewijzigd: op basis van een hernieuwde risicoanalyse op het stelsel en een consultatie met auditors zijn normen verduidelijkt, toegevoegd of verwijderd.

Governance

Beleid

- Gewijzigd: positie beleid verduidelijkt op pagina Beleid.
- Gewijzigd: Zorgaanbiedersnamenbeleid aangescherpt.
- Gewijzigd: Toezicht- en handhavingsbeleid aangepast naar Nalevingsbeleid en nader uitgewerkt.
- Gewijzigd: Privacy- en informatiebeveiligingsbeleid aangescherpt.
- Gewijzigd: Toetredingsbeleid uitgebreid.
- Gewijzigd: Klachten- en geschillenbeleid nader uitwerkt.
- Toegevoegd: OAuthclient-namenbeleid toegevoegd.
- Toegevoegd: Samenwerkings- en escalatiebeleid.
- Toegevoegd: Gegevensdienstenbeleid.
- Toegevoegd: Kwalificatie- en acceptatiebeleid.

Operationele processen

- Gewijzigd: Operationele processen uitgebreid en nader uitwerkt.

Communicatie

- Gewijzigd: Uitgangspunten Merkgebruik nader uitgewerkt.
- Gewijzigd: Toestemmingsverklaring verbeterd en in lijn gebracht met de architectuur.
- Gewijzigd: Gebruikersvoorlichting losgekoppeld van afsprakenset en verwijzing opgenomen.
- Toegevoegd: Bevestigingsverklaring voor gebruik in UC Delen.

Managementinformatie

- Toegevoegd: Beschrijving van de managementinformatie die periodiek door de deelnemer moet worden aangeleverd.

Changelog release 1.0

Changelog release 1.0 bevat de changelogs voor de (tussen)versies van release 1.0.

Changelog release 1.0 versie 1.0

Release 1.0 versie 0.991 vastgesteld door bestuur en eigenaarsraad Stichting MedMij. Geen inhoudelijke wijzigingen.

Changelog release 1.0 versie 0.991

De belangrijkste wijzigingen in deze versie zijn:

Architectuur en technische specificaties

- Gewijzigd: uitzondering 2, 3 en 4 in de UC en UCI Verzamelen leiden nu tot dezelfde terugkoppeling naar de PGO Server. Daarmee kan de PGO Server niet langer afleiden of er mogelijk een behandelrelatie bestaat tussen de zorgaanbieder en de persoon, voordat de persoon toestemming heeft gegeven om gegevens te delen met de PGO Server.
- Gewijzigd: de terugkoppeling in uitzondering 1 in de UC en UCI Verzamelen vindt plaats naar de PGO Server en niet naar de Zorggebruiker; hiermee wordt aangesloten bij de OAuth-specificaties.
- Toegevoegd: in de toelichting is opgenomen dat de in de UC en UCI's benoemde uitzonderingen in de autorisatieflow aanvullend of verdiepend zijn ten opzichte van de OAuth-specificaties; daarin benoemde uitzonderingssituaties moeten conform de standaard geïmplementeerd worden.

XML-schema's

- Toegevoegd: XML-voorbeeldbestanden.
- Toegevoegd: ontwerpafwegingen.
- Verwijderd/gewijzigd: basisschema. De relevante elementen zijn nu opgenomen in de afzonderlijke XSD's van de lijsten.
- Gewijzigd: pattern HostnameType.
- Toegevoegd: patterns op BackchanneluriType en FrontchanneluriType.
- Toegevoegd: verplichte aanduiding tijdzone bij tijdstempel.
- Gewijzigd: opbouw van de namespace-URI.
- Gewijzigd: een van de elementen "Systeemrol" hernoemd naar "Systeemrolcode".
- Toegevoegd: controle op uniciteit van sleutelelementen.
- Gewijzigd: release- en versienummering.

Normenkader

- Gewijzigd: certificeringseisen NEN 7510 aangescherpt. Alleen Conformiteit Beoordelende Instellingen die NEN 7510 geaccrediteerd zijn door de Raad voor Accreditatie of een NEN 7510 licentieovereenkomst hebben met NEN mogen de certificering afgeven.

Changelog release 1.0 versie 0.99

De belangrijkste wijzigingen in deze versie zijn:

Architectuur en technische specificaties

- Toegevoegd: XML-producten voor de Zorgaanbiederslijst, de whitelist en de OAuth Client List.
- Toegevoegd: nadere afspraken over de technische adressering van endpoints en de opbouw van OAuth-URI's.
- Gewijzigd: uitbreiding en verbetering van het metamodel en de bijbehorende invarianten en stringtypes.
- Gewijzigd: relatie tussen de componenten op de applicatielaag enerzijds en de netwerklaag anderzijds.
- Gewijzigd: term "gateway" vervangen door de afzonderlijke componenten op de applicatielaag.
- Toegevoegd: afspraken over logging.
- Gewijzigd: whitelist is gesplitst in een whitelist en een OAuth Client List.
- Gewijzigd: frequentie van het ophalen van de ZAL, OAuth Client List en whitelist verhoogd.

Governance

- Gewijzigd: eisen waaraan zorgaanbiedersnamen moeten voldoen.
- Verwijderd: proces opvragen en consolideren logging.

Communicatie

- Gewijzigd: accessibility toestemmingsverklaring bètaversiefase verbeterd.

Changelog release 1.0 versie 0.9

De belangrijkste wijzigingen in deze versie zijn:

Grondslagen

- Gewijzigd: de tekst rond de optie van centrale voorzieningen om barrières te overwinnen is verduidelijkt en uitgebreid zodat het ook de keuze voor decentrale voorzieningen voor de aansluiting van zorgaanbieders op het MedMij-netwerk omvat.
- Gewijzigd: de begrippenlijst is ingekort en beschrijft nu enkel de belangrijkste begrippen die relevant zijn voor de grondslagen.

Juridisch kader

- Toegevoegd: data van publicatie van toegepaste wetsartikelen.
- Gewijzigd: wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg is opgenomen in de Wet gebruik burgerservicenummer in de zorg (Wet BSN-z). Toelichting op beide wetten in het juridisch kader zijn daarom samengenomen en de Wet BSN-z heeft een nieuwe titel gekregen, namelijk de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz).
- Gewijzigd: beschrijving van de relatie met de AVG is aangepast.

Overeenkomsten

- Gewijzigd: nieuwe introductie op de overeenkomstenstructuur met een toelichting op de verschillende rechtsrelaties.
- Toegevoegd: in deelnemersovereenkomsten en verwerkersovereenkomst opgenomen dat alleen gegevens over personen ouder dan 16 jaar worden verstrekt.
- Toegevoegd: artikel met afspraken rond uittreding van een deelnemer (7.5).
- Gewijzigd: uitbreiding artikelen met betrekking tot het intellectueel eigendom (11).
- Toegevoegd: de verplichting om minimaal één gegevensdienst aan te bieden.

Architectuur en technische specificaties

- Gewijzigd: beperking van de Juridica-laag tot alleen de rollen.
- Gewijzigd: restyling en detaillering van de totaalplaat en de platen per laag.
- Gewijzigd: detaillering op vele aspecten op alle lagen.
- Toegevoegd: grondige uitbreiding van de toelichtingen op de keuzes.
- Gewijzigd: strakkere ordening van het setje use cases en use case-implementaties.
- Toegevoegd: mitigatie van beveiligingsrisico's van het OAuth-protocol.
- Toegevoegd: eerste versie van een (logisch) metamodel.
- Toegevoegd: werken met PKIoverheid-servercertificaten voor versleuteling en authenticatie van gateways.
- Gewijzigd: opzet van de gegevenscatalogus.
- Toegevoegd: enkele gegevensdiensten.
- Verwijderd: use cases rond registratie (vervangen door operationele processen).
- Gewijzigd: OCSP in plaats van CRL voor controle geldigheid certificaten.

Normenkader informatiebeveiliging

- Toegevoegd: beschrijving van manier van toetsing van de normen.
- Gewijzigd: introductie op de opzet en bedoeling van het normenkader.

Governance

- Gewijzigd: inrichting Stichting MedMij.

- Gewijzigd: beleid op de volgende onderwerpen:
  - Toetreding: op termijn beschrijvingen verwijderd;
  - Klachten en geschillen: op termijn beschrijvingen verwijderd;
  - Change en release: passend gemaakt bij inrichting Stichting MedMij en aanduiding releases veranderd.
- Toegevoegd: zorgaanbiedersnamenbeleid.
- Verwijderd: op termijn beschrijving van inrichting governance.
- Toegevoegd: overzicht van de operationele processen waarbij deelnemers een rol spelen.

Communicatie

- Toegevoegd: aangepast scherm voor de verkorte toestemmingsverklaring.

Changelog release 1.0 versie 0.8

De belangrijkste wijzigingen in deze versie zijn:

Grondslagen

- Gewijzigd: onderscheid gemaakt in gegevensdienstonafhankelijke en gegevensdienstafhankelijke afspraken.
- Verwijderd: de beschrijving van de interacties op hoofdlijnen rond het verkrijgen van nieuwe gegevens zodra deze bij de zorgaanbieder beschikbaar komen. Dit laat ruimte om dit in latere releases goed uit te werken.

Juridisch kader

- Toegevoegd: bij de toepassing van de AVG informatie over dataportabiliteit toegevoegd.
- Toegevoegd: bij de toepassing van de wet Gebruik Burgerservicenummer in de Zorg tekst toegevoegd. Vanaf: "In het geval ...".
- Toegevoegd: aanpassingswet richtlijn inzake elektronische handel opgenomen.
- Toegevoegd: implementatiewet richtlijn consumentenrechten opgenomen.
- Toegevoegd: aansprakelijkheid wederom opgenomen. Dit dient nog verder uitgewerkt te worden.

Overeenkomsten

- Gewijzigd: specifieke deelnemersovereenkomsten opgenomen voor de bètaversiefase (bètaversieovereenkomsten).
- Toegevoegd: toestemmingsverklaring bètafase opgenomen.
- Toegevoegd: modelverwerkersovereenkomst zorgaanbieder - dienstverlener zorgaanbieder MedMij opgenomen.
- Gewijzigd: tekst bij de pagina Overeenkomsten is herschreven. De basis hiervoor stond eerst op de pagina Juridica.

Architectuur en technische specificaties

- Gewijzigd: architectuurplaten. In een matrixmodel zijn de rollen, processen en informatie in de verschillende lagen met elkaar in verbinding gebracht.
- Gewijzigd: teksten omgezet naar de vorm: rolbeschrijvingen en verantwoordelijkheden (afspraken met toelichtingen).
- Gewijzigd: solutions als bijlagen opgenomen in de vorm van usecases.
- Gewijzigd: use cases herschreven naar een nieuw format: flow, beschrijving processtappen, specificatie informatie en soms voorbeelden ter toelichting:
    - UC Registreren;
    - UC Opvragen zorgaanbiederslijst;
    - UC Verzamelen;
- Toegevoegd: afspraken over logging;
- Toegevoegd: model en eerste vulling van de gegevenscatalogus;
- Toegevoegd: use case implementaties bij de use cases op de laag Applicatie.

Normenkader informatiebeveiliging

- Toegevoegd: normenkader met overzicht van informatiebeveiligingsmaatregelen.

Governance

- Toegevoegd: inrichting van de governance uitgewerkt. Hierbij is onderscheid gemaakt tussen een inrichting voor de bètaversiefase en een inrichting op termijn.

- Toegevoegd: het beleid is uitgewerkt op de volgende onderwerpen:
  - Toetreding;
  - Toezicht en handhaving;
  - Klachten en geschillen;
  - Change en release;
  - Privacy en veiligheid;
  - Intellectueel eigendom.

Communicatie

- Toegevoegd: communicatiehandboek met daarin afspraken over de manier waarop het merk MedMij mag worden gehanteerd.
- Gewijzigd: de gebruikersvoorlichting is aangepast en verplaatst naar communicatie. Bij zowel de Gebruikersvoorlichting persoon als de Gebruikersvoorlichting zorgaanbieder is een stuk tekst opgenomen omtrent de bètaversiefase.
- Gewijzigd: bij de Gebruikersvoorlichting persoon is tevens een stuk tekst opgenomen omtrent algemene rechten, zoals het recht op rectificatie en het recht op vergetelheid.

Changelog release 1.0 versie 0.3

Versie 0.3 van het Afsprakenstelsel MedMij is de eerstvolgende versie voor publicatie buiten het programma MedMij na versie 0.1. De 0.2 versie diende voor interne doeleinden. De 0.3 versie is een tussenversie op weg naar een 0.9 versie. De publicatie van deze 0.3 versie is bedoeld om een terugkoppeling te geven over de verwerking van de marktconsultatie op de 0.1 versie, onder begeleiding van Nederland ICT en OIZ. Het is tevens bedoeld als input voor een proof of concept (POC) fase in samenwerking met Zorgverzekeraars Nederland en het programma gespecificeerde toestemming (GTS). In deze POC worden de beschreven usecases verder uitgewerkt en getoetst waarbij ook gekeken wordt naar de toepassing van enkele centrale voorzieningen die nodig zijn in de werking van het afsprakenstelsel en GTS. Middels deze activiteiten wordt het afsprakenstelsel verder doorontwikkeld. Tussenresultaten worden voortdurend teruggekoppeld via de werkgroepenstructuur van het programma MedMij. Via die weg kunnen diverse belanghebbenden bij het afsprakenstelsel dan ook hun reactie geven op deze documentatie. Verder dient deze versie als startdocument voor een uit te voeren risicoanalyse naar informatiebeveiliging op basis waarvan het normenkader beveiliging voor het afsprakenstelsel ontwikkeld kan worden.

Wijzigingen of aanvullingen in de uitgangspunten

- De definitie van het ‘Minimum Viable Product’ waarmee het afsprakenstelsel in de bètaversiefase live gaat (versie 1.0) is op hoofdlijnen beschreven.
- Het centrale kenmerk van het afsprakenstelsel – “decentrale operatie, centraal vertrouwen” – is beschreven.

Wijzigingen of aanvullingen in de overeenkomsten

- Deelnemersovereenkomsten zijn samengevoegd tot één overeenkomst om de leesbaarheid van het geheel te vergroten. Artikel 3 is voor de verschillende rollen specifiek. Deelnemers krijgen wel een eigenstandige overeenkomst voor de rol waarin zij deelnemen ter ondertekening.
- Deelnemer is gebonden aan Nederlands recht (artikel 3, lid 2 dienstverlener persoon; artikel 3 lid 2 dienstverlener zorgaanbieder)
- Vereisten omtrent screening van personeel (artikel 3, lid 3 dienstverlener persoon; artikel 3 lid 3 dienstverlener zorgaanbieder)
- Vereisten rondom verplichtende kader model bewerkersovereenkomst (artikel 3, lid 10 dienstverlener persoon; artikel 3 lid 11 dienstverlener zorgaanbieder)
- Aanspreekbaarheid van de deelnemer voor de gebruiker vastgelegd (artikel 3, lid 11 dienstverlener persoon; artikel 3 lid 12 dienstverlener zorgaanbieder)
- Vereisten rondom het verlenen van medewerking om tot oplossingen te komen bij netwerkfalen (artikel 5, lid 2)
- Verwijzing naar het operationeel handboek opgenomen omtrent het handelen bij incidenten, calamiteiten en crisissituaties (artikel 6, lid 3)
- Verwijzing naar de Algemene verordening gegevensbescherming; was voorheen Wet bescherming persoonsgegevens (artikel 7, lid 1)
- Vereisten rondom toestemming voor alle partijen vastgelegd in de deelnemersovereenkomst (artikel 7, lid 3 en 4)
- Vereisten rondom logging vastgelegd in de deelnemersovereenkomst (artikel 7, lid 9)
- Gebruiksrecht MedMij zoals omschreven in de overeenkomst; was conform artikel 7, lid 2 (artikel 9, lid 3)
- Toevoeging artikel 10, lid 2
- Toevoeging verwijzing naar het proces uittreden in het operationeel handboek (artikel 11, lid 3)
- Vereisten rondom In het geval de deelnemer van juridische status verandert (artikel 15, lid 4)

Wijzigingen of aanvullingen in het juridisch kader

- Relevante elementen uit de EGIZ opgenomen

- Bewerkers/verantwoordelijke-relatie tussen dienstverlener zorgaanbieder en de zorgaanbieder nader uitgewerkt
- Wbp termen vervangen voor de AVG termen.
- Verwijzingen naar verschillende relevante AVG documentatie opgenomen.
- Verwijzingen naar gebruikersovereenkomst vervangen door gebruikersvoorlichting.
- Wet kwaliteit, klachten en geschillen zorg verwijdert uit het juridisch kader.
- Verordening (EU) 2017/745 van het Europees parlement en de Raad betreffende medische hulpmiddelen opgenomen in het juridisch kader.

Wijzigingen of aanvullingen in de functionele weergave

- Nadere specificatie functionele use cases (opzoeken zorgaanbieder in het zorgaanbiedersregister, vinden/abonneren op informatie, notificeren, authenticatie, haal gegevens op uit xIS).

Wijzigingen of aanvullingen in de technische weergave

- Nadere uitwerking technisch architectuur gezichtspunt.
- Specificatie van een generiek Medmij Gateway prototype.
- Specificatie van een Medmij gateway voor het LSP, met tevens:
    - Mappings voor uitwisseling van medicatie informatie tussen HL7v3 en Medmij/FHIR voor uitwisseling met het LSP.
    - Specificatie van integratie met het LSP.
    - Specificatie van de Medmij FHIR API.
    - Specificatie infrastructuurmodel.
    - Specificatie van abonnementen en notificatie.
    - Specificatie van de authenticatie van de persoon door de zorgaanbieder.
    - Specificaties Testomgeving met hierop werkende demonstraties

Wijzigingen of aanvullingen in het onderwerp governance

- Nieuwe documentatie over rollen, verantwoordelijkheden, inrichting en beleid
- Eerste uitwerking van de inrichting van de MedMij-beheerorganisatie op zowel korte als lange termijn

Grondslagen

De grondslagen beschrijven het fundament waarop de uitwerking van de afspraken in het afsprakenstelsel is gebaseerd.

Allereerst worden de omgeving van en de 'opdracht' aan het afsprakenstelsel geschetst. De Achtergrond beschrijft de achtergrond en de probleemstelling van het afsprakenstelsel, evenals de keuze voor een vrijwillig en decentraal afsprakenstelsel met dienstverleners. De Criteria expliciteren waaraan het afsprakenstelsel moet voldoen (randvoorwaarden) en op grond van welke factoren het succes van het afsprakenstelsel wordt afgemeten (doelen).

Vervolgens worden de belangrijkste ontwerpkeuzes benoemd, waarmee het afsprakenstelsel invulling geeft aan de opdracht. De Principes geven een overzicht van de richtinggevende ontwerpkeuzes. De Opzet van het afsprakenstelsel geeft aan hoe dit zich doorvertaalt in de werking van de gegevensuitwisseling en doet dat aan de hand van een overzicht van de betrokken rollen, hun verantwoordelijkheid en de interacties tussen de rollen.

Tot slot geeft de Begrippenlijst de formele definities van begrippen die in de uitwerking van het afsprakenstelsel worden gebruikt.

Achtergrond

Steeds meer mensen willen inzicht in hun gezondheid. MedMij zorgt ervoor dat iedereen die dat wil kan beschikken over zijn gezondheidsgegevens in een zelfgekozen persoonlijke gezondheidsomgeving. Bijvoorbeeld in een app of een website. Daarvoor moet zo'n app of site veilig kunnen communiceren met alle plekken waar de informatie opgeslagen staat. Denk aan ziekenhuis, de huisarts, het consultatiebureau en de apotheek. MedMij is dé Nederlandse standaard voor het veilig en betrouwbaar uitwisselen van gezondheidsgegevens tussen jou en gezondheidsprofessionals.

De persoonlijke gezondheidsomgeving

MedMij hanteert de volgende definitie van een persoonlijke gezondheidsomgeving (PGO), zoals deze oorspronkelijk door de Patiëntenfederatie Nederland is geformuleerd:

> *Een persoonlijk gezondheidsdossier (PGD):*
>
> - *Is een universeel toegankelijk, voor leken begrijpelijk, gebruiksvriendelijk en levenslang hulpmiddel om relevante gezondheidsinformatie te verzamelen, te beheren en te delen, en om regie te kunnen nemen over gezondheid en zorg en om zelfmanagement te ondersteunen via gestandaardiseerde gegevensverzamelingen voor gezondheidsinformatie en geïntegreerde digitale zorgdiensten.*
> - *Wordt beheerd en/of gedeeld door de patiënt of zijn wettelijke vertegenwoordiger.*
> - *Is op zo danige wijze beveiligd dat de vertrouwelijkheid van gezondheidsgegevens en de privacy van de gebruiker worden beschermd.*
> - *Is geen wettelijk medisch dossier, tenzij aldus gedefinieerd en daarom onderworpen aan wettelijke beperkingen.*
>
> *Bron: Bierma, L. & Heldoorn, M. (2013),* Het persoonlijk gezondheidsdossier - De visie van patiëntenfederatie NPCF*.*

Een persoonlijke gezondheidsomgeving is daarmee een digitale omgeving die je in staat stelt om al je relevante gezondheidsgegevens, die verspreid staan opgeslagen bij professionals, zorginstellingen en overheden, overzichtelijk en veilig in te zien, aan te vullen met eigen metingen en te delen met wie je dat wilt. Inhoudelijke functionaliteiten, bijvoorbeeld in de vorm van digitale zorgdiensten, zijn optioneel en zullen per individu verschillen op basis van persoonlijke behoefte en situatie. Een persoon moet daarbij kunnen kiezen voor één persoonlijke gezondheidsomgeving en niet gedwongen worden meerdere omgevingen bij te houden.

Leveranciers van PGO's maken gebruik van informatie uit achterliggende systemen van aanbieders en kunnen via hun persoonlijke gezondheidsomgeving waarde toevoegen aan die gegevens met behulp van digitale zorgdiensten. Ook zullen er aanbieders van losse functionaliteiten zijn, zoals van mobiele apps die bijvoorbeeld medicatie reminders geven, die via het MedMij Afsprakenstelsel gegevens kunnen uitwisselen.

Grip op je eigen gezondheidsgegevens en toegang tot eHealth toepassingen stellen je in staat op je zelfgekozen manier aan je eigen gezondheid te werken en je zorgproces te laten ondersteunen.

Huidige situatie

Het aanbod en gebruik van PGO's komt voorzichtig op gang. De afgelopen jaren is gewerkt aan invulling van de randvoorwaarden voor veilige gegevensuitwisseling met tussen aanbieders en gebruikers van een persoonlijke gezondheidsomgeving.. Voor een groot deel vult het MedMij Afsprakenstelsel deze randvoorwaarden in. Denk hierbij aan veiligheidseisen, eisen aan sets van informatie (gegevensdiensten) die uitgewisseld mag worden en checks op wettelijke kaders. Door VWS zijn middelen beschikbaar gesteld om

de nieuwe markt van PGO-leveranciers te stimuleren en startte grote stimuleringsprogramma's in meerdere sectoren om de informatie die professionals registreren, beschikbaar te maken voor hun patiënten, in portalen en later ook in PGO's.

In 2021 zullen voor het eerst echt grote aantallen zorgprofessionals – met hun bronsystemen –aangesloten zijn op het MedMij-netwerk. Hierdoor wordt het voor mensen mogelijk hun gezondheidsgegevens vanuit verschillende bronnen op te halen richting hun PGO.

Wat zijn kenmerken van een goed afsprakenstelsel?

Om tot een goed afsprakenstelsel voor gegevensuitwisseling met PGO's te komen, loont het om naar voorbeelden in andere sectoren te kijken waar afspraken zijn gemaakt die barrières rond vertrouwen en interoperabiliteit wegnemen, onder waarborging van collectieve belangen. De afspraken hebben een wisselende mate van vrijwilligheid; veelal zijn afspraken eerst ontstaan in een vrijwillig kader en later verplichtend opgelegd. In onder andere de rechtspraak, het financiële systeem en rond elektronische identiteiten is veel ervaring opgedaan met stelsels van samenhangende afspraken. Enkele gemeenschappelijke kenmerken komen in al deze sectoren terug en kunnen als uitgangspunt dienen voor het MedMij Afsprakenstelsel.

De afspraken richten zich vrijwel altijd op professionele partijen, vaak intermediairs die optreden namens burgers of consumenten. De burgers zelf worden in hoge mate ontzorgd. Er is vaak sprake van professionele partijen die de interactie tussen twee partijen bevorderen. Een debiteur en een crediteur, een gedaagde en een eiser of een webwinkel en een klant maken gebruik van dienstverleners die de ingewikkelde uitvoering van de gewenste interactie mogelijk maken. Geld overmaken is voor de betaler en de ontvanger relatief gemakkelijk; banken handelen het ingewikkelde betalingsverkeer af voor hun klanten. Dat geldt ook voor het starten van een juridische procedure; advocaten en andere spelers in het rechtssysteem hanteren complexe procedures die gericht zijn op het bereiken van doelen voor hun cliënten. In deze sectoren is sprake van zakelijke dienstverlening door professionele partijen die onderling in een ander spel verwikkeld zijn dan degenen die zij vertegenwoordigen. Ook bij PGO's is een dergelijk model voorzienbaar; het zijn immers niet de persoon en de aanbieder zelf die de daadwerkelijke informatie-uitwisseling op zich nemen, maar aanbieders van ict-oplossingen.

Afspraken die worden gemaakt in stelsels met intermediaire dienstverleners richten zich veelal op twee niveaus. Allereerst worden regels gesteld voor de relatie tussen de vertegenwoordiger (dienstverlener) en de vertegenwoordigde. Dit zijn tamelijk statische afspraken die zich richten op het waarborgen dat de vertegenwoordiger de belangen van de vertegenwoordigde voldoende kan dienen. Zij gaan over zaken als transparantie, het voorkomen van belangenverstrengeling, het voldoen aan professionele normen, klacht- en verhaalsmogelijkheden, de redelijkheid van commerciële bepalingen, vertrouwelijkheid en het kunnen overstappen naar concurrenten. Deze afspraken dragen bij aan het vertrouwen van de uiteindelijke gebruiker, die wordt gecompenseerd voor de kennisvoorsprong van de professionele dienstverlener. Het verlaagt ook de transactiekosten en draagt bij aan een gezonde mededinging.

Daarnaast bestaat een afsprakendomein tussen de dienstverleners onderling. Dit zijn veel dynamischer afspraken die vooral gaan over de werkwijzen; dergelijke afspraken zijn dan ook niet technologieneutraal. De professionele afspraken gaan over onderwerpen zoals procedures, informatieverplichtingen, de inhoud van professionele kwaliteitsnormen, certificering, technische en organisatorische toelatingseisen en onderlinge garantstelling. Ook deze afspraken zijn gericht op het verlagen van de transactiekosten, het bevorderen van de mededinging en dienen uiteindelijk het vertrouwen van de persoon. De inhoud van de afspraken is voor de afnemer van de diensten echter moeilijk toetsbaar; het is een discours van vakgenoten onderling.

Voor elk afsprakenstelsel geldt dat een goede besturing ervan op de inzet, doorontwikkeling, beheer en het controleren van de afspraken een randvoorwaarde is. Daarin dient een heldere vertegenwoordiging van de betrokken partijen geregeld te zijn en moet de inbreng en besluitvorming transparant en open toegankelijk zijn. Voor vertrouwen in het stelsel is duidelijk toezicht ook noodzakelijk. De overheid kan in de besturing en het toezicht verschillende rollen en mate van invloed uitoefenen.

Waarom zou een partij toetreden tot een afsprakenstelsel?

Wanneer de normen tot stand komen in een vrijwillig stelsel, kunnen de professionele partijen (dienstverleners en eventueel aanbieders) er zelf voor kiezen om wel of niet deel te nemen. Deelnemende partijen zullen invloed moeten hebben op de afspraken, zodat er vertrouwen ontstaat in het realiteitsgehalte van de afspraken en het tempo van de doorontwikkeling. De kwaliteit en de continuïteit van de afspraken is daarbij ook van belang.

Om de deelname van partijen te bevorderen is het zowel nodig om de aard van de afspraken af te stemmen op de potentiële deelnemers, als om de governance zodanig in te richten dat de belangen van deelnemers doorlopend goed worden geborgd en er voorspelbaarheid en vertrouwen kunnen ontstaan.

Doel en scope van het MedMij Afsprakenstelsel

Het MedMij Afsprakenstelsel draagt eraan bij dat persoonsgebonden, gevoelige en vertrouwelijke gegevens op een veilige en gebruiksvriendelijke wijze uitgewisseld kunnen worden tussen PGO's enerzijds en anderzijds aanbieders (in eerste instantie), overheden en andere partijen (in een latere fase) die over relevante gezondheidsgegevens beschikken. De uitwisseling geschiedt in twee richtingen; personen kunnen gegevens ophalen en delen.

MedMij streeft naar het realiseren van interoperabiliteit voor het uitwisselen van persoonlijke gezondheidsgegevens tussen PGO-gebruikers en aanbieders. Hiertoe wordt een afsprakenstelsel overeengekomen, bestaande uit afspraken op juridisch, organisatorisch, financieel, communicatief, semantisch en technisch gebied, zodat PGO-gebruikers en aanbieders op een veilige manier gegevens kunnen uitwisselen. Partijen die deelnemen aan het MedMij Afsprakenstelsel committeren zich aan de afspraken, en kunnen diensten aanbieden op basis van de reeds overeengekomen afspraken.

Het afsprakenstelsel gaat uit van *centraal vertrouwen en decentrale operatie*. Dit houdt in dat het afsprakenstelsel eisen stelt waar deelnemers zich aan moeten houden. Dat stichting MedMij controleert of de deelnemers aan deze eisen voldoen. De decentrale operatie betekent dat de daadwerkelijke gegevensuitwisseling, zonder tussenkomst van MedMij, tussen deelnemers plaatsvindt. Het afsprakenstelsel biedt waarborgen voor een faire omgang met de belangen van de verschillende stakeholders. Bij de uitwisseling van gegevens via het MedMij-netwerk wordt echter uitgegaan van decentrale technische voorzieningen.

De waarde van het MedMij Afsprakenstelsel voor de persoon en zijn of haar persoonlijke gezondheidsomgeving

Door een persoonlijke gezondheidsomgeving te gebruiken die het MedMij-label draagt, kan iemand erop vertrouwen, dat deze PGO deelneemt aan het MedMij-netwerk en op een veilige manier gegevens kan uitwisselen met aanbieders. Voorwaarden opgelegd vanuit het MedMij Afsprakenstelsel borgen dat een persoonlijke gezondheidsomgeving met het MedMij-label op een veilige manier omgaat met gegevens. Het kan daarmee voorkomen dat er apps of eHealth-toepassingen zijn die niet kunnen of mogen werken via het MedMij Afsprakenstelsel.

Een persoonlijke gezondheidsomgeving met het MedMij-label is een waarborg voor betrouwbare grip op je gezondheidsgegevens.. MedMij zegt dus iets over integriteit, validiteit, actualiteit en interoperabiliteit, maar niet over de inhoudelijke functionaliteit van een PGO. Het gebruik van aanvullende functionaliteiten stelt mensen in staat om gezonder te leven en actiever bij te dragen aan een behandeling.

De inrichting van een persoonlijke gezondheidsomgeving zal net zo gepersonaliseerd zijn met aanvullende functionaliteiten als een smartphone dat is met apps. Mensen zullen zelf de functionaliteiten en apps gebruiken en kiezen die zij goed vinden. Op die manier wordt ingespeeld op de behoefte van de PGO-gebruiker via marktwerking. MedMij zegt om deze redenen niets over inhoudelijke functionaliteit en apps. Dat

kan veranderen onder invloed van de verdere afspraken tussen PGO-gebruiker, aanbieders, overheid en leveranciers over hetgeen preconcurrentieel en/of standaard gegarandeerd moet zijn voor de persoon in het MedMij Afsprakenstelsel.

Criteria

Inleiding

Criteria geven aan langs welke meetlat het succes van het afsprakenstelsel kan worden afgemeten. Criteria bestaan uit doelen (factoren waarbij gestreefd wordt naar een zo hoog mogelijke score, waarbij afwegingen tussen de doelen kunnen bestaan) en randvoorwaarden (niet-onderhandelbare eisen). De totstandkoming van het stelsel (het ontwerp- en beheerproces) en de inhoud van de afspraken zijn verweven; doelen kunnen dan ook betrekking hebben op beide aspecten. De nummering impliceert geen prioritering.

In doelstelling 7 wordt gesproken over zowel regie op gezondheid als over zelfmanagement. Deze begrippen hebben een verschillende betekenis.

> *"**Regie over gezondheid** gaat in de eerste plaats over gezond blijven."*
>
> *Bron: Bierma, L. & Heldoorn, M. (2013),* Het persoonlijk gezondheidsdossier - De visie van patiëntenfederatie NPCF*.*

> *“Het individuele vermogen om goed om te gaan met symptomen, behandeling, lichamelijke en sociale consequenties van de chronische aandoening en de bijbehorende aanpassingen in leefstijl. **Zelfmanagement** is effectief wanneer mensen in staat zijn zelf hun gezondheidstoestand te monitoren en de cognitieve, gedragsmatige en emotionele reacties te vertonen die bijdragen aan een bevredigende kwaliteit van leven.”*
>
> *Bron: NPCF (2009),* Zelfmanagement 2.0 - over zelfmanagement van de patiënt en wat eHealth daaraan kan bijdragen*.*

Doelen

Nr.	Titel
D1	**Creëren van vertrouwen bij personen en zorgaanbieders in gegevensuitwisseling**
D1a	Vertrouwelijkheid van persoonsgegevens
D1b	Duidelijkheid over aansprakelijkheid voor gegevensverwerkingen
D1c	Transparantie over voldoen aan normen
D1d	Betrouwbare en veilige authenticatie
D1e	Duidelijkheid over toezicht en handhaving
D1f	Helderheid over de rol van de overheid
D2	**Interoperabiliteit van gegevensuitwisseling**
D2a	Beschikbaarheid van generieke authenticatie-oplossingen
D2b	Duidelijkheid van de voorgeschreven standaarden
D2c	Volledigheid van de voorgeschreven standaarden

D2d	Implementatiegemak van de voorgeschreven standaarden
D2e	Aanpasbaarheid van voorgeschreven standaarden in toekomst
D2f	Implementatiegemak bij aanpassingen in de toekomst
D3	**Creëren van een tweezijdige markt met de juiste innovatie- en kwaliteitsprikkels en voldoende keuzemogelijkheden**
D3a	Reële marktwerking voor dienstverlening in het persoonsdomein
D3b	Reële marktwerking voor dienstverlening in het zorgaanbiedersdomein
D3c	Vertrouwen in de toekomstbestendigheid van het afsprakenstelsel
D3d	Duidelijkheid over businessmodellen
D4	**Gebruiksvriendelijkheid**
D4a	Begrijpelijkheid en snelheid van de interacties rond gegevensuitwisseling
D4b	Begrijpelijkheid en snelheid van het initieel starten met MedMij voor de persoon
D4c	Universele toegankelijkheid van de interacties rond gegevensuitwisseling
D5	**Snelheid van implementatie door dienstverleners**
D6	**Toekomstvastheid van de oplossing**
D6a	Strategische flexibiliteit voor de uitwisseling met nieuwe domeinen
D6b	Strategische flexibiliteit voor het gebruik van nieuwe informatiestandaarden
D6c	Duidelijkheid over de governance op langere termijn
D6d	Schaalbaarheid bij grote aantallen gebruikers
D6e	Schaalbaarheid bij grote datavolumes
D6f	Schaalbaarheid bij hoogfrequente uitwisselingen
D6g	Schaalbaarheid bij grote aantallen deelnemers
D7	**Compatibiliteit met zoveel mogelijk gewenste kenmerken van een persoonlijke gezondheidsomgeving**
D7a	Mogelijkheden om de wettelijke vertegenwoordiger van de patiënt gegevens te laten verzamelen of delen via de persoonlijke gezondheidsomgeving
D7b	Mogelijkheden voor het verzamelen van relevante gezondheidsinformatie
D7c	Mogelijkheden voor het delen van relevante gezondheidsinformatie
D7d	Mogelijkheden voor het voeren van regie over gezondheid en zorg
D7e	Mogelijkheden voor het ondersteunen van zelfmanagement

D8	**Betaalbaarheid**

Randvoorwaarden

Nr.	Titel	Toelichting
R1	**Voldoen aan actuele wet- en regelgeving**	De uitvoering van de afspraken zal op elk moment in lijn moeten zijn met de Nederlandse wet- en regelgeving. Daarom moet het afsprakenstelsel zo zijn opgezet dat partijen die betrokken zijn bij de uitvoering ervan in staat worden gesteld te voldoen aan deze wet- en regelgeving; dit betekent vooral dat een goede uitvoering van het afsprakenstelsel niet mag vereisen dat partijen afwijken van wet- en regelgeving.
R1a	Voldoen aan Algemene Verordening Gegevensbescherming	De opzet van het afsprakenstelsel dient aan te sluiten bij de Algemene Verordening Gegevensbescherming en daarvan afgeleide wet- en regelgeving.
R1b	Voldoen aan zorgwetgeving	De opzet van het afsprakenstelsel dient aan te sluiten bij gezondheidsrechtelijke wetgeving.
R1c	Voldoen aan mededingingswetgeving	De opzet van het afsprakenstelsel mag niet in strijd zijn met mededingingswetgeving. Dit behelst onder andere dat de toegang van deelnemers niet-discriminatoir moet zijn.
R1d	Voldoen aan overige wet- en regelgeving	De opzet van het afsprakenstelsel is conform overige relevante wet- en regelgeving.
R2	**Snelle oplevering van een eerste werkende versie van het afsprakenstelsel en het MedMij-netwerk**	Er is grote behoefte aan het mogelijk maken van gegevensuitwisseling tussen personen en zorgaanbieders. Wanneer het afsprakenstelsel niet snel genoeg beschikbaar is en baten kan opleveren, ontstaat het gevaar dat partijen alternatieve oplossingen kiezen waarmee fragmentatie ontstaat en een deel van de beoogde baten uitblijft.
R3	**Verbinden van meerdere domeinen**	Gezondheid en gezondheidsgegevens betreft alle aspecten van het leven en gaat niet alleen over gezond zijn of ziek zijn. Gezondheid gaat ook over bewust leven, over het verkrijgen van hulp, over zelfmanagement, over mantelzorg en over langdurige zorg en ondersteuning bij het ouder worden en voor het leven met een handicap. Het verzamelen van relevante gezondheidsgegevens betekent dan ook meer voor een persoonlijke gezondheidsomgeving dan alleen gegevens verzamelen vanuit de professionele curatieve zorg. Het afsprakenstelsel hoeft niet vanaf de start meerdere domeinen te verbinden, maar de fundamentele keuzes moeten het wel mogelijk maken om in de toekomst meerdere domeinen te ondersteunen.
R4	**Transparante en open besluitvorming over (door)ontwikkeling**	Voor zowel gebruikers, deelnemers als overige belanghebbenden geldt dat het vertrouwen in het afsprakenstelsel wordt ondersteund als de voortgang van de ontwikkeling ervan inzichtelijk is, en helder is hoe belangrijke afwegingen zijn gemaakt.

Principes

Inleiding

Principes zijn richtinggevende uitspraken over ontwerpkeuzes in het afsprakenstelsel. Zij gaan over de manier waarop de doelen zo goed mogelijk worden bereikt en recht wordt gedaan aan de randvoorwaarden. Principes op deze pagina betreffen algemene uitspraken. Daar waar principes betrekking hebben op een specifieke invalshoek (bijvoorbeeld juridica of architectuur) zijn zij te vinden bij de betreffende onderdelen van het afsprakenstelsel. Principes worden voorzien van een rationale, waarin de belangrijkste ontwerpafwegingen zijn opgenomen.

De principes zijn geordend in vier groepen:

- Neutraliteitsprincipes gaan over aspecten waarover het MedMij Afsprakenstelsel geen nadere beperkingen wil toevoegen aan wat in andere toepasselijke kaders al is voorzien. Daarmee bakenen deze principes het MedMij Afsprakenstelsel af op de aspecten waarover zij wel en niet wil gaan.
- Speelveldprincipes gaan over de centrale rol van dienstverleners in het MedMij Afsprakenstelsel.
- Informatieregieprincipes gaan over de aard van de regie die de persoon in het MedMij Afsprakenstelsel kan voeren, in relatie tot aanbieders en gezondheidsinformatie.
- Ontwikkelingsprincipes gaan over hoe het MedMij Afsprakenstelsel zich ontwikkelt en hoe die ontwikkeling gestuurd wordt.

Principes

De onderstaande tabel kan worden gebruikt om de principes te sorteren op nummer of op groep.

Nummer	Titel	Groep
1	Het MedMij-netwerk is zoveel mogelijk gegevensneutraal	Neutraliteit
2	Dienstverleners zijn transparant over de gegevensdiensten	Speelveld
3	Dienstverleners concurreren op de functionaliteiten	Speelveld
4	Dienstverleners zijn aanspreekbaar door de gebruiker	Speelveld
5	De persoon wisselt gegevens uit met de aanbieder	Informatieregie
6	MedMij spreekt alleen af wat nodig is	Neutraliteit
7	De persoon en de aanbieder kiezen hun eigen dienstverlener	Speelveld
8	(vervallen)	-
9	De dienstverleners zijn deelnemers van het afsprakenstelsel	Speelveld
10	Alleen de dienstverleners oefenen macht uit over persoonsgegevens bij de uitwisseling	Speelveld
11	Stelselfuncties worden vanaf de start ingevuld	Ontwikkeling
12	Het afsprakenstelsel is een groeimodel	Ontwikkeling
13	Ontwikkeling geschiedt in een half-open proces met verschillende stakeholders	Ontwikkeling

14	Uitwisseling is een keuze	Neutraliteit
15	Het MedMij-netwerk is gebruiksrechten-neutraal	Neutraliteit
16	De burger regisseert zijn gezondheidsinformatie als uitgever	Informatieregie
17	Aan de persoonlijke gezondheidsomgeving zelf worden eisen gesteld	Speelveld
18	Afspraken worden aantoonbaar nageleefd en gehandhaafd	Speelveld
19	Het afsprakenstelsel snijdt het gebruik van normen en standaarden op eigen maat	Neutraliteit

De principes worden hieronder per groep beschreven.

Neutraliteit

P1 - Het MedMij-netwerk is zoveel mogelijk gegevensneutraal

De dienstverleners vormen onderling een netwerk voor de uitwisseling van gegevens tussen het persoonsdomein en het aanbiedersdomein. Dit netwerk bestaat uit alle dienstverleners die deelnemen aan het afsprakenstelsel. Via een dienstverlener in het ene domein kunnen alle dienstverleners in het andere domein bereikt worden. Een dienstverlener die deelneemt aan het netwerk is verplicht om te interacteren met andere dienstverleners wanneer de gebruiker daarom vraagt. Daarmee kan een gebruiker via een dienstverlener in potentie toegang krijgen tot alle gebruikers in het andere domein. Het MedMij-netwerk regelt de totstandkoming van gegevensuitwisselingen, inclusief het proces van adressering en authenticatie, en het feitelijke transport van de gegevens tussen de dienstverleners. De opzet van het netwerk is zoveel mogelijk neutraal met betrekking tot de structuur of de inhoud van de gegevens zelf. Deze kern van afspraken is gegevensdienstonafhankelijk. Daarbovenop kunnen specifieke afspraken gelden die van toepassing zijn voor een bepaalde gegevensdienst of verzameling van gegevensdiensten.

P6 - MedMij spreekt alleen af wat nodig is

Onderwerpen die al geregeld zijn in wet- en regelgeving of de facto technisch geen barrière vormen, worden niet opgenomen in het afsprakenstelsel. Het stelsel richt zich op afspraken die nodig zijn om barrières te doorbreken en streeft geen volledigheid na. Op deze wijze wordt de kracht van bestaande normen ook zoveel mogelijk gebruikt en verbetert de onderhoudbaarheid van MedMij. Wijzigingen in wet- en regelgeving of generieke technische innovaties (mits zij de overige keuzes in het afsprakenstelsel niet raken) kunnen door deelnemers worden op- en nagevolgd zonder dat een wijziging van de formele afspraken noodzakelijk is.

P14 - Uitwisseling is een keuze

Het afsprakenstelsel laat de persoon en de aanbieder vrij om wel of niet een zekere uitwisseling aan te gaan met een zekere aanbieder respectievelijk persoon. Elke uitwisseling in het kader van het MedMij Afsprakenstelsel vindt plaats met goedvinden van persoon en aanbieder. De evidentie van dat goedvinden kan verschillen. Soms kan een partij dat goedvinden wettelijk niet weigeren. Soms is wettelijk geregeld dat voorafgaand aan de uitwisseling expliciete toestemming wordt verkregen. Maar ook in andere gevallen zal het afsprakenstelsel ervoor zorgdragen dat dat goedvinden wordt vastgesteld.

P15 - Het MedMij-netwerk is gebruiksrechten-neutraal

Het afsprakenstelsel laat de persoon en de aanbieder vrij in het gebruik van gezondheidsgegevens, in de betekenis en bedoeling die zij hebben. De gebruiksrechten van gezondheidsinformatie die omgaat in het kader van het MedMij Afsprakenstelsel volgen enkel uit de betekenis en bedoeling van die gegevens zelf en uit wet- en regelgeving. Personen en aanbieders, en/of hun respectievelijke dienstverleners, verbinden via

het MedMij-netwerk aan de gegevens geen nadere gebruiksbeperkingen jegens de ander, bijvoorbeeld door middel van aan die gegevens verbonden policy's. Zo worden aanbieders niet gehinderd in hun professionele praktijk en worden Personen in de gelegenheid gesteld regie te voeren over (de informatie over) hun gezondheid.

P19 - Het afsprakenstelsel snijdt het gebruik van normen en standaarden op eigen maat

Vanwege principe P6 legt het MedMij Afsprakenstelsel een voorkeur aan de dag voor het gebruik van elders gespecificeerde normen en standaarden. Daarbij gelden voorkeuren voor:

- internationale boven nationale boven sectorale normen en standaarden, opdat de schaalbare interoperabiliteit en de gelijkheid in het MedMij-speelveld worden bevorderd;
- open boven half-open boven gesloten standaarden, opdat gelijkheid in het MedMij-speelveld wordt bevorderd en wordt voorkomen dat al te specifieke en niet-beïnvloedbare belangen de norm of standaard inhoudelijk gaan vervreemden van toepasbaarheid in MedMij-context;
- bewezen boven experimentele normen en standaarden, opdat de stabiliteit en kwaliteit van het MedMij Afsprakenstelsel worden bevorderd;
- standaarden en normen die ontwikkeld zijn vanuit contexten, principes en hoofdkeuzes die passen bij die van het MedMij Afsprakenstelsel, opdat het gebruik ervan voor het MedMij Afsprakenstelsel niet vroeg of laat tot ingrijpende discontinuïteit leidt en zo de duurzaamheid van het afsprakenstelsel bedreigt.

Daar waar het MedMij Afsprakenstelsel gebruik maakt van normen en standaarden, verwijst het ernaar louter als product, niet als ontwikkel-, beheer- of besturingsproces. De verwijzing geldt enkel specifieke versies van een norm of standaard, en dus geen andere versies, huidig of toekomstig. Het MedMij Afsprakenstelsel maakt voor zover nodig specifieke keuzes binnen de norm of standaard, om het gebruik te laten passen in MedMij-context.

Speelveld

P2 - Dienstverleners zijn transparant over de gegevensdiensten

De dienstverleners zijn naar elkaar en naar de gebruikers transparant over de gegevensdiensten die zij namens hun gebruikers kunnen aanbieden over het MedMij-netwerk. MedMij definieert welke gegevensdiensten over het MedMij-netwerk aangeboden mogen worden en biedt een faciliteit om het aanbod van de dienstverleners inzichtelijk te maken.

P3 - Dienstverleners concurreren op de functionaliteiten

De dienstverleners bieden hun gebruikers functionaliteit in de vorm van een persoonlijke gezondheidsomgeving, koppelingen met zorginformatiesystemen, apps en dergelijke. De dienstverleners zijn vrij in het vormgeven van dit aanbod en concurreren met elkaar om de gunst van de gebruiker. De opzet van het MedMij-netwerk maakt het mogelijk dat een gebruiker meerdere dienstverleners heeft.

P4 - Dienstverleners zijn aanspreekbaar door de gebruiker

Dienstverleners kunnen functionaliteiten zelf aanbieden, of de gegevens die zij namens de persoon hebben ontvangen op verzoek van de persoon beschikbaar stellen aan andere partijen die functionaliteit leveren in het persoonsdomein. Ook kunnen dienstverleners, in beide domeinen, ervoor kiezen de dienstverlening rond de gegevenslogistiek uit te besteden aan andere partijen. De MedMij-dienstverlener blijft echter altijd door de gebruiker aanspreekbaar op de correcte wijze van omgang met persoonsgegevens en de kwaliteit van de interactie via het MedMij-netwerk.

P7 - De persoon en de aanbieder kiezen hun eigen dienstverlener

De persoon en de aanbieder kiezen elk hun eigen dienstverlener(s), door wie zij vertegenwoordigd worden in de gegevensuitwisseling. Het werken met één dienstverlener in het gehele stelsel is niet mogelijk, omdat er

dan geen keuzevrijheid zou zijn en de facto een centrale voorziening in plaats van een afsprakenstelsel zou ontstaan. Dit betekent ook dat elke deelnemende dienstverlener aanbieder alle deelnemende dienstverleners persoon op het MedMij Netwerk gelijk moet behandelen en dat elke deelnemende dienstverlener persoon alle deelnemende dienstverleners aanbieder op het MedMij Netwerk gelijk moet behandelen. Interne ontwerpkeuzen van een dienstverlener in het ene domein dienen niet die in het andere domein te beïnvloeden.

P9 - De dienstverleners zijn deelnemers van het afsprakenstelsel

Het afsprakenstelsel leidt tot afspraken tussen de dienstverleners. Gebruikers zijn niet rechtstreeks deelnemer in het stelsel; dit doen we om hen zo veel mogelijk te ontzorgen. De dienstverleners zijn deelnemers in het afsprakenstelsel en binden zich privaatrechtelijk en vrijwillig aan het geheel van de afspraken.

P10 - Alleen de dienstverleners oefenen macht uit over persoonsgegevens bij de uitwisseling

De dienstverleners wisselen tussen de domeinen persoonsgegevens uit. Dienstverleners mogen gebruikmaken van derde partijen voor de uitoefening van taken maar blijven geheel verantwoordelijk voor en aanspreekbaar op het nakomen van de afspraken. Partijen die niet onder de volledige verantwoordelijkheid van een dienstverlener vallen, mogen niet in staat worden gesteld om macht uit te oefenen over de persoonsgegevens. Denk hierbij aan telecomproviders die connectiviteit aanbieden tussen de dienstverleners; zij kunnen een rol vervullen bij het transport van de gegevens maar alleen als zij op geen enkele manier kennis kunnen nemen van de inhoud van de uitwisseling. Met dit principe wordt gewaarborgd dat altijd helder is wie potentieel toegang hebben gehad tot persoonsgegevens, zonder dat voor gebruikers of toezichthouders een zoekplaatje ontstaat. Een decentrale oplossing voor gegevensuitwisseling zonder derde partijen tussen de dienstverleners is technisch en juridisch goed mogelijk. Vanuit het oogpunt van eenvoud is het daarom ook niet nodig om partijen te introduceren in het stelsel die niet onder de verantwoordelijkheid van dienstverleners vallen.

P17 - Aan de persoonlijke gezondheidsomgeving zelf worden eisen gesteld

MedMij voorziet in afspraken over de relatie tussen de deelnemer en de gebruiker. De persoon behoeft hierbij een bijzondere bescherming. Anders dan de aanbieder is hij geen professionele partij (het werken met gezondheidsgegevens is geen dagelijkse kost). Daarbij zijn de mogelijkheden van personen om volledig geïnformeerde afwegingen te maken in hun eigen belang onderling zeer verschillend en soms beperkt. Ook hebben personen een relatief grote vertrouwensdrempel te overwinnen omdat het gebruik van een persoonlijke gezondheidsomgeving volgens de MedMij-afspraken betrekking heeft op hun eigen gegevens (en niet die van een ander). Verder geldt dat door het gebruik van persoonlijke gezondheidsomgevingen nieuwe gegevensverzamelingen ontstaan, waarvoor minder specifieke regelgeving en ervaringen bestaan dan wanneer het gaat om gegevensverzamelingen in het aanbiedersdomein. Denk daarbij aan het ontbreken van een patiëntgeheim, waar wel een medisch beroepsgeheim bestaat in het aanbiedersdomein. Ten slotte zal de waarde van het merk MedMij en de mate waarin het erin slaagt om vertrouwensbarrières voor gegevensuitwisseling te overwinnen, mede afhankelijk zijn van de mate waarin personen vertrouwen hebben in persoonlijke gezondheidsomgevingen die uitwisselen via MedMij. Dat betekent dat er een stelselbelang is bij het waarborgen van de betrouwbaarheid van de persoonlijke gezondheidsomgevingen en de deelnemers die deze omgevingen aanbieden.

Dit leidt ertoe dat MedMij eisen stelt aan de Dienstverlener Persoon die niet alleen de uitwisseling met aanbieders betreffen, en betrekking hebben op de persoonlijke gezondheidsomgeving zelf.

P18 - Afspraken worden aantoonbaar nageleefd en gehandhaafd

Dienstverleners dienen aan te tonen dat zij zich houden aan afspraken uit het MedMij Afsprakenstelsel. Daarbij kan toetsing door derde partijen worden vereist. Enkel een intentie tot het volgen van of een juridische binding aan de afspraken is niet voldoende. Toetsing kan ook vooraf plaatsvinden. Er wordt toezicht gehouden op de naleving door een van de deelnemers onafhankelijke partij, die over een proportioneel en effectief sanctie-instrumentarium beschikt. Op deze manier wordt het onaantrekkelijker voor

partijen om bewust af te wijken van de afspraken in eigen voordeel, ontstaat een actievere omgang met de afspraken die een juiste interpretatie en suggesties voor doorontwikkeling tot gevolg heeft, en wordt bijgedragen aan het vertrouwen van alle betrokkenen.

Informatieregie

P5 - De persoon wisselt gegevens uit met de aanbieder

Personen wisselen gezondheidsgegevens uit met aanbieders. Veel van de gegevens zijn geregistreerd of worden gebruikt door individuele zorgverleners. De gegevens worden vaak echter bijgehouden in een informatiesysteem op het niveau van de organisatie. Denk hierbij aan een huisartsenpraktijk of een ziekenhuis die elektronische dossiers over patiënten bijhoudt, waarbij meerdere zorgverleners het medisch dossier bijwerken en raadplegen. Steeds vaker worden dossiers ook specialisme-overstijgend bijgehouden; de ontwikkeling van een kerndossier is hiervan een goed voorbeeld. Ook kan MedMij betrekking hebben op zorgadministratieve gegevens (zoals afspraken), die worden bijgehouden door anderen dan de zorgverleners zelf. Voor de uitwisseling van gegevens is het daarom passend om te spreken van een interactie tussen de persoon en de aanbieder, waarbij de aanbieder een organisatie is van een of meer zorgverleners. Wanneer we zouden uitgaan van de zorgverlener wordt het beschrijven van het afsprakenstelsel nodeloos ingewikkeld, omdat de zorgverlener dan vaak een relatie heeft met andere zorgverleners of met niet-medische medewerkers of organisaties. De aanbieder is een logische partij om over het geheel dat nodig is voor de uitwisseling van gezondheidsgegevens met de patiënt namens de zorgverleners afspraken te maken met de dienstverlener in het MedMij-netwerk.

P16 - De burger regisseert zijn gezondheidsinformatie als uitgever

MedMij wil iedereen meer regie op zijn gezondheid geven. Daarvoor is het nodig dat iedereen, door middel van een persoonlijke gezondheidsomgeving, inzicht in zijn eigen gezondheidsinformatie heeft, en op die gezondheidsinformatie regie kan voeren. Voor dat laatste zijn meerdere vormen denkbaar, die aanzienlijk verschillen in de kracht van de regie en in de eruit voortvloeiende verantwoordelijkheden en vrijheden voor alle betrokkenen. Ook verschillen zij sterk in hoe het informatieverkeer is ingericht, ook functioneel en technisch. Het MedMij afsprakenstelsel kiest voor een regiemodel waarin de burger zijn eigen gezondheidspublicaties samenstelt en uitgeeft, dat wil zeggen, deelt met lezers. Daartoe is het hem gegeven bronnen aan te boren. Bronnen en lezers zijn allereerst aanbieders van zorg- en gezondheidsdiensten. De uitgever is dus de hoofdrol in het persoonsdomein; bron en lezer zijn de twee hoofdrollen in het aanbiedersdomein. Deze vorm van informatieregie legt het initiatief in hoge mate bij de burger (de uitgever) en is daarmee krachtiger dan het model waarin de burger alleen kan reageren - instemmend of afkeurend - op verkeer tussen aanbieders. Anderzijds gaat de regievorm niet zover dat zij de burger het onverminderde economische eigendom toedicht over de gezondheidsinformatie, en het intellectuele eigendom evenmin. Achter deze vormen zouden nog geheel andere regiemodellen schuilgaan, met onwenselijke consequenties en risico's.

Ontwikkeling

P11 - Stelselfuncties worden vanaf de start ingevuld

Het functioneren van het MedMij-netwerk en het afsprakenstelsel is mede afhankelijk van de mate waarin het stelsel als geheel in staat is om in te spelen op ontwikkelingen in de omgeving of in de operatie, zowel positieve als negatieve. Daarbij zijn rollen nodig die zich richten op het belang van het stelsel, en niet op een specifieke deelnemer of een specifieke relatie tussen twee deelnemers daarin. Immers, er zijn vraagstukken (zoals doorontwikkeling, het beslechten van geschillen of het reageren op een beveiligingsincident) die het belang van een of twee deelnemers overstijgen. De belangrijkste stelselfuncties, waaronder ten minste ontwikkeling, toezicht en handhaving, worden vanaf de start van het afsprakenstelsel ingevuld. De diepgang van deze functies en de organisatie(s) die deze rollen vervullen kunnen in de loop van de tijd wijzigen.

P12 - Het afsprakenstelsel is een groeimodel

Om snel een eerste versie van het afsprakenstelsel te kunnen krijgen én te kunnen leren van tussentijdse ervaringen, wordt het afsprakenstelsel opgezet als groeimodel. De belangrijkste barrières voor de uitwisselingen met de meeste potentiële baten worden als eerste opgepakt. Daarbij is ook de haalbaarheid van realisatie, waaronder de aansluiting op de huidige ontwikkelingen in de markt, een criterium. Daar waar duidelijkheid benodigd is in de afspraken die pas op termijn van kracht zijn maar die op enig moment nog niet haalbaar zijn, kan een groeipad worden afgesproken.

Het afsprakenstelsel start met de uitwisseling tussen de persoon en de aanbieder. De opzet van het stelsel is echter wel zodanig dat een uitwisseling tussen de persoon en derden op termijn mogelijk is.

P13 - Ontwikkeling geschiedt in een half-open proces met verschillende stakeholders

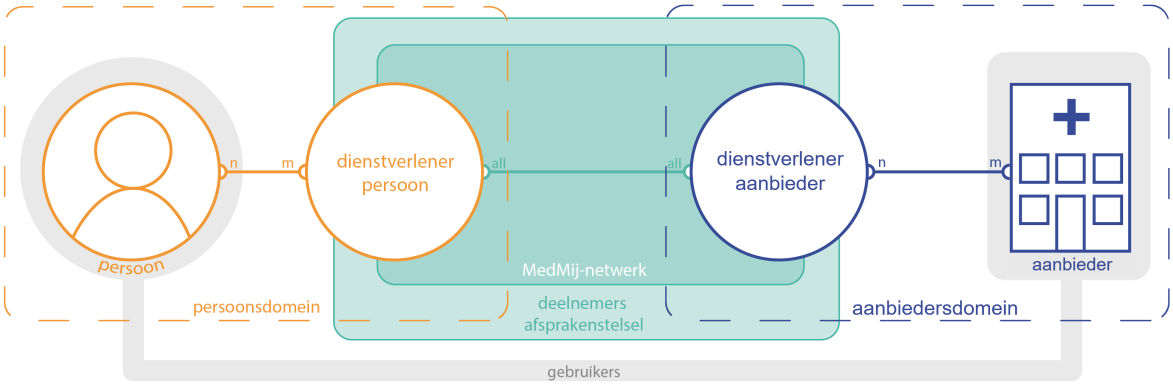
Het afsprakenstelsel wordt (door)ontwikkeld in samenspraak met de belangrijkste stakeholders, waaronder vertegenwoordigers van de deelnemers, de gebruikers en partijen met een belang bij het functioneren van het stelsel. Dit zorgt ervoor dat (door)ontwikkeling en gebruik zoveel mogelijk van elkaar profiteren, versnelling optreedt in de implementatie, en draagvlak wordt verworven bij de afnemers van het ontwikkelproces. Vanwege de gevraagde snelheid en de aansluiting op andere centraal gestuurde initiatieven vindt de ontwikkeling plaats in een half-open proces. Deelname is mogelijk voor iedere partij die zich afdoende kan kwalificeren op toegevoegde waarde; de kaders voor en de ritmiek van het ontwerpproces worden echter bepaald door het programma MedMij en later de Stichting MedMij.

Opzet

Inleiding

De opzet van het afsprakenstelsel geeft op het hoogst mogelijke niveau een overzicht van de rollen in de gegevensuitwisseling via het MedMij-netwerk, hun onderlinge relaties, de interacties tussen deze rollen en de belangrijkste begrippen die geassocieerd zijn met rollen en partijen.

Rollen en relaties



We onderscheiden het Persoonsdomein en het Aanbiedersdomein. Deze begrippen helpen om een onderscheid te kunnen maken tussen datgene dat zich afspeelt in de controlesfeer van de Persoon (door hemzelf of namens hem door zijn Dienstverlener persoon) en datgene dat zich afspeelt in de controlesfeer van de Aanbieder (door hemzelf of namens hem door zijn Dienstverlener aanbieder). Op beide domeinen is verschillende wetgeving van toepassing, en in beide domeinen kan de onderlinge verhouding tussen de Dienstverlener en de Gebruiker verschillend zijn.

De Persoon en de door hem of haar gekozen Dienstverleners persoon vormen het Persoonsdomein. Een Persoon kan gebruikmaken van een of meer Dienstverleners persoon. Een Dienstverlener persoon kan actief zijn voor een of meer Personen. In de afbeelding is dit weergegeven als een n-op-m-relatie.

De Aanbieder en de door hem gekozen Dienstverlener aanbieder vormen het Aanbiedersdomein. De Aanbieder kiest een of meer Dienstverleners aanbieder. Een Dienstverlener aanbieder kan actief zijn voor een of meer Aanbieders. In de afbeelding is dit weergegeven als een n-op-m-relatie.

De Persoon en de Aanbieder zijn Gebruiker van MedMij. De Dienstverlener persoon en de Dienstverlener aanbieder zijn Deelnemer in het afsprakenstelsel. Alle Dienstverleners persoon en alle Dienstverleners aanbieder vormen samen het MedMij-netwerk. Elke Dienstverlener persoon moet elke Dienstverlener aanbieder kunnen bereiken, en vice versa. Daarom is een 'all-to-all'-relatie opgenomen in de afbeelding.

De Dienstverleners zijn voor de interactie via het MedMij-netwerk gehouden aan een set afspraken over het gewenste en toegestane gedrag op het netwerk. Het afsprakenstelsel bevat afspraken over de interacties via het netwerk, en een aantal aanvullende afspraken waaraan de Dienstverlener zich dient te houden vanuit het oogpunt van bescherming van de Gebruiker. De Dienstverleners leveren de Gebruiker daarnaast diensten waarover geen afspraken worden gemaakt via het afsprakenstelsel.

Interacties tussen de rollen

In onderstaande tabel zijn op het hoogste niveau de gegevensuitwisselingen tussen de gebruikers van het MedMij-netwerk beschreven. Hierbij is aangegeven wat de kernverantwoordelijkheid is van de verschillende

rollen in het afsprakenstelsel. Het interactie-overzicht gaat niet in op de wijze waarop dit wordt gerealiseerd, en ook niet op randvoorwaardelijke interacties of gegevensuitwisselingen tussen de partijen (zoals het aansluiten op het MedMij-netwerk).

Nr.	Beoogd resultaat	Interacties
1	De Persoon heeft de door hem of haar gevraagde gezondheidsgegevens verkregen, die de Aanbieder digitaal over hem of haar beschikbaar heeft.	De Persoon verzoekt de Dienstverlener persoon om namens hem of haar de Dienstverlener aanbieder te verzoeken de gevraagde gegevens zoals die bij de Aanbieder bekend zijn te verzenden naar de Dienstverlener persoon.
2	De Persoon heeft de Aanbieder gegevens over de gezondheid van de Persoon verstrekt.	De Persoon verzoekt de Dienstverlener persoon om namens hem of haar aan de Dienstverlener aanbieder een door de Persoon aan de Dienstverlener persoon beschikbaar gestelde gegevensset te verzenden. De Dienstverlener aanbieder informeert de Aanbieder over de nieuwe gegevens.

Begrippenlijst

Inleiding

De begrippenlijst geeft een eenduidige definitie van de belangrijkste begrippen die in het afsprakenstelsel worden gebruikt.

Begrippen

Begrip	Domein	Definitie	Synoniemen
Abonnement	tussen Persoonsdomein en Aanbiedersdomein	Overeenkomst tussen een *Aanbieder* en een *Persoon* voor het (mogen) leveren van *Notificaties* door *Aanbieder* aan *Dienstverlener persoon*. Deze release van het MedMij Afsprakenstelsel betreft enkel *Abonnementen* die betrekking hebben op *Gegevensdiensten* die zijn gebaseerd op de functie *Verzamelen*.	
Addendum aanbieder zonder behandelrelatie	Aanbiedersdomein	Het addendum maakt het mogelijk om *Aanbieders* zonder behandelrelatie die voor de *Persoon* relevante gezondheidsgegevens over de *Persoon* beschikbaar hebben gebruik te laten maken van het MedMij-netwerk. Dit Addendum maakt onderdeel uit van het MedMij Afsprakenstelsel en is hiermee onlosmakelijk is verbonden.	
Afsprakenstelsel	alle domeinen samen	Set van afspraken op juridisch, organisatorisch, financieel, semantisch en technisch gebied om alle partijen voldoende vertrouwen te geven in hetgeen het stelsel hen biedt. Partijen die deelnemen aan het MedMij Afsprakenstelsel committeren zich aan de afspraken, en kunnen op basis van de reeds overeengekomen afspraken, diensten aanbieden.	MedMij Afsprakenstelsel
Backchannel-verkeer	tussen Persoonsdomein en Aanbiedersdomein	Verkeer dat niet zichtbaar is voor *Persoon*. Het gaat hierbij om verkeer tussen servers uit verschillende domeinen, die	

		zonder tussenkomst van een *Persoon* met elkaar communiceren.	
Catalogus	alle domeinen samen	Verzameling van *Gegevensdiensten* die op enig moment door *Aanbieders* aangeboden mogen (of mochten) worden op het MedMij-netwerk.	
Deelnemer	Persoonsdomein of Aanbiedersdomein	Een partij die dienstverlening aanbiedt binnen het MedMij Afsprakenstelsel. De *Dienstverlener persoon* en de *Dienstverlener aanbieder* zijn Deelnemer in het afsprakenstelsel en daarmee gebonden aan de afspraken, bekrachtigd door het tekenen van een deelnemersovereenkomst.	
Dienstverlener persoon	Persoonsdomein	Dit betreft een rol in het MedMij Afsprakenstelsel. Levert een Persoonlijke gezondheidsomgeving, een dienst aan de *Persoon* voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de *Aanbieder* mogelijk maakt middels het MedMij Afsprakenstelsel.	
Dienstverlener aanbieder	Aanbiedersdomein	Dit betreft een rol in het MedMij Afsprakenstelsel. Levert Diensten aan de *Aanbieder* gerelateerd aan de uitwisseling tussen *Persoon* en *Aanbieder* en committeert zich hiervoor aan de naleving van de afspraken van het MedMij Afsprakenstelsel.	
Frontchannel-verkeer	tussen Persoonsdomein en Aanbiedersdomein	Al het verkeer dat zichtbaar is voor *Persoon*, vaak is hierbij een *User-Agent* betrokken.	
Gebruiker	Persoonsdomein of Aanbiedersdomein	Een partij die gebruik maakt van dienstverlening van deelnemers aan het afsprakenstelsel. De *Persoon* en de *Aanbieder* zijn Gebruiker van MedMij.	
Gegevensdienst	tussen Persoonsdomein en Aanbiedersdomein	Een gestandaardiseerde dienst voor gegevensuitwisseling met waarde voor de Gebruiker die door een Dienstverlener kan worden ontsloten over het MedMij-netwerk. MedMij definieert welke	

		gegevensdiensten over het MedMij-netwerk ontsloten mogen worden en biedt een faciliteit om het aanbod van de dienstverleners inzichtelijk te maken.	
Gezondheidsgegeven	tussen Persoonsdomein en Aanbiedersdomein	Gegeven betreffende de geestelijke en/of lichamelijke gesteldheid van een *Persoon*.	Persoonlijke gezondheidsinformatie, gezondheidsinformatie
MedMij-netwerk	tussen Persoonsdomein en Aanbiedersdomein	Alle *Dienstverleners persoon* en alle *Dienstverleners aanbieder* vormen samen het MedMij-netwerk. Elke *Dienstverlener persoon* moet elke *Dienstverlener aanbieder* kunnen bereiken, en vice versa.	Netwerk
Notificatie	tussen Persoonsdomein en Aanbiedersdomein	Kennisgeving, van *Aanbieder* aan *Dienstverlener persoon.* Deze release van het MedMij Afsprakenstelsel betreft • notificaties van wijzigingen in (gezondheids)informatie met betrekking tot een *Persoon* en en *Gegevensdienst*, zoals beheerd bij de *Aanbieder*. Dergelijke notificaties heten inhoudelijke notificaties of r esource notifications. • notificaties van beperking of beëindigen van een *Abonnement* op initiatief van *Aanbieder*. Deze notificaties heten abonnementsnotificaties of subscription notifications.	
Persoon	Persoonsdomein	Degene, 16 jaar of ouder, op wie Gezondheidsgegevens betrekking hebben die via MedMij worden uitgewisseld en tevens de Gebruiker in het Persoonsdomein.	Betrokkene, burger, individu, patiënt, cliënt, zorgconsument, zorggebruiker
Persoonlijke gezondheidsomgeving	Persoonsdomein	Een Persoonlijke gezondheidsomgeving is een dienst aan de *Persoon* voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de *Aanbieder* mogelijk maakt middels het MedMij Afsprakenstelsel.	PGO, persoonlijk gezondheidsplatform

Persoonsdomein	Persoonsdomein	Alle *Personen* en alle *Dienstverleners personen* vormen samen het Persoonsdomein.	
Rol	alle domeinen samen	Een samenhangende set van verwachte en overeengekomen verantwoordelijkheden en interacties in het MedMij Afsprakenstelsel. Aan een Rol zijn afspraken gekoppeld zoals vastgelegd in het Afsprakenstelsel MedMij. Een rol kan worden vervuld door een natuurlijke persoon en/of organisatie.	
Zorgaanbieder	Aanbiedersdomein	Een zorgverlener of een verband van zorgverleners die behandelingsovereenkomsten kunnen aangaan met patiënten op grond van art. 7:446 BW en tevens de Gebruiker in het Aanbiedersdomein.	Zorginstelling, zorgorganisatie, brondossierhouder
Aanbiedersdomein	Aanbiedersdomein	Alle *Aanbieders* en alle *Dienstverleners aanbieder* vormen samen het Aanbiedersdomein.	
Zorginformatiesysteem	Aanbiedersdomein	Het systeem of geheel van de systemen waarin de zorgaanbieder het medisch dossier van de persoon bijhoudt.	XIS

Juridische context

De juridische context bestaat uit:

- Het Juridisch kader, waarin de relevante wet- en regelgeving wordt geanalyseerd. De analyse biedt inzicht voor deelnemers en de beheerorganisatie aangaande de eisen die de wet aan hen stelt, en biedt tevens onderbouwing voor enkele nadere afspraken binnen het MedMij Afsprakenstelsel.
- Een beschrijving van het stelsel van Overeenkomsten en rechtsrelaties die gelden binnen het MedMij Afsprakenstelsel.
- Een analyse van de verwerkingsverantwoordelijkheden voor de gegevensuitwisseling via het MedMij Afsprakenstelsel. De analyse biedt inzicht voor deelnemers en de beheerorganisatie aangaande de eisen die de wet aan hen stelt, en biedt tevens onderbouwing voor en toelichting op enkele nadere afspraken binnen het MedMij Afsprakenstelsel.
- Een toelichting op de verantwoordelijkheden en normen voor deelnemers die voortvloeien uit de AVG. Daarbij is op onderdelen aangegeven wat het MedMij afsprakenstelsel hierop aanvullend of invullend vereist evenals eventuele opmerkingen of aandachtspunten voor deelnemers.

Juridisch kader

Het juridisch kader geeft een overzicht van de relevante wet- en regelgeving voor deelnemers aan het MedMij Afsprakenstelsel. Deze wet- en regelgeving heeft betrekking op de dienstverlening die met behulp van het MedMij Afsprakenstelsel wordt uitgeoefend. Dit overzicht pretendeert niet volledig te zijn. Het is en blijft te allen tijde de verantwoordelijkheid van de betrokken partijen om aan de voor hen geldende (specifieke) wet- en regelgeving te voldoen. Voor de toepassing van de in het overzicht opgenomen wet- en regelgeving voor het MedMij Afsprakenstelsel is een toelichting opgenomen.

De privaatrechtelijke afspraken, op basis waarvan partijen gerechtigd zijn hun diensten in relatie tot het MedMij Afsprakenstelsel aan te bieden, zijn aanvullend op de geldende wet- en regelgeving en zijn opgenomen bij Overeenkomsten en rechtsrelaties.

> Het juridisch kader is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moeten de wetgevingen voor dat betreffende domein worden toegevoegd aan het juridisch kader. Ook moeten dan de generieke wetten zo beschreven worden, dat ze van toepassing zijn op de verschillende domeinen in het afsprakenstelsel.

Wetgeving	Toelichting	Toepassing	Van toepa in dome
Algemene Verordening Gegevensbescherming (AVG) (gepubliceerd 27-04-2016, geldend vanaf 25-05-2018)	MedMij-deelnemers verwerken persoonsgegevens. De Algemene Verordening Gegevensbescherming (AVG) is daarmee van toepassing. De AVG behelst de waarborgen voor een aantoonbare en controleerbare rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. Een belangrijk onderdeel hiervan zijn de rechten van betrokkenen, zoals het recht op informatie en inzage. Een aantoonbare en controleerbare verwerking van persoonsgegevens houdt in dat iedere organisatie die persoonsgegevens verwerkt actief en controleerbaar moet kunnen aantonen dat zij zich aan de beginselen van een rechtmatig, behoorlijke en transparante verwerking van persoonsgegevens	Of een partij die met gebruikmaking van het MedMij Afsprakenstelsel verwerker of verwerkingsverantwoordelijke is, is voor de verwerking van persoonsgegevens in relatie tot het aanbieden van MedMij diensten of -gegevensdiensten, dus afhankelijk van de vraag: • welke partij(en) in de concrete situatie feitelijk (gezamenlijk) doel en middelen bepaalt (bepalen) van de verwerking van persoonsgegevens; • of er een partij is die voor de verwerkingsverantwoordelijke 'slechts' handelt volgens de vooraf door de verwerkingsverantwoordelijke opgestelde en schriftelijke instructies en geen zeggenschap heeft over de persoonsgegevens. Hieronder geven wij - gelet op de technische inrichting en	Zorgd

houdt. Door aan deze beginselen te voldoen, wordt gewaarborgd dat de betrokkene zicht heeft op wie voor welke doeleinde(n) welke persoonsgegevens van hem /haar verwerkt en kan hij/zij ook controle uitoefenen over de verwerking van zijn persoonsgegevens.

Twee belangrijke begrippen uit de AVG zijn die van 'verwerkingsverantwoordelijke' en 'verwerker'. De verwerkingsverantwoordelijke heeft zeggenschap over de verwerking van persoonsgegevens en stelt het doel of de middelen voor de verwerking van persoonsgegevens vast. De verwerker verwerkt de persoonsgegevens in opdracht van en volgens schriftelijke instructie van de verwerkingsverantwoordelijke. Alhoewel de primaire verantwoordelijkheid voor de gegevensverwerking bij de verwerkingsverantwoordelijke ligt, is ook de verwerker aansprakelijk indien de verwerking van persoonsgegevens in strijd met de beginselen van de AVG plaatsvindt, dan wel wanneer bij de verwerking van de persoonsgegevens niet conform de rechtmatige instructies van de verwerkingsverantwoordelijke is gehandeld.

werking van het MedMij Afsprakenstelsel en de daaruit voortvloeiende verwerking van persoonsgegevens - een zienswijze op de invulling van verwerkingsverantwoordelijke en verwerker. Zie voor een meer uitgebreide toelichting op de rechtsrelaties tussen de bij het MedMij Afsprakenstelsel betrokken partijen Overeenkomsten en rechtsrelaties.

Ten eerste wordt - voor wat betreft de verantwoordelijkheidsverdeling ten aanzien van de naleving van de wet- en regelgeving in z'n algemeenheid - opgemerkt dat wettelijke verantwoordelijkheden en afspraken ten aanzien van bestaande eHealth toepassingen en/of initiatieven (tussen betrokken partijen) niet worden doorkruist door gebruikmaking van het MedMij Afsprakenstelsel.

Gebruikmaking van het MedMij Afsprakenstelsel betekent ook geen wijziging in de verantwoordelijkheid voor de naleving van wettelijke verplichtingen in relatie tot de uitwisseling van (persoons) gegevens en/of gezondheidsgegevens ten opzichte van de situatie zoals deze gelden op basis van de WGBO, de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de AVG. Dit betekent dat voor een rechtmatige, behoorlijke en transparante verwerking van de (persoons) gegevens en gezondheidsinformatie via MedMij de actoren die een rol spelen in de gegevensuitwisseling via MedMij de volgende verantwoordelijkheid hebben:

1. De Zorgaanbieder als Gebruiker van Diensten van de Dienstverlener zorgaanbieder van het MedMij

			Afsprakenstelsel is gehouden tot naleving van de WGBO, de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en is in deze hoedanigheid ‘verwerkingsverantwoordelijke’ voor de verwerking van persoonsgegevens in de zin van de AVG. In het geval de Zorgaanbieder als ‘verwerkingsverantwoordelijke’ de Dienstverlener Zorgaanbieder inschakelt om in opdracht van hem (bijzondere) persoonsgegevens met de Persoon (via het MedMij-netwerk) te verwerken, is de Zorgaanbieder voor deze verwerking van persoonsgegevens verplicht een verwerkersovereenkomst met de Dienstverlener Zorgaanbieder af te sluiten. Hiervan is bijvoorbeeld sprake bij authenticatie van de Persoon door de Zorgaanbieder als gevolg van de identificatieplicht voor de Zorgaanbieder overeenkomstig de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Voor onder meer deze situatie wordt door het MedMij Afsprakenstelsel een Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener zorgaanbieder ter beschikking gesteld. 2. De Dienstverlener Zorgaanbieder is ‘verwerker’ van de Zorgaanbieder, voor zover de Dienstverlener in opdracht van en op basis van schriftelijke instructies van de Zorgaanbieder persoonsgegevens verwerkt. Van een dergelijke situatie is bijvoorbeeld sprake bij authenticatie - in opdracht van de Zorgaanbieder - van de Persoon die (via de

			Dienstverlener Persoon) informatie opvraagt bij zijn Zorgaanbieder. Zie ook punt 1. 3. De Dienstverlener Persoon is ‘verwerkingsverantwoordelijke’ voor de verwerking van persoonsgegevens voor Diensten en Gegevensdiensten die hij via het MedMij Afsprakenstelsel ten behoeve van de Persoon ontsluit. In het MedMij Afsprakenstelsel wordt de persoon niet gezien als verwerkingsverantwoordelijke. De filosofie achter de AVG is om een persoon te beschermen tegen de macht van de overheden en bedrijven over hun persoonsgegevens. Als een persoon alle plichten van de verantwoordelijke op zich moet laden en niet meer de rechten heeft die hem in de zin van de AVG toekomen, dan is hij niet beschermd, moet hij zelf het informatiebeveiligingsbeleid opstellen, verwerkersovereenkomsten sluiten etc. Dat past niet bij de bedoelingen van het wettelijk kader ter bescherming van de betrokkene. De persoon heeft wel zeggenschap over de gegevens in een persoonlijke gezondheidsomgeving, maar niet de volledige macht hierover, inclusief de verantwoordelijkheden zoals hiervoor genoemd. Hij/ zij staat in die zin in ongelijke machtsverhouding ten opzichte van bedrijven, zorgaanbieders en overheden. De Dienstverlener persoon wordt daarom gezien als zelfstandig verwerkingsverantwoordelijke binnen het afsprakenstelsel. Alleen in het geval dat Diensten en Gegevensdiensten via het MedMij Afsprakenstelsel worden geleverd, dient er dus een Deelnemersovereenkomst Dienstverlener Persoon of een

		Deelnemersovereenkomst Dienstverlener Zorgaanbieder met Stichting MedMij te worden afgesloten en kan het zijn dat eventuele bestaande overeenkomsten worden aangepast en/of uitgebreid ter waarborging van de naleving van de afspraken van het MedMij Afsprakenstelsel bij de levering van Diensten via MedMij. Zie voor een nadere uitwerking van de verwerkingsverantwoordelijkheid bij de Diensten en Gegevensdiensten Toelichting verwerkingsverantwoordelijkheid. Gegevens die via MedMij worden uitgewisseld betreffen bijna altijd bijzondere persoonsgegevens. Deelnemers moeten hiervoor voldoen aan de normen die de AVG stelt met betrekking tot het verwerken van deze persoonsgegevens. Deelnemers zijn zelf verantwoordelijk voor de correcte implementatie van de wet. Vanwege het belang van een correcte uitvoering van deze wet door deelnemers aan het MedMij Afsprakenstelsel heeft MedMij een toelichting op de verantwoordelijkheden en normen in de AVG opgenomen. De AP biedt ondersteuning bij de uitvoering van de AVG. Daarnaast kan gebruik worden gemaakt van de 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming' van het Ministerie van Justitie en Veiligheid. De AP heeft tevens een praktijkgids 'Patiëntgegevens in de cloud' uitgegeven. De AP heeft deze praktijkgids uitgegeven omdat het gebruik van de cloud risico's met zich meebrengt.	
Wet op de geneeskundige behandelingsovereenkomst (WGBO)	De Wet op de geneeskundige behandelingsovereenkomst	Zorgaanbieders dienen de wettelijke bepalingen te volgen voor dossiervorming. Een persoonlijke	Zorgd

(geldend vanaf 01-02-2006)	(WGBO) beschrijft de rechten en plichten van patiënten in de zorg. Er is sprake van een geneeskundige behandelingsovereenkomst wanneer een arts een patiënt onderzoekt of behandelt. De wet is bedoeld om de positie te versterken van patiënten die medische zorg nodig hebben. De WGBO regelt onder andere het recht op informatie over de medische situatie, inzage in het medisch dossier, recht op privacy en geheimhouding van medische gegevens (beroepsgeheim).	gezondheidsomgeving is juridisch gezien geen dossier dat valt onder deze dossierplicht. Een Persoon houdt in een persoonlijke gezondheidsomgeving, in aanvulling op het dossier van de zorgaanbieder, vrijwillig gezondheidsdata bij. De Zorgaanbieder is verplicht bij het verstrekken van gegevens vanuit of het opnemen van gegevens in het medisch dossier de identiteit van de Persoon te verifiëren. Binnen het MedMij Afsprakenstelsel zal een derde partij, de Dienstverlener persoon, namens de persoon gegevens ophalen bij de Zorgaanbieder via de Dienstverlener zorgaanbieder. De Persoon zal in die gegevensuitwisseling de Zorgaanbieder toestemming moeten verlenen om de gegevens beschikbaar te stellen aan deze derde partij, de Dienstverlener persoon. De Dienstverlener zorgaanbieder registreert, in opdracht van en volgens instructie van de Zorgaanbieder, de verkregen toestemming van de Persoon om gegevens te delen met de Dienstverlener Persoon. Op grond van de WGBO mogen minderjarigen alleen rechtshandelingen verrichten met toestemming van hun wettelijk vertegenwoordiger. De leeftijdsgrens is in de WGBO op 16 jaar gesteld. Personen vanaf 16 jaar mogen dus zelfstandig beslissen over de medische behandeling. Op het omgaan met de door de Persoon aangeleverde gegevens berusten de plichten van de zorgaanbieder conform 'goed hulpverlenerschap', die nader zijn gedefinieerd in de WGBO, evenals de bepalingen rond dossiervorming en medisch beroepsgeheim. Dat betekent dat de Zorgaanbieder bepaalt welke gegevens uiteindelijk worden

		opgenomen in het medisch dossier en welke actie hierop wordt ondernomen. Bij een persoonlijke gezondheidsomgeving geniet de Persoon niet de bescherming van het medisch beroepsgeheim. In aanvulling op de bestaande privacy wet- en regelgeving wordt daarom binnen het MedMij Afsprakenstelsel van belang geacht om de Persoon tevens bewust te laten zijn van de gevoeligheid van de gezondheidsgegevens. In de Gebruikersvoorlichting zijn hiervoor ondersteunende teksten opgenomen.	
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (geldend vanaf 01-01-2018)	De wet aanvullende bepalingen verwerking persoonsgegevens in de zorg vervangt de wetten gebruik burgerservicenummer in de zorg en de wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg. De wet introduceert rechten en waarborgen voor cliënten bij elektronische gegevensuitwisseling en het beschikbaar stellen van gegevens via elektronische uitwisselingssystemen. Daarnaast verplicht het zorgaanbieders het burgerservicenummer (BSN) van hun patiënten vast te leggen in hun administratie. Met het BSN kan de identiteit van de patiënt zeker worden gesteld. Ook bij het verstrekken van persoonsgegevens met betrekking tot de verlening van, indicatiestelling voor of verzekering van zorg aan andere zorgaanbieders, een indicatieorgaan of aan zorgverzekeraars moet de zorgaanbieder het burgerservicenummer gebruiken.	De Zorgaanbieder, in het BSN-domein, is verplicht bij het verstrekken van gegevens vanuit of het opnemen van gegevens in het medisch dossier de identiteit van de Persoon te verifiëren aan de hand van het BSN. In Nederland wijst het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de digitale identiteitsmiddelen aan die gebruikt kunnen worden voor deze verificatie. Binnen het MedMij Afsprakenstelsel gebruikt de Dienstverlener zorgaanbieder, onder verwerkingsrelatie van de Zorgaanbieder, in verband met de verplichting het BSN te gebruiken, deze hiertoe aangewezen middelen. De Zorgaanbieder is verantwoordelijk voor het bepalen van het betrouwbaarheidsniveau waartegen de identificatie plaatsvindt. Meer informatie voor het bepalen van het juiste betrouwbaarheidsniveau is te vinden in de Handreiking Betrouwbaarheidsniveaus voor digitale dienstverlening en Onderzoek patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg, PrivacyCare en PBLQ, 2016. Binnen het MedMij Afsprakenstelsel wordt gebruik	Zorgd

		Gebruik van het BSN is vastgelegd in een gesloten stelsel. Alleen als er wettelijke gronden zijn voor de verwerking van het BSN, is het gebruik van het BSN toegestaan. Verwerkingsverantwoordelijken bij de overheid en de zorg, inclusief zorgaanbieders, indicatieorganen en zorgverzekeraars mogen – onder voorwaarden – het BSN verwerken. Er is een uitzondering voor verwerkers die optreden namens verwerkingsverantwoordelijken (AVG). Verwerkers mogen, in het kader van hun verwerkersrol, gegevens verwerken ten behoeve van de eerder genoemde verwerkingsverantwoordelijken, waaronder het BSN. In de wet is de bepaling opgenomen dat voor beschikbaarstelling van gegevens via een elektronisch uitwisselingssysteem de Zorgaanbieder voorafgaande toestemming van de betreffende cliënt moet krijgen (art. 15a lid 1). Bij dit alles gaat het om zogenaamde 'gespecificeerde toestemming', dat wil zeggen toestemming voor het beschikbaar stellen van alle of bepaalde gegevens aan bepaalde door de cliënt aan te duiden Zorgaanbieders of categorieën van Zorgaanbieders. Alle (categorieën van) Zorgaanbieders die de Persoon niet expliciet heeft benoemd zijn automatisch uitgesloten om gegevens die beschikbaar zijn gesteld in een elektronisch uitwisselingssysteem, te raadplegen. Ook biedt deze wet een recht op elektronische inzage.	gemaakt van een door BZK aangewezen authenticatiemiddel. Dit middel zorgt voor de verificatie van de identiteit van de Persoon door de Zorgaanbieder. Het gebruik van dit middel is momenteel door BZK niet aan leeftijd gebonden. Dit betekent personen onder de 16 jaar in de zin van de WGBO ook kunnen beschikken over een authenticatiemiddel. Voor personen onder de 16 jaar gelden echter specifieke wettelijke regels. Voor het verstrekken en delen van gegevens aan een minderjarige moet op grond van de WGBO toestemming of een machtiging tot toestemming worden verleend door degene die de ouderlijke verantwoordelijkheid of de wettelijke verantwoordelijkheid voor het kind draagt. Het MedMij Afsprakenstelsel voorziet in het opvragen of delen van gegevens door de Persoon zelf en kent (nog) geen mogelijkheden om (digitaal) toestemming te verkrijgen van een wettelijk vertegenwoordiger of de ouderlijke verantwoordelijke. Er worden daarom voorlopig alleen gegevens en/of gezondheidsinformatie van personen van 16 jaar en ouder verstrekt door of gedeeld met de zorgaanbieder. Dit betekent dat personen jonger dan 16 jaar die inloggen door middel van het door BZK aangewezen middel geen gegevens en/of gezondheidsinformatie ontvangen of delen via het MedMij Afsprakenstelsel. In het geval de Persoon zich voor het eerst tot een Zorgverlener wendt, moet de Zorgverlener bij het eerste fysieke contact het BSN verifiëren. Zie ook artikel 4 en 5 sub a Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Vervolgens valt de interactie tussen de Persoon en zijn Zorgverlener onder het vervolg van de verlening van zorg. Voor dit

	Zowel het recht op gespecificeerde toestemming als het recht op elektronische inzage vergt nog dermate veel aanpassing in bestaande zorg-ict-systemen dat de wetgever vanaf de inwerkingtredingsdatum van deze wet op 1 juli 2017 nog drie jaar de tijd heeft gegeven om aan deze verplichtingen te voldoen.	vervolg van de verlening van zorg mag het BSN worden verwerkt. Op grond van artikel 5 sub b Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg dient de Zorgverlener zich namelijk ook voor het vervolg van een goede zorgverlening zich ervan te vergewissen dat het burgerservicenummer betrekking heeft op de Persoon. De gegevensuitwisseling met een persoonlijke gezondheidsomgeving van de Persoon en de Zorgaanbieder wordt beschouwd als het vervolg van een goede zorgverlening, waarvoor het redelijkerwijs nodig is dat het BSN wordt verwerkt door de Zorgaanbieder bij het verstrekken of opnemen van gegevens. De Dienstverlener persoon heeft geen wettelijke grondslag om het BSN te mogen verwerken en heeft het BSN ter identificatie van de Persoon ook niet nodig. De Dienstverlener persoon is wel verantwoordelijk voor een goede toegangsbeveiliging aan de kant van de Persoon. Wat de afspraken zijn binnen het MedMij Afsprakenstelsel over toegangsbeveiliging en digitale identificatie is toegelicht in Architectuur en technische specificaties evenals in het Normenkader informatiebeveiliging. Voor de uitwisseling van gegevens tussen Zorgaanbieder en de Persoon is geen gespecificeerde toestemming vereist, zoals bedoeld in deze wet. De persoon heeft het recht te mogen beschikken over de over hem/haar vastgelegde gegevens. Wel zal, voortkomend uit de AVG, toestemming moeten zijn verleend door de Persoon aan de Dienstverlener persoon om namens de Persoon gegevens te verwerken en voortkomend uit de

		WGBO toestemming aan de Zorgaanbieder voor het ophalen van gegevens van of het verstrekken van gegevens aan de Dienstverlener persoon, als derde partij in opdracht van de Persoon (zie eerder). Hoe het verlenen van deze toestemming plaatsvindt, is beschreven in Architectuur en technische specificaties. N.B. de set van persoonsgegevens en informatie uit het medisch dossier die de Zorgaanbieder, nadat de Persoon is geïdentificeerd en de Persoon hiervoor zijn toestemming heeft verleend, verstrekt aan de Dienstverlener Persoon, zou mogelijk ook het BSN van de Persoon kunnen behelzen. De verstrekking van het BSN als onderdeel van deze rechtshandeling is niet toegestaan! De Dienstverlener Persoon is immers niet gerechtigd het BSN te verwerken. Het verdient derhalve aanbeveling dat de Zorgaanbieder bij de verstrekking van de gegevens controleert of het BSN uit de gegevensset is verwijderd.	
Toezicht en controle op de naleving	Binnen het zorgaanbiedersdomein zijn verschillende instanties die wettelijk toezicht houden. Dit toezicht op de uitvoering van geldende wet- en regelgeving blijft onverminderd van kracht. Via het afsprakenstelsel wordt slechts aanvullend toezicht gedefinieerd op de specifieke afspraken binnen het MedMij Afsprakenstelsel. De instanties die toezicht houden, zijn: • Autoriteit Persoonsgegevens (AP) - De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor	De Stichting MedMij is verantwoordelijk voor controle op de naleving van de verplichtingen van het MedMij Afsprakenstelsel door de deelnemers. De Stichting MedMij zal niet toezien op de uitvoering van wet- en regelgeving door de deelnemers in het MedMij Afsprakenstelsel. Dit is de verantwoordelijkheid van de genoemde toezichthouders. Het MedMij Afsprakenstelsel betreffen aanvullende afspraken op wet- en regelgeving, vastgelegd in een privaatrechtelijke overeenkomst tussen de deelnemer en de Stichting MedMij. Overtredingen van de wet- en regelgeving	Zorgd

	bescherming van persoonsgegevens en adviseert over nieuwe regelgeving; • Autoriteit Consument en Markt (ACM) - De Autoriteit Consument en Markt houdt toezicht op de mededinging, een aantal specifieke sectoren en het consumentenrecht. De ACM zet zich in voor een gelijk speelveld met bedrijven die zich aan de regels houden, en goed geïnformeerde consumenten die voor hun recht opkomen; • Inspectie Gezondheidszorg en Jeugd (IGJ) - De Inspectie Gezondheidszorg en Jeugd is onafhankelijk toezichthouder in de Nederlandse gezondheidszorg. Door toezicht, handhaving en opsporing van strafbare feiten bewaken en bevorderen zij de veiligheid en kwaliteit van zorg; • Nederlandse Zorgautoriteit (NZa) - De Nederlandse Zorgautoriteit zet zich in voor goede en betaalbare zorg die beschikbaar is als je die nodig hebt. Vanuit dat perspectief maakt de NZa regels en houdt zij toezicht op zorgaanbieders en zorgverzekeraars; • Working Party op grond van artikel 29 van de Europese richtlijn (alle toezichthouders op persoonsgegevens in Europa gezamenlijk, in Nederland AP) - De Working Party geeft ‘Opinions’ hoe de wet geïnterpreteerd moet worden. Zoals de interpretatie van	kunnen wel gevolgen hebben voor de positie van de Deelnemer in het MedMij Afsprakenstelsel.

	voorwaarden voor anonimiseren, certificeren en PIA's.		
Verordening (EU) 2017/745 van het Europees parlement en de Raad betreffende medische hulpmiddelen (gepubliceerd 05-04-2017, geldend vanaf 26-05-2020)	Deze verordening heeft tot doel het soepel functioneren van de interne markt voor medische hulpmiddelen te garanderen, uitgaande van een hoog beschermingsniveau voor de gezondheid van patiënten en gebruikers, en rekening houdend met de kleine en middelgrote ondernemingen die in deze sector actief zijn. Tegelijkertijd stelt deze verordening hoge kwaliteits- en veiligheidseisen aan medische hulpmiddelen, teneinde tegemoet te komen aan gemeenschappelijke veiligheidsbezwaren ten aanzien van dergelijke producten. Beide doelstellingen worden gelijktijdig nagestreefd en zijn onlosmakelijk met elkaar verbonden waarbij de ene niet ondergeschikt is aan de andere.	De Inspectie Gezondheidszorg en Jeugd beschrijft op haar eigen website de toepassing van de verordening. Daarbij geeft de IGJ aan dat "de nieuwe regelgeving omvat veel (met name technische) zaken die de komende tijd nog nader worden uitgewerkt door de Europese Commissie en de lidstaten van de EU". Vanuit het MedMij Afsprakenstelsel worden geen aanvullende zaken geregeld met betrekking tot medische hulpmiddelen. Deelnemers dienen zelf een afweging te maken met betrekking tot de toepassing van deze verordening voor hun eigen dienstverlening.	Zorgd
Aanpassingswet richtlijn inzake elektronische handel (geldend vanaf 30-06-2014)	Met deze wet wordt de Richtlijn inzake elektronische handel geïmplementeerd. Deze richtlijn heeft tot doel om bij te dragen aan de goede werking van de interne markt door het vrije verkeer van diensten van de informatiemaatschappij tussen de lidstaten te waarborgen. Dit wordt gerealiseerd door belemmeringen voor de elektronische handel weg te nemen.	Vanuit het MedMij Afsprakenstelsel worden geen aanvullende zaken geregeld met betrekking tot deze aanpassingswet. Deelnemers dienen zelf een afweging te maken met betrekking tot de invulling van deze aanpassingswet voor hun eigen dienstverlening.	Alle domei
Implementatiewet richtlijn consumentenrechten (geldend vanaf 13-06-2014)	Deze wet implementeert de richtlijn consumentenrechten. Met deze wet wordt consumenteninformatie voor verkoop in de winkel, op afstand (via onder andere internet en telefoon) en buiten	Vanuit het MedMij Afsprakenstelsel worden geen aanvullende zaken geregeld met betrekking tot deze implementatiewet. Deelnemers dienen zelf een afweging te maken met betrekking tot de invulling van	Alle domei

	verkoopruimten (bijvoorbeeld colportage) geregeld. Ook wordt er voor verkoop op afstand en buiten verkoopruimten het herroepingsrecht (bedenktijd voor de consument) geregeld.	deze implementatiewet voor hun eigen dienstverlening.	
Wet gelijke behandeling op grond van handicap en chronische ziekte (wgbh/cz) (geldend vanaf 03-04-2003)	De wet gelijke behandeling op grond van handicap en chronische ziekte (wgbh/cz) is ook van toepassing op digitale goederen en diensten. Dit houdt in dat aanbieders van goederen en diensten gehouden zijn om doeltreffende aanpassingen te verrichten (art. 2) en geleidelijk toe te werken naar algemene toegankelijkheid (art. 2a), mits dit geen onevenredige belasting vormt. Het Besluit Toegankelijkheid licht toe dat sectoren werk kunnen maken van de stap naar algemene toegankelijkheid via actieplannen.	Vanuit het MedMij Afsprakenstelsel worden geen aanvullende zaken geregeld met betrekking tot deze aanpassingswet. Deelnemers dienen zelf een afweging te maken met betrekking tot de invulling van deze wet voor hun eigen dienstverlening. Het advies in algemene zin is: ga als ontwikkelaar van digitale goederen en diensten, waaronder ook de deelnemers in het MedMij afsprakenstelsel vallen, vooral ook het gesprek aan met gebruikersgroepen waarin gebruikers met een beperking vertegenwoordigd zijn. Om in dialoog te bepalen welke ontwerpbepalingen je kunt meenemen. Vaak kom je in die dialoog vanzelf ook tot de evenredige aanpassingen, die je bovendien dan vanaf de start kunt meenemen. Handvatten/concreet stappenplan voor uitvoering: https://www.digitoegankelijk.nl/onderwerpen/stappenplan-toegankelijkheid De verplicht te gebruiken schermen voor de toestemmings- en bevestigingsverklaring binnen het afsprakenstelsel in de usecases voor verzamelen en delen (architectuur en technische specificaties) zijn toegankelijk gemaakt conform de bepalingen in deze wet. Hetzelfde geldt voor de schermen van een door BZK aangewezen authenticatiemiddel.	Zorgd
Aansprakelijkheid	Voor de aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en	Binnen het MedMij Afsprakenstelsel is iedere deelnemer aansprakelijk voor zijn eigen handelen en/of nalaten	Alle domei

	omvang van wettelijke verplichtingen tot schadevergoeding. Aansprakelijkheid kan voortvloeien uit het niet nakomen van een wettelijke verplichting en/of het niet betrachten van de nodige zorgvuldigheid die gelet op de omstandigheden van het geval redelijkerwijs van de desbetreffende partij kan worden verwacht. • Bij het 'niet nakomen van een wettelijke verplichting' gaat het bijvoorbeeld om de niet naleving van de voor de deelnemer van toepassing zijnde (specifieke) wet- en regelgeving omtrent privacy en informatiebeveiliging. • Bij het 'betrachten van de nodige zorgvuldigheid' gaat het dan bijvoorbeeld om de inrichting van processen die ervoor zorgen dat aan de eisen die voor de deelnemer in het MedMij Afsprakenstelsel zijn opgenomen wordt voldaan en deze ook worden nageleefd.	binnen de rol die hij vervult. De deelnemers mogen en kunnen niet afwijken van de algemene regels van het Nederlands recht. Hoe deze regels in een concreet geval uitwerken, is afhankelijk van de feiten en de omstandigheden van het geval. De aansprakelijkheid is voor Deelnemers in ieder geval uitdrukkelijk beperkt tot het eigen handelen van de Deelnemer. Hiermee wordt voorkomen dat een Deelnemer aansprakelijk zou worden gesteld voor gevallen waarbij schade optreedt die niet door hem is veroorzaakt of aan hem is toe te rekenen.	

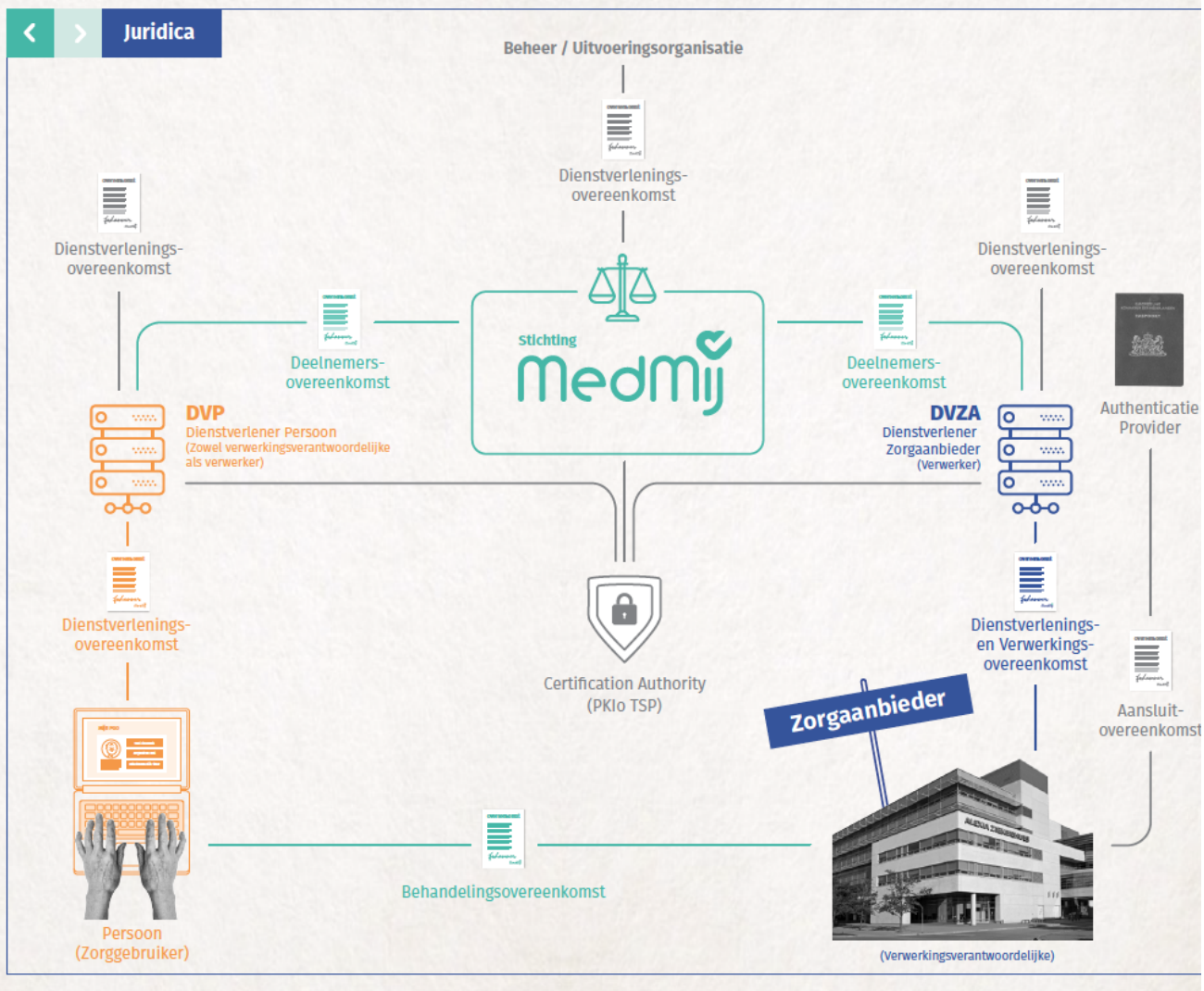
Overeenkomsten en rechtsrelaties

> Overeenkomsten en rechtsrelaties is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moet deze pagina herzien worden. Er moet dan een generieke tekst geschreven worden, of per domein wordt een tekst opgesteld.

MedMij maakt onderscheid tussen het *Persoonsdomein (oranje)* en het *Zorgaanbiedersdomein (blauw)*. Binnen de context van MedMij valt de verwerking van persoonsgegevens in het *Zorgaanbiedersdomein* onder de verwerkingsverantwoordelijkheid van de *Zorgaanbieder*. In dit domein is het verwerken van het BSN is voor de identificatie van personen wettelijk verplicht. In het *Persoonsdomein* valt de verwerking van persoonsgegevens onder de verwerkingsverantwoordelijkheid van de Dienstverlener Persoon (DVP). De DVP heeft, sec in zijn MedMij rol, geen wettelijke grondslag voor het verwerken van het BSN.

In beide domeinen definieert MedMij een aantal rollen. MedMij verbindt deze rollen, en daarmee de domeinen, door alle voor gegevensuitwisseling benodigde afspraken vast te leggen in deelnemersovereenkomsten en in het MedMij afsprakenstelsel. Een partij die in MedMij een rol speelt is altijd volledig verantwoordelijk voor de juiste uitvoering van die rol. Partijen kunnen verantwoordelijkheden niet verschuiven tussen rollen, wel mag gebruik gemaakt worden van onderaannemers (verwerkers). Voor onderaannemers blijft de verantwoordelijke aansprakelijk.

Alle rechtsrelaties zijn privaatrechtelijk van aard en alle deelnemers zijn gebonden aan het Nederlands recht. De figuur hieronder geeft de verschillende rechtsrelaties weer, de relaties en actoren worden later in dit hoofdstuk toegelicht. De gebruikte kleuren zijn in lijn met de huisstijl in de architectuur van het MedMij Afsprakenstelsel: In oranje de rollen en relaties in het Persoonsdomein; In blauw de rollen en relaties in het Zorgaanbiedersdomein; In groen de rollen en relaties tussen de twee domeinen.



Het MedMij Afsprakenstelsel waarborgt dat binnen het MedMij-netwerk op een veilige en betrouwbare manier persoonsgegevens en/of gezondheidsinformatie tussen de partijen (zoals Zorggebruikers, dienstverleners en zorgaanbieders) worden uitgewisseld. Om dit te bewerkstelligen behelst het MedMij Afsprakenstelsel informatiestandaarden, technische, organisatorische en juridische afspraken. Als gevolg van het afsluiten van de Deelnemersovereenkomst tussen Dienstverleners en de Stichting MedMij - nadat hiertoe de toetredingsprocedure succesvol is doorlopen - worden de Dienstverleners Zorgaanbieder en Dienstverleners Persoon *Deelnemer* van het MedMij Afsprakenstelsel. Iedere partij die aantoonbaar voldoet aan de afspraken van het MedMij Afsprakenstelsel kan toetreden en Deelnemer worden van het MedMij Afsprakenstelsel. Als onderdeel van het toetredingsproces zijn Deelnemers tevens gehouden de Zelfverklaring integriteit te overleggen.

Als Deelnemer van het MedMij Afsprakenstelsel committeren partijen zich aan de naleving van de verplichtingen en afspraken die voor hun rol uit het MedMij Afsprakenstelsel voortvloeien. Deelnemers mogen op basis van de Deelnemersovereenkomst hun Diensten leveren aan *Gebruikers* (personen die een PGO gebruiken, maar ook zorgaanbieders) onder de merknaam MedMij. Om *Diensten* via het MedMij-netwerk te kunnen leveren zijn Deelnemers toegetreden tot het MedMij Afsprakenstelsel.

De Persoon en de Zorgaanbieder zijn Gebruikers van Diensten van Deelnemers in het MedMij Afsprakenstelsel.

De Deelnemers zijn zelf verantwoordelijk voor het afsluiten van dienstverleningsovereenkomsten met hun Gebruikers. Deelnemers zijn immers zelf verantwoordelijk voor de veilige en betrouwbare werking van de Diensten die zij aanbieden. Om ervoor te zorgen dat dienstverleningsovereenkomsten tussen de Deelnemers en Gebruikers goed aansluiten op de Diensten die, met inzet van het MedMij-netwerk, worden geleverd, worden vanuit het MedMij Afsprakenstelsel voorbeelden ter beschikking gesteld die door de Deelnemer kan worden gebruikt bij het afsluiten van de dienstverleningsovereenkomst met de Gebruiker. Overige voorbeelden van informatie die via het MedMij Afsprakenstelsel voor Deelnemers ter beschikking zijn gesteld zijn:
- de Gebruiksvoorlichting persoonsdomein,
- Gebruiksvoorlichting zorgdomein en de
- Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener Zorgaanbieder.

De *Persoon* als *Gebruiker* heeft vrije keuze welke persoonlijke gezondheidsomgeving (PGO) hij of zij gebruikt. Op de website van MedMij is een lijst met alle Deelnemers gepubliceerd.

Overzicht van partijen en rechtsrelaties

Bij de uitwisseling van (persoons)gegevens en gezondheidsinformatie tussen Gebruikers via het MedMij-netwerk worden verschillende partijen onderscheiden die zich weer in verschillende rechtsrelaties tot elkaar verhouden. In de architectuur en technische specificaties van het MedMij Afsprakenstelsel is uitgewerkt welke rollen de partijen (Gebruikers en Deelnemers) vervullen, de functies die zij op de verschillende architectuurlagen vervullen, alsmede welke gegevens zij met elkaar uitwisselen.

Om de verantwoordelijkheden binnen het proces van de uitwisseling van gezondheidsgegevens binnen het MedMij-netwerk inzichtelijk te maken, is hieronder vanuit juridisch perspectief een overzicht van de rechtsrelaties tussen de verschillende partijen opgenomen die een rol spelen binnen het MedMij Afsprakenstelsel. De uitwerking van het MedMij Afsprakenstel gaat uit van de volgende rollen en actoren:

1. de Stichting MedMij als eindverantwoordelijke voor het MedMij Afsprakenstelsel;
2. de Beheerorganisatie en/of uitvoeringsorganisatie die in opdracht van de Stichting zorgdraagt voor het beheer van het MedMij Afsprakenstelsel;
3. de Deelnemer Dienstverlener Zorgaanbieder die binnen de kaders van het MedMij Afsprakenstelsel Diensten aanbiedt aan de Zorgaanbieder;
4. de Deelnemer Dienstverlener Persoon die binnen de kaders van het MedMij Afsprakenstelsel Diensten aanbiedt aan de Persoon;
5. de Zorgaanbieder die Diensten afneemt van de Dienstverlener Zorgaanbieder;
6. de Persoon als Gebruiker die Diensten afneemt van de Dienstverlener Persoon;
7. de Persoon als Zorggebruiker die gebruik maakt van de diensten van een zorgaanbieder;
8. de Authenticatieprovider die een Zorggebruiker (Persoon) onder verantwoordelijkheid van een Zorgaanbieder authentiseert, en
9. De Certification Authority die authenticatiemiddelen verstrekt aan Deelnemers en voor de Stichting MedMij.

Rechtsrelaties MedMij Afsprakenstelsel

Hieronder is het overzicht opgenomen van rechtsrelaties tussen de rollen/actoren waarop het MedMij Afsprakenstelsel van toepassing is met verwijzing naar de overeenkomsten in het MedMij Afsprakenstelsel.

Het uitgangspunt van het MedMij Afsprakenstelsel is dat Deelnemers (dus Dienstverlener Zorgaanbieder en Dienstverlener Persoon) als tussenpersoon fungeren voor interacties tussen Zorggebruikers en Zorgaanbieders. Dit houdt in dat de Deelnemers in opdracht van respectievelijk de Persoon en de Zorgaanbieder de gegevensuitwisseling tussen de Persoon en de Zorgaanbieder verzorgen. De Diensten die in het kader van deze opdrachtverlening via het MedMij-netwerk worden geleverd bestrijken de contractuele relaties van het Afsprakenstelsel MedMij.

Rechtsrelaties binnen MedMij	Type overeenkomst
1. Stichting MedMij - Dienstverlener Persoon	Deelnemersovereenkomst Dienstverlener Persoon
2. Stichting MedMij - Dienstverlener Zorgaanbieder	Deelnemersovereenkomst Dienstverlener Zorgaanbieder

De Deelnemersovereenkomst Dienstverlener persoon en de Deelnemersovereenkomst Dienstverlener zorgaanbieder bevatten de basisafspraken tussen Stichting MedMij en de Dienstverlener persoon respectievelijk de Dienstverlener zorgaanbieder. De Deelnemersovereenkomst is voor alle Deelnemers in dezelfde rol gelijk en zorgt ervoor dat Deelnemers gehouden zijn de op hen rustende verantwoordelijkheden te nemen en verplichtingen en afspraken uit het MedMij Afsprakenstelsel zorgvuldig uit te voeren en aantoonbaar na te leven. Ook bindt de overeenkomst Deelnemers aan de besturingsafspraken die noodzakelijk zijn voor het borgen van het vertrouwen in MedMij. Deelnemers mogen binnen MedMij in hun rol alleen Diensten verrichten indien zij een Deelnemersovereenkomst hebben gesloten met de Stichting MedMij. Het onderlinge vertrouwen tussen partijen bij het gebruik van MedMij is (mede) gebaseerd op de overeenkomsten die Deelnemers en de Stichting MedMij ten aanzien van het nakomen van de afspraken in het MedMij Afsprakenstelsel. De Deelnemers zijn verantwoordelijk voor de doorvertaling van de afspraken naar hun klanten (Gebruikers) en eventueel derden (onderaannemers, verwerkers). De Deelnemers zijn, binnen de kaders van het MedMij Afsprakenstelsel, vrij om zelf in een overeenkomst met de Gebruiker nadere afspraken te maken over de inhoud en de omvang van hun dienstverlening.

Overige rechtsrelaties

Hieronder is een tabel opgenomen van mogelijke rechtsrelaties die van wezenlijke invloed zijn op het vertrouwen in een veilige en betrouwbare verwerking van en gegevensuitwisseling via het MedMij Afsprakenstelsel. Onder de tabel zijn deze relaties verder beschreven. Deze rechtsrelaties zijn van belang omdat in het technische ontwerp en de architectuur van het MedMij Netwerk componenten zijn opgenomen waarbij partijen in deze rechtsrelaties een uitvoerende verplichting hebben. Dat betekent dat afspraken tussen deze partijen ook randvoorwaardelijk zijn voor een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de persoonlijke gezondheidsomgeving en de informatiesystemen van de Zorgaanbieders.

Rechtsrelaties die van belang zijn voor MedMij	Type overeenkomst
I. Stichting MedMij - Beheer /uitvoeringsorganisatie	Opdrachtverlening voor ondersteuning en uitvoering van taken van Stichting MedMij
II. Dienstverlener Persoon –Gebruiker	Dienstverleningsovereenkomst Persoon.
III. Zorgaanbieder - Persoon als Zorggebruiker	Behandelingsovereenkomst
IIV. Dienstverlener Zorgaanbieder – Persoon als Zorggebruiker	Toestemming (Wabvpz)
V. Zorgaanbieder – Dienstverlener Zorgaanbieder	Verwerkersovereenkomst en Dienstverleningsovereenkomst
VI. Zorgaanbieder – Authenticatieprovider	Dienstverleningsovereenkomst
	Dienstverleningsovereenkomst

VII. Dienstverlener Zorgaanbieder – Certification Authority	
VIII. Dienstverlener Persoon – Certification Authority	Dienstverleningsovereenkomst
IX. Stichting MedMij – Certification Authority	Dienstverleningsovereenkomst

De rechtsrelaties genoemd onder I t/m IX zijn additioneel ten aanzien van de overeenkomsten die moeten worden afgesloten voor toetreding tot het MedMij Afsprakenstelsel maar dienen dus - voor het vertrouwen en een betrouwbare en veilige werking van het MedMij Afspakenstelsel - tussen de betrokken partijen te worden afgesloten. Partijen zijn echter zelf verantwoordelijk voor het afsluiten van deze overeenkomsten. Hieronder volgt een toelichting op de relaties.

I. Stichting MedMij - Beheer /uitvoeringsorganisatie

Stichting MedMij heeft een overeenkomst met een of meer *Beheer /uitvoeringsorganisaties.* Dit gebeurt op basis van opdrachtstrekking voor ondersteuning en uitvoering van taken voor Stichting MedMij zoals:

1. De instandhouding van de goede technische werking van de gemeenschappelijke voorzieningen in het afsprakenstelsel.
2. Het beheer van het MedMij Afsprakenstelsel.
3. Administratie van Deelnemers
4. Acceptatie van Deelnemers

II. Dienstverlener Persoon – Gebruiker

De *Gebruiker* heeft een *Dienstverlenersovereenkomst* met de *Dienstverlener Persoon*. Binnen het MedMij Afsprakenstelsel wordt voor deze rechtsrelatie de Gebruiksvoorlichting persoonsdomein ter beschikking gesteld.

III. Zorgaanbieder - Persoon als Zorggebruiker

De *Zorggebruiker* heeft of had een behandelingsovereenkomst met de *Zorgaanbieder* en is dus het onderwerp van de dossiervoering van deze *Zorgaanbieder*.

IV. Zorgaanbieder –Persoon als Gebruiker

De *Gebruiker* moet *toestemming* geven aan de *Zorgaanbieder* voordat de *Zorgaanbieder* gegevens mag verstrekken aan de *Dienstverlener Persoon* die betrekking hebben op de *Gebruiker.*

V. Zorgaanbieder – Dienstverlener Zorgaanbieder

Veelal zullen de *Zorgaanbieder* en *Dienstverlener Zorgaanbieder* verschillende partijen zijn waarbij de *Zorgaanbieder* verwerkingsverantwoordelijk is en de *Dienstverlener Zorgaanbieder* verwerker. De afspraken rondom de verwerking van persoonsgegevens door een Verwerker dienen geregeld te zijn in een schriftelijke overeenkomst tussen Verwerker en Verwerkingsverantwoordelijke. De meeste Dienstverleners zorgaanbieder zullen al een dergelijke verwerkersovereenkomst hebben met de Zorgaanbieder. Voor de specifieke MedMij-aspecten is daarvoor de Modelverwerkersovereenkomst te gebruiken. In het geval er al een bestaande overeenkomst is afgesloten tussen Verwerker en Verwerkingsverantwoordelijke kunnen Partijen kunnen ervoor kiezen de specifieke bepalingen in relatie tot de verwerking van persoonsgegevens voor MedMij uit de Modelverwerkersovereenkomst te integreren in een bestaande verwerkersovereenkomst of een andere modeloverkomst die veel sectoren hebben. Hierbij valt te denken

aan zaken zoals het in opdracht van de verantwoordelijke verwerken van het burgerservicenummer, het verkrijgen van toestemming van de Persoon voor het verstrekken van gegevens aan een derde partij, namelijk de Dienstverlener persoon, het verwerken van persoonsgegevens ten behoeve van de gegevensuitwisseling (zoals logging) en de verwerking van de betreffende persoonsgegevens zelf.

VI. Zorgaanbieder –Authenticatieprovider

De *Dienstverlener Zorgaanbieder* moet, ten behoeve van haar dienstverlening aan de *Zorgaanbieder*, de identiteit van de *Gebruiker* vaststellen en heeft daarvoor een *Authenticatieprovider* nodig. De *Zorgaanbieder* en/of de *Dienstverlener Zorgaanbieder* kunnen daarvoor een overeenkomst aangaan met een *Authenticatieprovider*.

VII. Dienstverlener Zorgaanbieder – Certification Authority

Dienstverleners Zorgaanbieder moeten zich kunnen authentiseren bij *stichting MedMij* en bij *Dienstverleners Persoon*. Hiervoor dienen zij een authenticatiemiddel (certificaat) van een *Certification Authority* te betrekken.

VIII. Dienstverlener Persoon – Certification Authority

Dienstverleners Persoon moeten zich kunnen authentiseren bij stichting MedMij en bij *Dienstverleners Zorgaanbieder*. Hiervoor dienen zij een authenticatiemiddel (certificaat) van een *Certification Authority* te betrekken.

IX. Stichting MedMij – Certification Authority

*Stichting MedMi*j moet zich kunnen authentiseren bij *Dienstverleners Zorgaanbieder* en bij *Dienstverleners Persoon*. Hiervoor dient zij een authenticatiemiddel (certificaat) van een *Certification Authority* te betrekken.

Toelichting verwerkingsverantwoordelijkheid

Inleiding

> Toelichting verwerkingsverantwoordelijkheid is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moet deze pagina herzien worden. Er moet dan een generieke tekst geschreven worden, of per domein wordt een tekst opgesteld.

Het MedMij Afsprakenstelsel onderscheidt om te beginnen twee functies voor de gegevensuitwisseling tussen de *Persoon* en zijn *Aanbieder*, namelijk de functies Verzamelen en Delen. Met de functie Verzamelen kan de *Persoon* zijn gegevens en gezondheidsinformatie in zijn PGO inkijken, opslaan en beheren. Met de functie *Delen* kan de *Persoon* gegevens en gezondheidsinformatie vanuit zijn PGO aan zijn *Aanbieder* aanbieden, opdat de *Aanbieder* deze informatie kan opnemen in zijn medisch dossier.

Daarnaast is er de functie *Abonneren*, waarmee *Persoon* en *Aanbieder* kunnen afspreken dat de *Aanbieder* gedurende een zekere looptijd meldingen kan doen bij de PGO over wijzigingen in beschikbare gezondheidsgegevens. Die meldingen heten *Notificaties*. Na het afspreken van zo'n abonnement gebruiken partijen de functie *Notificeren* voor het uitwisselen van die meldingen.

In de uitvoering van de functies *Verzamelen* en *Delen* zijn verschillende rollen betrokken. Hieronder wordt voor de voornoemde functies uitgewerkt welke partij waar in het proces welke (verwerkings) verantwoordelijkheid heeft gelet op de (specifieke) privacy wet- en regelgeving die op betrokken partijen van toepassing is.

Authenticatie

Voor de functies Verzamelen, Delen en Abonneren geldt dat in het geval de *Persoon* gegevens en/of gezondheidsinformatie met zijn *Aanbieder* wil uitwisselen, of een abonnement aangaat, de *Zorgaanbieder* de *Persoon* altijd eerst moet identificeren en authenticeren. Zoals ook in het Juridisch kader is aangeven wordt hiervoor binnen het MedMij Afsprakenstelsel gebruik gemaakt van een door het ministerie van BZK aangewezen authenticatiemiddel. Het identificatie- en authenticatieproces geschiedt onder de verantwoordelijkheid van de *Zorgaanbieder*. De *Zorgaanbieder* is immers op grond van de artikelen 4, 5 en 6 van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, in het kader van het verlenen van zorg, verplicht de identiteit van de patiënt vast te stellen. Hiervoor mag op basis van deze wet het BSN door de *Zorgaanbieder* worden verwerkt. De interactie tussen de *Persoon* en zijn *Zorgaanbieder* via het MedMij Afsprakenstelsel wordt beschouwd als een handeling die valt onder (het vervolg van) de verlening van zorg. Hiervoor mag dan ook het BSN worden verwerkt. In het licht van de AVG betekent dit dat het de *Zorgaanbieder* is toegestaan om het BSN te verwerken op grond van art. 87 AVG en 46 Uitvoeringswet AVG. De rechtmatigheidsgrondslag voor de verwerking van het BSN op grond van de AVG is hiermee de uitvoering van een wettelijke verplichting die op de *Zorgaanbieder* als verwerkingsverantwoordelijke rust (art. 6 lid 1 sub c AVG).

De *Zorgaanbieder* maakt in het authenticatieproces van de *Persoon* — die via MedMij gegevens /gezondheidsinformatie met zijn Zorgaanbieder wil delen — gebruik van een verwerker: de *Dienstverlener zorgaanbieder*. Deze *Dienstverlener zorgaanbieder* heeft enerzijds — om als *Deelnemer* in het MedMij Afsprakenstelsel zijn *Diensten* aan de *Zorgaanbieder* te mogen aanbieden — een *Deelnemersovereenkomst* met de Stichting MedMij gesloten. Anderzijds heeft deze *Dienstverlener zorgaanbieder* een verwerkersovereenkomst met de *Zorgaanbieder* gesloten. Op basis van deze verwerkersovereenkomst zorgt hij feitelijk voor, weliswaar namens, onder controle en in opdracht van de *Zorgaanbieder,* de authenticatie van de *Persoon.* Deze verwerkersovereenkomst rechtvaardigt de verwerking van de gegevens, gezondheidsinformatie en het BSN door de *Dienstverlener zorgaanbieder* in de rol van verwerker. De *Dienstverlener zorgaanbieder* wordt in zijn rol als verwerker beschouwd als de feitelijk beheerder van het

medisch dossier die namens de *Zorgaanbieder* handelt en waarover de *Zorgaanbieder* als verwerkingsverantwoordelijke controle heeft (via de verwerkersovereenkomst). Voor deze situatie geldt het zogenoemde afgeleid beroepsgeheim. Dit houdt in dat de *Zorgaanbieder* aansprakelijk is als door de *Dienstverlener zorgaanbieder* in strijd met de geheimhoudingsplicht gegevens worden verwerkt. Vanwege het feit dat in de relatie tussen de *Dienstverlener zorgaanbieder* en de *Zorgaanbieder* het afgeleide beroepsgeheim geldt en de verwerkingsverantwoordelijke hier op kan worden aangesproken wordt de *Dienstverlener zorgaanbieder* hiermee als rechtstreeks betrokkene in de zin van art. 7:457 BW beschouwd . Voor deze situatie hoeft op grond van art 7:457 BW geen toestemming door de patiënt te worden gegeven.

Met het oog op authenticatie handelt de *Persoon* dus rechtstreeks (via de *Dienstverlener zorgaanbieder* als verwerker) met de *Zorgaanbieder.* Als hij gegevens wenst uit te wisselen met zijn *Zorgaanbieder,* dient de *Persoon* zich eerst te authenticeren bij zijn *Zorgaanbieder.* Met deze rechtstreekse relatie wordt gewaarborgd dat de *Dienstverlener persoon* nimmer de beschikking heeft over het BSN en/of informatie ten behoeve van de authenticatie van de *Persoon,* anders dan de terugkoppeling van de *Zorgaanbieder* (via de *Dienstverlener zorgaanbieder*) dat de *Persoon* wel of geen gegevens kan uitwisselen met de desbetreffende *Zorgaanbieder.* Identificatie en authenticatie van de *Persoon* is derhalve een aparte rechtstreekse rechtshandeling tussen de *Zorgaanbieder* (via de *Dienstverlener zorgaanbieder*) en de *Persoon.* Zonder deze identificatie en authenticatie worden er geen gegevens uitgewisseld. Pas nadat de identificatie en authenticatie heeft plaatsgevonden, kan de gegevensuitwisseling in het kader van MedMij plaatsvinden. Deze gegevensuitwisseling die op het authenticatieproces volgt, is een rechtshandeling tussen enerzijds de *Dienstverlener persoon* en de *Persoon* en de *Dienstverlener persoon* en de *Zorgaanbieder* anderzijds. In deze rechtshandeling vindt de uitwisseling van de gegevens over de gezondheid plaats op basis van uitdrukkelijke toestemming van de *Persoon.* Zie hiervoor ook onderstaande paragraaf UC Verzamelen en UC Delen.

UC Verzamelen en *UC Delen*

Toestemming aan de *Dienstverlener persoon* voor verstrekking

Zowel voor de use case Delen als de use case Verzamelen dient de *Dienstverlener persoon* op basis van de AVG toestemming te hebben voor de verwerking van de gegevens over de gezondheid van de *Persoon.* Om ervoor te zorgen dat de *Persoon* met gebruik van zijn PGO via het MedMij-netwerk gegevens kan uitwisselen en zijn gegevens en gezondheidsinformatie in zijn PGO kan beheren, sluit de *Persoon* een overeenkomst met de *Dienstverlener persoon*. Deze *Dienstverlener persoon* handelt — nadat identificatie en authenticatie tussen de *Persoon* en de *Zorgaanbieder* heeft plaatsgevonden — op basis van deze dienstverleningsovereenkomst namens de *Persoon* bij de gegevensuitwisseling tussen de *Persoon* en de *Zorgaanbieder.* In het licht van de AVG is de *Dienstverlener persoon* hiermee de verwerkingsverantwoordelijke in de uitvoering van de dienstverleningsovereenkomst waarbij de *Persoon* via de PGO MedMij persoonsgegevens/gezondheidsinformatie deelt of uitwisselt met zijn *Zorgaanbieder.* De rechtmatigheidsgrondslag 'noodzakelijk voor de uitvoering van de overeenkomst' (art. 6 lid 1 sub b AVG) is van toepassing voor de verwerking van de gewone persoonsgegevens in relatie tot de dienstverleningsovereenkomst die tussen de *Dienstverlener persoon* en de *Persoon* wordt afgesloten. Daarnaast is de rechtmatigheidsgrondslag 'uitdrukkelijke toestemming' (art 9 lid 2 sub a AVG) van toepassing voor de verwerking van de gegevens over de gezondheid van *Persoon* (bijzonder persoonsgegeven) in relatie tot de PGO. Vorenstaande betekent dat de *Dienstverlener persoon* zowel in relatie tot de use case Verzamelen als de use case Delen als verwerkingsverantwoordelijke de expliciete toestemming van de *Persoon* moet hebben alvorens de Persoon gebruik maakt van zijn PGO.

Op grond van de artikelen 7 en 8 AVG moet de *Dienstverlener persoon* als verwerkingsverantwoordelijke in relatie tot 'toestemming' voor de gegevensuitwisseling via de PGO het volgende kunnen aantonen:

a. dat en waarvoor de *Persoon* toestemming heeft verleend;

b. dat de toestemming vrijelijk, specifiek, geïnformeerd en ondubbelzinnig is gegeven, en

c. wie de verwerkingsverantwoordelijke is, wat de specifieke doeleinden/ het specifieke doel van de verwerking is, wie de ontvangers van de persoonsgegevens zijn en het recht om de toestemming te allen tijde in te trekken.

Om dit te kunnen aantonen, zal de *Dienstverlener persoon* een verklaring van toestemming moeten opstellen. Deze verklaring dient in een begrijpelijke, gemakkelijke, toegankelijke vorm en in duidelijke taal te worden opgesteld. Bij het geven van de toestemming moet om een actieve handeling van de *Persoon* gaan. De voornoemde informatie in relatie tot toestemming zal voorafgaand aan het daadwerkelijk geven van de toestemming moeten zijn verstrekt. Ook dit zal door de *Dienstverlener persoon* moeten kunnen worden aangetoond.

Toestemming aan de *Zorgaanbieder* voor verstrekking

Zowel voor de use case Delen als de use case Verzamelen dient de *Persoon* voor een rechtmatige uitwisseling van gegevens over zijn gezondheid zijn toestemming ook aan de *Zorgaanbieder* te hebben verleend. Deze toestemming heeft betrekking op de situatie dat de *Dienstverlener persoon* de gegevens die hij — via het MedMij-netwerk (door middel van de *Dienstverlener zorgaanbieder)* en na de authenticatie van de *Persoon* door de *Zorgaanbieder* — over de *Persoon* van de *Zorgaanbieder* ontvangt ook rechtmatig verwerkt. Deze toestemming vloeit voort uit de WGBO. Op basis van artikel 7: 457 BW mogen gegevens uit het medisch dossier immers niet met 'anderen' worden gedeeld, tenzij de patient hiervoor zijn toestemming heeft gegeven. De *Dienstverlener persoon* aan wie de *Zorgaanbieder* gegevens over de *Persoon* verstrekt ten behoeve van de PGO wordt als een 'ander' in de zin van de WGBO beschouwd. Voor deze specifieke situatie is een toestemmingsverklaring in het MedMij Afsprakenstelsel opgenomen, en wel in de use cases Verzamelen en Abonneren. In het geval van de use case Abonneren zijn het *Notificaties* die de gezondheidsgegevens vormen.

Rechtmatigheidsgrondslag *Zorgaanbieder* ontvangen

Tot slot nog de grondslag voor de *Zorgaanbieder* als verwerkingsverantwoordelijke om gezondheidsgegevens van de *Persoon* te ontvangen bij de use case Delen. Bij de use case Delen wordt op initiatief van de *Persoon* (door middel van de *Dienstverlener persoon)* persoonsgegevens en/of gegevens over de gezondheid van de *Persoon* (door middel van de *Dienstverlener zorgaanbieder)* aan de *Zorgaanbieder* aangeboden met het verzoek deze informatie op te nemen in het medisch dossier. De rechtmatigheidsgrondslag voor de verwerking van deze gegevens vloeit voort uit de behandelrelatie die de *Zorgaanbieder* met de *Persoon* heeft op grond van art. 7: 446 BW, alsmede de verplichting (op grond van art. 7: 454 BW) om een medisch dossier met betrekking tot de behandeling van de patiënt in te richten. In het licht van de AVG betekent dit dat het is toegestaan voor de *Zorgaanbieder* om persoonsgegevens te verwerken omdat dit noodzakelijk is voor de uitvoering van een overeenkomst (art. 6 lid 1 sub b AVG) en de uitvoering van een wettelijke verplichting (art. 6 lid 1 sub c AVG). Specifiek ten aanzien van de gezondheidsgegevens is het de *Zorgaanbieder* toegestaan om op grond van artikel 9 lid sub f AVG deze gegevens te verwerken.

Het is aan de *Zorgaanbieder* om te beoordelen of de gegevens en/of de gezondheidsinformatie die door de *Persoon* worden aangeboden ook relevant zijn voor het medisch dossier en in dit dossier worden opgenomen. Zie ook het Juridisch kader. Alvorens een *Zorgaanbieder* dit beoordeelt dient eerst door de *Dienstverlener zorgaanbieder* (namens de *Zorgaanbieder)* te worden gecontroleerd of er inderdaad in ieder geval een behandelrelatie is met de desbetreffende *Persoon.* Op basis van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg is de *Zorgaanbieder* voor deze situatie ook gehouden de identiteit van de *Persoon* te verifiëren. Indien blijkt dat er inderdaad een behandelrelatie is en de *Zorgaanbieder* (door middel van de *Dienstverlener zorgaanbieder* en de *Dienstverlener zorgaanbieder* via de *Dienstverlener persoon)* aan de *Persoon* laat weten dat hij ontvankelijk is om de gegevens te ontvangen, wordt door de *Dienstverlener zorgaanbieder,* in de vorm van een controle vraag nog eens aan de *Persoon* gevraagd of hij inderdaad gegevens wil delen met zijn *Zorgaanbieder.* Hiervoor is in het MedMij Afsprakenstelsel een bevestigingsverklaring opgenomen. Op het moment dat de *Persoon* dit heeft bevestigt, stuurt de *Dienstverlener zorgaanbieder* een zogenaamd access token aan de *Dienstverlener persoon* van de *Persoon*

op basis waarvan de *Dienstverlener persoon* kan afleiden dat de *Zorgaanbieder* ontvankelijk is voor het delen van gegevens door de desbetreffende *Persoon.* Met deze code kan de *Dienstverlener persoon* de gegevens en/of de gezondheidsinformatie die de *Persoon* wenst te delen (via de *Dienstverlener zorgaanbieder)* doorzetten aan de *Zorgaanbieder.* Zoals eerder aangegeven, bepaalt de *Zorgaanbieder* vervolgens of hij deze informatie ook wenst op te nemen in het medisch dossier.

Door een access token te gebruiken bij de use case Delen wordt gewaarborgd dat de *Dienstverlener persoon* ook in de use case Delen geen BSN verwerkt. Gelet op het feit dat de *Dienstverlener persoon* wel een access token ontvangt, kan door de *Dienstverlener persoon* echter wel worden afgeleid dat er sprake is van een behandelrelatie. Dit gegeven kan als een 'gegeven over de gezondheid' in de zin van artikel 4 lid 15 AVG worden beschouwd waarvoor voor de rechtmatige verwerking hiervan door de *Dienstverlener persoon* op grond van artikel 9 lid 2 sub a AVG 'uitdrukkelijke toestemming' door de *Persoon* moet worden verleend. Dit betekent dat de *Dienstverlener persoon* in zijn verklaring van toestemming die hij op grond van artikel 7 en 8 AVG moet opstellen, ook informatie over deze verwerking dient op te nemen.

In het geval de *Zorgaanbieder* (via de *Dienstverlener zorgaanbieder)* aan de *Persoon* laat weten dat er *geen* behandelrelatie is met de desbetreffende *Persoon* ontvangt de *Dienstverlener persoon* (via de *Dienstverlener zorgaanbieder)* het bericht dat de *Zorgaanbieder* niet ontvankelijk is voor het delen van gegevens door de desbetreffende *Persoon.* In deze situatie dient de *Dienstverlener zorgaanbieder* de persoonsgegevens die in relatie tot de use case Delen zijn verwerkt, overeenkomstig het bepaalde in de modelverwerkersovereenkomst, te verwijderen en/of te vernietigen. De rechtmatigheidsgrondslag voor de *Zorgaanbieder* en de *Dienstverlener zorgaanbieder* om in deze situatie wel het BSN te verwerken, is dat de *Zorgaanbieder* op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in het identificatieproces verplicht is het BSN te gebruiken.

Toelichting AVG-normen

Gegevens die door deelnemers aan het MedMij Afsprakenstelsel worden uitgewisseld betreffen bijna altijd bijzondere persoonsgegevens. Deelnemers moeten hiervoor voldoen aan de normen die de AVG stelt met betrekking tot het verwerken van deze persoonsgegevens. Vanwege het belang van een correcte uitvoering van deze wet door deelnemers aan het MedMij Afsprakenstelsel, heeft MedMij hieronder een toelichting op de verantwoordelijkheden en normen in de AVG opgenomen. Indien aan de orde, is in een tweede kolom aangegeven of het MedMij Afsprakenstelsel een nadere invulling, dan wel een aanvulling heeft gedefinieerd op dat onderwerp. In een derde kolom is een eventuele opmerking of een aandachtspunt voor deelnemers opgenomen.

Onderstaande tabel is een hulpmiddel voor de deelnemer. De publicatie van deze tabel doet niets af aan de eigen verantwoordelijkheid van de verwerkingsverantwoordelijke om de AVG te implementeren. Deelnemers zijn zelf verantwoordelijk voor de correcte implementatie van de wet. Bij Toetreding tot het stelsel verklaart de deelnemer met de Zelfverklaring integriteit te voldoen aan de AVG.

Artikel AVG	Norm AVG	Aanvulling MedMij Afsprakenstelsel	Opmerking en/of aandachtspunt
	Toepassingsgebied AVG		
Artikel 2, 3	De AVG is van toepassing op: • verwerkingen die geheel of gedeeltelijk geautomatiseerd zijn, alsmede; • op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Onder 'bestand' wordt elk gestructureerd geheel van persoonsgegevens begrepen die volgens bepaalde criteria toegankelijk zijn. Verwerking van persoonsgegevens waarop de AVG van toepassing is moet plaatsvinden in het kader van activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Europese Unie, ongeacht of de verwerking al dan niet plaatsvindt in de Europese Unie. De AVG is ook van toepassing op organisaties die buiten de Europese Unie zijn gevestigd, indien zij persoonsgegevens verwerken van betrokkenen in de Europese Unie óf indien zij het gedrag van betrokkenen in de Europese Unie monitoren.	Het MedMij Afsprakenstelsel bepaalt dat zijn deelnemers ingeschreven dienen te zijn in een handelsregister in de EU. Inschrijving in een handelsregister in de EU impliceert ofwel een vestiging in de EU, ofwel ondernemingsactiviteiten in de EU. Derhalve is de AVG van toepassing op deelnemers aan het afsprakenstelsel.	

	Algemene bepalingen en definities		
Artikel 4, 9	Het begrip 'persoonsgegevens' betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. De AVG maakt een onderscheid tussen: 1) persoonsgegevens, en 2) bijzondere categorieën van persoonsgegevens. Bijzondere categorieën van persoonsgegevens, hierna bijzondere persoonsgegevens, betreffen gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Het zullen vooral bijzondere persoonsgegevens zijn die via het MedMij-netwerk uitgewisseld worden, aangezien de verwerking voornamelijk op gegevens betreffende de gezondheid van personen zal plaatsvinden.		
Artikel 4	In de AVG worden twee rollen gedefinieerd:	Gelet op de rolomschrijvingen in het MedMij Afsprakenstelsel zullen de *Aanbieder* en de	

	• verwerkingsverantwoordelijke, • verwerker. Een **verwerkingsverantwoordelijke** is degene die alleen, of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Deze rol kan vervuld worden door een natuurlijk persoon, een rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan. Een **verwerker** is een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van, en op instructie van, de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Het is de feitelijke situatie waaruit afgeleid wordt welke partij welke rol vervult. Dit is contractueel niet af te spreken.	*Dienstverlener persoon* waarschijnlijk de rol van verwerkingsverantwoordelijke vervullen. De *Dienstverlener aanbieder* zal, indien gegevens verwerkt worden in opdracht van de *Aanbieder*, de rol aannemen van verwerker. Dit hangt echter wel altijd af van de feitelijke informatie en omstandigheden. Een toelichting is gegeven op de pagina Toelichting verwerkingsverantwoordelijkheden	
Artikel 4	Verwerking van persoonsgegevens is een breed begrip. Het omvat in feite elke handeling die de gegevens betreft, waaronder eenvoudigweg het houden, ontvangen, verzamelen, bewerken, opslaan of verwijderen van die gegevens.		
Artikel 5	Persoonsgegevens die verwerkt worden dienen juist te zijn en zo nodig geactualiseerd te worden. Redelijke maatregelen moeten worden genomen door		*Aanbieders* zijn zelf verantwoordelijk om te communiceren aan personen over de persoonsgegevens die zij verwerken.

	de verwerkingsverantwoordelijke om de persoonsgegevens die onjuist zijn, onverwijld te wissen of te wijzigen.		*Dienstverleners persoon*, als aanbieder van een PGO, dienen zich ervan bewust te zijn dat ze verantwoordelijk zijn om de persoonsgegevens die zij zelf verzamelen (en eventueel ook in een PGO aanwezig zijn) actueel te houden. De dienstverlener is niet verantwoordelijk voor de juistheid van de gegevens/ inhoud van de PGO die daarin zelf door de *Persoon* wordt opgenomen.
Artikel 5	In beginsel mogen persoonsgegevens slechts voor: • welbepaalde, • uitdrukkelijk omschreven, en • gerechtvaardigde doeleinden verwerkt worden. Indien persoonsgegevens voor een ander, secundair, doeleinde verwerkt worden, is dit slechts mogelijk indien de betrokkene toestemming heeft gegeven voor deze verdere verwerking, of indien dit noodzakelijk is voor een specifiek wettelijk voorschrift ter waarborging van een belangrijke doelstelling van algemeen belang. Tot slot mogen persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te	In het MedMij Afsprakenstelsel is bepaald dat in het kader van de uitvoering van de Deelnemersovereenkomst met MedMij het doel van de verwerking van de persoonsgegevens de waarborging en realisering van een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de *Persoon* en *Aanbieder* via de *Dienstverlener persoon* en de *Dienstverlener aanbieder* overeenkomstig het bepaalde in het MedMij Afsprakenstelsel is. Deze bepaling is ook opgenomen in artikel 9 van de Modelverwerkersovereenkomst Aanbieder – Dienstverlener aanbieder. In het MedMij Afsprakenstelsel zijn bewaartermijnen gegeven voor de vereiste logging van de gegevensuitwisseling en de verwerking.	Aanvullend dienen de *Dienstverlener persoon* en de *Aanbieder* de doeleinden voor (de verdere/eigen) verwerking van de persoonsgegevens specifiek te formuleren voor de *Persoon*, zodat duidelijk is waarom de verwerking van persoonsgegevens nodig is om dit doel te realiseren en ook in hoeverre de gegevens voor andere doeleinden kunnen worden verwerkt. Doordat het doel duidelijk geformuleerd is, wordt het ook snel duidelijk wanneer persoonsgegevens verwerkt zullen worden voor secundaire doeleinden. Voordat een *Persoon* zijn persoonlijke gezondheidsomgeving in gebruik neemt dient de *Dienstverlener persoon* een specifieke toestemming te verkrijgen van de *Persoon* voor het verwerken van persoonsgegevens.

	identificeren dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld en verder verwerkt.		
Artikel 5	Gegevensverwerkingen dienen te worden beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. De gegevensverwerking moet derhalve vooraf getoetst worden aan de beginselen van proportionaliteit en subsidiariteit. **Proportionaliteit** betekent dat moet worden beoordeeld of de inbreuk op de privacy van betrokkenen van de voorgenomen gegevensverwerking in een redelijke verhouding staat tot het doel. Daarbij zal moeten worden gekeken of de voorgenomen gegevensverwerking effectief is om het beoogde doel te bereiken en of de te verwerken persoonsgegevens relevant en toereikend zijn om het beoogde doel te bereiken. Bij **subsidiariteit** wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt.	In het MedMij Afsprakenstelsel is onder andere in de Architectuur en technische specificaties rekening gehouden met het proportionaliteits- en subsidiariteitsbeginsel. Op die manier is gestreefd naar afspraken waarbij niet meer gegevens worden verwerkt dan noodzakelijk is voor de gegevensuitwisseling (privacy by design en privacy bij default). Er vindt onafhankelijke toetsing daarvan plaats.	
Artikel 5, 6	Indien persoonsgegevens verstrekt worden aan derde partijen, moet de verwerking door deze derde partijen in lijn zijn met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld en verwerkt.	Deze bepaling is aanvullend op de AVG ook opgenomen in artikel 5.6 van de Deelnemersovereenkomst Dienstverlener persoon en Dienstverlener aanbieder.	

	Grondslagen & toestemming		
Artikel 6, 7, 9	Persoonsgegevens mogen slechts verwerkt worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen, indien de verwerking plaatsvindt op een van de grondslagen die limitatief opgesomd zijn in de AVG. Dit betreft de volgende **grondslagen**: 1) Toestemming van de betrokkene; 2) De gegevens zijn noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene een partij is; 3) De gegevens zijn noodzakelijk voor het volgen van een wettelijke verplichting; 4) De gegevensverwerking is noodzakelijk om vitale belangen van de betrokkene of van een ander natuurlijk persoon te beschermen; 5) De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag; 6) De gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van u of van een	**Algemeen:** In het afsprakenstelsel is bepaald dat in het kader van de uitvoering van de Deelnemersovereenkomst met MedMij het doel van de verwerking van de persoonsgegevens de waarborging en realisering van een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de *Persoon* en *Aanbieder* via de *Dienstverlener persoon* en de *Dienstverlener aanbieder* overeenkomstig het bepaalde in het MedMij Afsprakenstelsel is. In de overeenkomst met de deelnemer is bepaald dat: Voor zover de verwerking van persoonsgegevens door de Deelnemer wordt gebaseerd op de rechtmatigheidsgrondslag 'toestemming' in de zin van artikel 6 lid 1 AVG is de verwerking voor een ander doel dan genoemd in artikel 5.5 van deze Overeenkomst toegestaan, mits de beginselen van de AVG op deze verdere verwerking wordt toegepast, de *Persoon* over deze verdere verwerking wordt geïnformeerd alsmede over de rechten die de *Persoon* tegen deze verdere verwerking kan uitoefenen. Voor zover de verwerking van de persoonsgegevens wordt gebaseerd op de rechtmatigheidsgrondslag 'noodzakelijk voor de uitvoering van de overeenkomst' in de zin van artikel 6 lid 1 sub c AVG, is verdere verwerking van de persoonsgegevens door de Deelnemer alleen toegestaan indien de evenredigheidstoets van artikel 6 lid 4 AVG succesvol is doorlopen.	**Algemeen:** Let goed op het verschil tussen toestemming en expliciete toestemming. Een grondslag voor de verwerking van bijzondere persoonsgegevens is uitdrukkelijke toestemming. Dit betreft een verzwaarde vorm van toestemming. De betrokkene moet nadrukkelijk uitdrukking hebben gegeven aan zijn wil om toestemming te verlenen voor het verwerken van zijn bijzondere persoonsgegevens. Impliciete toestemming is niet mogelijk.

	derde aan wie de gegevens worden verstrekt. Bij verwerking van **bijzondere of strafrechtelijke persoonsgegevens** (zie de sectie Algemene bepalingen en definities bovenaan in deze tabel) dient één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing te zijn (art. 9 lid 2 AVG). Als geen van deze uitzonderingen van toepassing is, dan is de verwerking van dit type persoonsgegevens verboden. Op bovengenoemd **verwerkingsverbod** gelden samengevat de volgende **uitzonderingen**: 1. de betrokkene heeft **uitdrukkelijke toestemming** gegeven; 2. de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van arbeids- en sociaalzekerheidsrecht; 3. de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander; 4. de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;	Meer informatie is ook te vinden op de pagina Toelichting verwerkingsverantwoordelijkheden. De Deelnemer verstrekt geen persoonsgegevens van de *Persoon* aan anderen dan degenen waaraan de Deelnemer uit hoofde van de Deelnemersovereenkomst gegevens mag verstrekken c.q. op grond van een wettelijke verplichting moet verstrekken. Het is de Deelnemer uitdrukkelijk verboden om data betreffende de *Persoon* te verkopen.	

5. de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
6. de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
7. de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
8. de verwerking noodzakelijk is voor preventieve en arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid, medische diagnosen, het verstrekken van gezondheidzorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en –diensten of sociale stelsel en diensten;
9. de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;
10. de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Indien persoonsgegevens worden verwerkt op basis van gegeven **toestemming**, gelden er nog enkele specifieke **vereisten**:

- Aangetoond moet kunnen worden dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.

	• De toestemming moet zijn gegeven door middel van een duidelijke actieve handeling. • De toestemming moet gevraagd zijn in een begrijpelijk en gemakkelijk toegankelijke vorm. • De toestemming moet vrijelijk gegeven kunnen worden. • De toestemmingsvraag moet in duidelijke en eenvoudige taal gepresenteerd worden. • De toestemming moet ten alle tijden ingetrokken kunnen worden. Indien een verdere verwerking niet verenigbaar is met het oorspronkelijke doel, dan zal de verwerkingsverantwoordelijke een specifieke wettelijke grondslag moeten hebben of toestemming moeten vragen van de betrokkene voor de verdere verwerking. Onder de AVG, anders dan onder de Wbp, is het BSN geen bijzonder persoonsgegeven meer, maar kent wel een specifieke bepaling in verband met de gegevensverwerking en opgenomen in art 87 AVG/46 Uitvoeringswet AVG.	Voor de rechtmatigheid van de verwerking van het BSN binnen de scope van het MedMij Afsprakenstelsel wordt verwezen naar het Juridisch kader (wet aanvullende bepalingen verwerking persoonsgegevens in de zorg) en de Toelichting verwerkingsverantwoordelijkheid	
Artikel 8	Specifieke voorwaarden worden gesteld in de AVG voor toestemming van kinderen in het geval er sprake is van **diensten van de informatiemaatschappij**. Indien sprake is	**Algemeen:** In het afsprakenstelsel is afgesproken dat voorlopig alleen gezondheidsgegevens van personen van 16 jaar en ouder uitgewisseld worden.	**Let op:** Voor het verwerken van persoonsgegevens van kinderen gelden specifieke (strengere) eisen en evenueel de betrokkenheid van ouder of voogd.

	van een dergelijke situatie, dient de toestemming verleend te worden door de ouder of voogd. Het aanbieden van een PGO door een *Dienstverlener persoon* kan gekwalificeerd worden als het aanbieden van een dienst van de informatiemaatschappij zoals omschreven in artikel 3:15d lid 3 BW. Onder dienst van de informatiemaatschappij wordt namelijk verstaan elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van de afnemer van de dienst wordt verricht zonder dat partijen gelijktijdig op dezelfde plaats aanwezig zijn.		Bovendien is het momenteel niet mogelijk om gegevens van personen jonger dan 16 jaar via het MedMij Afsprakenstelsel te (laten) uitwisselen. Bekijk goed wat u wel/ niet toestaat in de registratie van personen jonger dan 16 jaar voor een PGO.
		Informatievoorziening	
Artikel 12, 13, 14	Een verwerkingsverantwoordelijke is verantwoordelijk om betrokkenen te **informeren** over de verwerking van persoonsgegevens. Deze informatie dient zowel verschaft te worden indien de persoonsgegevens rechtstreeks bij de betrokkene worden verzameld, alsook wanneer de persoonsgegevens niet rechtstreeks bij de betrokkene worden verzameld. Indien persoonsgegevens rechtstreeks bij de betrokkene worden verzameld, dient de volgende informatie bij de verkrijging van	**Algemeen:** De *Dienstverlener persoon* is aanvullend op de AVG ook op grond van de Deelnemersovereenkomst (artikel 4.1) verplicht verwerking van de persoonsgegevens overeenkomstig de privacywet- en -regelgeving uit te voeren. Specifiek voor de *Dienstverlener persoon* is nog opgenomen dat Gebruikers worden geïnformeerd over hoe de *Persoon* zijn rechten in deze bij de *Dienstverlener persoon* kan uitoefenen. .	

de persoonsgegevens verstrekt te worden door de verwerkingsverantwoordelijke:

- De identiteit en contactgegevens van de verwerkingsverantwoordelijke, en indien van toepassing van de vertegenwoordiger;
- De contactgegevens van de functionaris voor gegevensbescherming indien aanwezig;
- De verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd;
- De grondslag voor de verwerking;
- Indien de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van u of van een derde aan wie de gegevens worden verstrekt, dient informatie omtrent de gerechtvaardigde belangen verstrekt te worden;
- De ontvangers of categorieën van ontvangers van de persoonsgegevens indien van toepassing;
- Indien de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een derde land of een internationale organisatie dient aangegeven te worden of er een adequaatheidsbesluit van de Europese Commissie bestaat, of welke passende of geschikte waarborgen er zijn voor deze doorgifte;
- De periode gedurende welke de persoonsgegevens zullen worden

opgeslagen. Indien deze informatie niet verstrekt kan worden, dienen de criteria ter bepaling van die termijn verstrekt te worden;
- De rechten die betrokkenen toekomen;
- Of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
- Het bestaan van eventuele geautomatiseerde besluitvorming en/of profilering.

Indien persoonsgegevens niet rechtstreeks van betrokkenen worden verkregen, dient in aanvulling op bovenstaande opsomming, door de verwerkingsverantwoordelijke ook informatie verstrekt te worden over:

- de betrokken categorieën van persoonsgegevens;
- de bron waar de persoonsgegevens vandaan komen en, in voorkomend geval, of zij afkomstig zijn van openbare bronnen.

De verwerkingsverantwoordelijke verstrekt in dit geval de informatie binnen een redelijke termijn, maar uiterlijk binnen één

	maand na de verkrijging van de persoonsgegevens. Indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, dient de verwerkingsverantwoordelijke de informatie uiterlijk op het moment van het eerste contact met de betrokkene te verstrekken.		
		Rechten van betrokkenen	
Artikel 15, 16, 17, 18, 20, 21, 22, 23	**Betrokkenen** waarvan persoonsgegevens verwerkt worden komen verschillende **rechten** toe op grond van de AVG. De verwerkingsverantwoordelijke is degene die de uitoefening van deze rechten moet faciliteren. Daarnaast is de verwerkingsverantwoordelijke verantwoordelijk om iedere ontvanger aan wie de persoonsgegevens zijn verstrekt, in kennis te stellen van ieder verzoek tot rectificatie of wissing van persoonsgegevens, of verzoek tot beperking van de verwerking. **Recht op inzage** Betrokkenen hebben het recht om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hen betreffende persoonsgegevens. Indien dit het geval is, heeft de betrokkene het recht om inzage te verkrijgen van die	**Algemeen**: Betrokkenen, *Personen* in termen van het MedMij Afsprakenstelsel, kunnen hun rechten uitoefenen jegens de *Dienstverlener persoon* voor de gegevens die verwerkt worden binnen de PGO. Verzoeken die gebaseerd zijn op een recht dat de betrokkene toekomt dienen daarom rechtstreeks aan de *Dienstverlener persoon* gericht te worden indien het gaat om persoonsgegevens die verwerkt worden in de PGO. In art. 4.1 van de Deelnemersovereenkomst hebben we opgenomen dat de deelnemers de verwerking van de persoonsgegevens overeenkomstig de privacywet- en -regelgeving uitvoeren. Specifiek voor de *Dienstverlener persoon* is nog opgenomen dat Gebruikers worden geïnformeerd over hoe de *Persoon* zijn rechten in deze bij de *Dienstverlener persoon* kan uitoefenen. **Algemeen** : Betrokkenen, *Personen* in termen van het MedMij Afsprakenstelsel, kunnen daarnaast hun rechten uitoefenen jegens de *Aanbieder* met betrekking tot de gegevens die verwerkt worden door de *Aanbieder* in de uitoefening van zijn zorgtaken. De relatie *Persoon* –	**Algemeen**: Zorg dat betrokkenen, *Personen*, de genoemde rechten kunnen uitoefenen en richt hiervoor processen in. Het is van belang dat de deelnemer kan aantonen dat dit gebeurt/is gebeurd. Indien mogelijk, richt dit dan zo in dat veel rechten, zoals hier genoemd, al automatisch uit te oefenen zijn in onder andere de PGO zelf.

persoonsgegevens. Bovendien dient dan informatie omtrent de verwerking van persoonsgegevens verstrekt te worden, die ook verstrekt dient te worden indien de persoonsgegevens verzameld worden bij de betrokkenen.

Indien de betrokkene een verzoek tot inzage doet, verstrekt de verwerkingsverantwoordelijke een kopie van de persoonsgegevens die verwerkt worden aan de betrokkene.

Recht op rectificatie

Indien persoonsgegevens onjuist zijn, heeft de betrokkene het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van deze onjuiste persoonsgegevens te verkrijgen. Indien bepaalde persoonsgegevens onvolledig worden verwerkt, gelet op de doeleinden van de verwerking, heeft de betrokkene ook het recht om deze persoonsgegevens te vervolledigen.

Recht op gegevenswissing

Betrokkenen hebben het recht om van de verwerkingsverantwoordelijke, zonder onredelijke vertraging, wissing van hem betreffende persoonsgegevens te verkrijgen. De verwerkingsverantwoordelijke is in de

Aanbieder valt buiten de scope van het Afsprakenstelsel MedMij. De *Dienstverlener aanbieder* is de *Deelnemer*. Om ervoor te zorgen dat de *Aanbieder* zijn verantwoordelijkheid kan nemen bij een verzoek om uitoefening van rechten van één van zijn patiënten die gebruik maakt van een PGO dat via MedMij-afspraken gegevens uitwisselt, is in art. 3.7 van de modelverwerkersovereenkomst tussen de *Dienstverlener aanbieder* en de *Aanbieder* opgenomen dat de *Dienstverlener aanbieder* zijn medewerking verleent.

volgende gevallen verplicht om de persoonsgegevens te wissen:

1. indien de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of verwerkt;
2. de betrokkene trekt gegeven toestemming in, en er is geen andere rechtsgrond voor de verwerking;
3. de betrokkene maakt bezwaar tegen de verwerking, waarbij er geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking aanwezig zijn;
4. de persoonsgegevens zijn onrechtmatig verwerkt;
5. de persoonsgegevens moeten worden gewist om als verwerkingsverantwoordelijke te kunnen voldoen aan een wettelijke verplichting die op hem rust;
6. de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij aan een kind jonger dan 16 jaar.

Een verwerkingsverantwoordelijke hoeft niet te voldoen aan een verzoek tot gegevenswissing indien de verwerking noodzakelijk is:

- voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;

- voor het nakomen van een wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust;
- om redenen van algemeen belang op het gebied van volksgezondheid;
- met het oog op archivering in het algemeen belang, wetenschappelijke of historisch onderzoek of statistische doeleinden;
- voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Recht op beperking van de verwerking

Betrokkenen hebben het recht om de verwerking van hen betreffende persoonsgegevens te beperken (de gegevens mogen in dat geval alleen door de verwerkingsverantwoordelijke worden bewaard en alleen voor beperkte doeleinden worden gebruikt) indien:

- de nauwkeurigheid van de gegevens wordt betwist (en alleen zolang als nodig is om die nauwkeurigheid te verifiëren);
- de verwerking onrechtmatig is en de betrokkene verzoekt om beperking en zich verzet tegen het wissen van de persoonsgegevens;
- de verwerkingsverantwoordelijke de gegevens niet meer nodig heeft voor het oorspronkelijke doel, maar de betrokkene de gegevens nog wel nodig

heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering; of
- de betrokkene bezwaar heeft gemaakt tegen de verwerking, en in afwachting is van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan zijn eigen rechten.

Recht op overdraagbaarheid van gegevens

Betrokkenen hebben het recht om:

- een kopie te ontvangen van hun betreffende persoonsgegevens in een gestructureerde, veelgebruikte, machineleesbare vorm die hergebruik ondersteunt;
- hen betreffende persoonsgegevens rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere over te dragen.

Recht van bezwaar

Betrokkenen hebben het recht om bezwaar te maken, vanwege met specifieke situatie verband houdende redenen, tegen de verwerking van persoonsgegevens indien die grondslag voor die verwerking is:

- noodzakelijkheid voor de vervulling van een taak van algemeen belang, of
- noodzakelijkheid voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde.

De verwerkingsverantwoordelijke moet deze verwerking staken, tenzij de verantwoordelijke:

- aan kan tonen dat hij dwingende gerechtvaardigde gronden heeft voor de verwerking die prevaleren boven de belangen, rechten en vrijheden van de betrokkene, of
- er gerechtvaardigde gronden zijn die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

Daarnaast hebben betrokkenen het recht om bezwaar te maken tegen de verwerking van persoonsgegevens met het oog op direct marketing, inclusief profilering.

Geautomatiseerde individuele besluitvorming, waaronder profilering

Betrokkenen hebben tot slot het recht niet te worden onderworpen aan een besluit dat tot stand is gekomen door een uitsluitend geautomatiseerde verwerking of profilering.

	NB Er zijn uitzonderingen mogelijk op de uitoefening van de rechten van betrokkene, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang. Uitzonderingen dienen altijd een wettelijke grondslag te hebben.		
		Verplichtingen verwerkingsverantwoordelijken	
Artikel 5, 24 t/m 28, 30 t/m 36	Op partijen die de rol van **verwerkingsverantwoordelijke** vervullen rusten diverse **verplichtingen**. 1. Allereerst is de verwerkingsverantwoordelijke verantwoordelijk voor, en moet hij in staat zijn om aan te tonen dat de gegevensbeschermingsbeginselen zoals neergelegd in de AVG worden nageleefd. 2. De verwerkingsverantwoordelijke is verantwoordelijk voor het implementeren van passende **technische en organisatorische maatregelen** om te garanderen, en om aan te tonen, dat zijn verwerkingsactiviteiten voldoen aan de vereisten van de AVG. Deze maatregelen kunnen het implementeren van een passend gegevensbeschermingsbeleid	**Algemeen**: Het afsprakenstelsel bepaalt dat de deelnemers aan het afsprakenstelsel ingeschreven dienen te zijn in een handelsregister in de EU. In het MedMij Afsprakenstelsel is onder andere in de architectuur en technische specificaties rekening gehouden met het proportionaliteits- en subsidiariteitsbeginsel. Op die manier is gestreefd naar afspraken waarbij niet meer gegevens worden verwerkt dan noodzakelijk is voor de gegevensuitwisseling (privacy by design en privacy bij default) en vindt onafhankelijke toetsing daarvan plaats.	

omvatten. Het naleven van goedgekeurde gedragscodes kan een bewijs zijn van naleving.

3. Verwerkingsverantwoordelijken moeten ervoor zorgen dat zowel in de ontwerpfase van nieuwe verwerkingsactiviteiten, als in de implementatiefase van een nieuw product of dienst (bijvoorbeeld een nieuw ontwikkelde PGO), gegevensbeschermingsbeginselen en passende voorzorgsmaatregelen worden onderzocht en geïmplementeerd. Daarnaast dienen de nodige waarborgen in de verwerking ingebouwd te worden ter bescherming van de rechten van de betrokkenen. Dit wordt ook wel **gegevensbescherming door ontwerp** genoemd**.**

Daarnaast dienen passende technische en organisatorische maatregelen getroffen te worden om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Dit wordt ook wel **gegevensbescherming door standaardinstellingen** genoemd.

4. Indien twee of meer verwerkingsverantwoordelijkheden gezamenlijk de doeleinden en de middelen van de verwerking bepalen, zijn zij **gezamenlijke**

verwerkingsverantwoordelijken. In dit geval dienen zij hun respectievelijke verantwoordelijkheden met betrekking tot de nakoming van de verplichtingen uit de AVG vast te stellen door middel van een onderlinge regeling. Betrokkenen kunnen in dit geval hun rechten uitoefenen jegens iedere verwerkingsverantwoordelijke afzonderlijk.

5. Een verwerkingsverantwoordelijke die buiten de EU is gevestigd, moet een vertegenwoordiger aanwijzen in een van de lidstaten waar de verwerkingsverantwoordelijke goederen of diensten aanbiedt of EU-ingezetenen monitort, tenzij de verwerking incidenteel en kleinschalig is en geen gevoelige persoonsgegevens bevat.

6. Verwerkingsverantwoordelijken kunnen verwerkers inschakelen om persoonsgegevens te verwerken op hun instructie, zoals een hostingbedrijf dat de PGO-gegevens moet hosten.

Slechts verwerkers die de naleving van de AVG garanderen mogen ingeschakeld worden. De verwerkingsverantwoordelijke dient een **verwerkersovereenkomst** af te sluiten met de verwerker. Er is een MedMij Modelverwerkersovereenkomst

6. Verwerkersovereenkomst. Aanvullend op de verplichtingen in de AVG wordt in het MedMij Afsprakenstelsel bepaald dat verwerkers van persoonsgegevens, die in opdracht van de verwerkingsverantwoordelijke werken, waaronder de *Dienstverlener aanbieder* die de gegevensuitwisseling conform MedMij-afspraken regelt, een verwerkersovereenkomst af moeten sluiten. Hiervoor is een model verwerkersovereenkomst beschikbaar gesteld, waarin expliciet rekening is gehouden met de situatie die voortvloeit uit deelname aan het MedMij Afsprakenstelsel.

beschikbaar die gebruikt kan worden tussen de *Aanbieder* en de *Dienstverlener aanbieder*.

Indien er wordt gekozen voor een eigen verwerkersovereenkomst moet daarin informatie opgenomen te worden over:

- het onderwerp van de verwerking(en);
- de duur van de verwerking;
- de aard van het doel van de verwerking;
- het soort persoonsgegevens en de categorieën van betrokkenen;
- de rechten en verplichtingen van de verwerkingsverantwoordelijke.

In de verwerkersovereenkomst moet bovendien opgenomen worden dat de verwerker:

1. alleen persoonsgegevens mag verwerken op basis van gedocumenteerde instructies door de verwerkingsverantwoordelijke;
2. waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen;
3. de beveiliging van de persoonsgegevens die hij verwerkt moet garanderen;
4. aan regels is gebonden indien hij een sub-verwerker in wilt schakelen;

5. maatregelen implementeert om de verwerkingsverantwoordelijke te kunnen helpen bij de naleving van de rechten van betrokkenen;
6. de verwerkingsverantwoordelijke assisteert bij het verkrijgen van goedkeuring van een toezichthouder indien nodig;
7. na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt;
8. alle informatie verstrekt aan de verwerkingsverantwoordelijke die noodzakelijk is om naleving van de AVG aan te kunnen tonen.

7. Een verwerkingsverantwoordelijke dient een register van de verwerkingsactiviteiten, ook wel **verwerkingsregister** genoemd, bij te houden. Dit register dient minimaal de volgende gegevens te bevatten:

- De naam en contactgegevens van:
  - de verwerkingsverantwoordelijke
  - indien van toepassing die van de gezamenlijke verwerkingsverantwoordelijken en/of vertegenwoordiger van de verwerkingsverantwoordelijke, en van de functionaris voor gegevensbescherming;
- De verwerkingsdoeleinden;

7. Verwerkingsregister. Een verwerkingsregister biedt ook een goed uitgangspunt voor een verwerkingsverantwoordelijke om de data die verzameld is goed in beeld te krijgen. Door de identificatie van alle data ontstaat ook een goed beeld over de stappen die ondernomen moeten worden op het gebied van beveiliging van de data. Voor een deelnemer is het dus belangrijk een dergelijk register bij te houden en hierin ook de verwerkingen op te nemen die het gevolg zijn van deelname aan het MedMij Afsprakenstelsel.

	• Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens; • De categorieën van ontvangers aan wie de persoonsgegevens zijn óf zullen worden verstrekt; • Indien van toepassing: doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of internationale organisatie en de passende waarborgen; • De van toepassing zijnde bewaartermijnen; • Een omschrijving van de geïmplementeerde beveiligingsmaatregelen. 8. Een verwerkingsverantwoordelijke is, samen met de verwerker, verplicht om desgevraagd samen te werken met de toezichthoudende autoriteit bij het vervullen van haar taken. 9. De verwerkingsverantwoordelijke moet **passende technische en organisatorische beveiligingsmaatregelen** treffen om persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging of verlies, wijziging, ongeautoriseerde openbaarmaking of toegang. Afhankelijk	**9. Passende technische en organisatorische beveiligingsmaatregelen**. In het MedMij Afsprakenstelsel is een aanvullend normenkader informatiebeveiliging opgenomen. Op basis van een stelselrisicoanalyse en/of PIA worden maatregelen (her)overwogen en eventueel aanvullende privacy- en informatiebeveiligingsmaatregelen gedefinieerd. Dit kan resulteren in bijstelling van het Normenkader informatiebeveiliging en de Architectuur en technische specificaties. **10. Datalek**. Deelnemers aan het MedMij Afsprakenstelsel zijn zelf verantwoordelijk om eventuele datalekken te signaleren. Zie hiervoor ook de Guidelines on Personal data breach notification van de Europese privacytoezichthouders:	.	

van de verwerkingsactiviteiten kunnen de beveiligingsmaatregelen het volgende omvatten:

- Pseudonimisering en versleuteling van persoonsgegevens;
- Doorlopende beoordelingen van de beveiligingsmaatregelen;
- Redundantie en back-up mogelijkheden;
- Regelmatig testen, beoordelen en evalueren van de beveiligingsmaatregelen.

Wat een passend niveau van beveiliging is, dient te worden getoetst aan de hand van de verwerkingsrisico's die met de verwerkingsactiviteit gepaard gaan.

10. De verwerkingsverantwoordelijke is verplicht om een inbreuk in verband met persoonsgegevens, ook wel **datalek** genoemd, zonder onredelijke vertraging en uiterlijk 72 uur nadat hij er kennis van heeft genomen te melden bij de bevoegde toezichthoudende autoriteit. (In Nederland is dit de Autoriteit Persoonsgegevens). De enige uitzondering hierop is wanneer beoordeeld is dat het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van betrokkenen. De melding moet minimaal de volgende informatie bevatten:

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken.

In het MedMij Afsprakenstelsel is in het Normenkader informatiebeveiliging opgenomen dat beveiligingsincidenten binnen 48 uur gemeld dienen te worden bij de beheerorganisatie. Hieronder vallen ook datalekken.

De beheerorganisatie is verantwoordelijk om een impact analyse te doen op het beveiligingslek en/of beveiligingsincident voor het stelsel als geheel, en dit te delen met andere partijen indien dit nodig wordt geacht.

1. Een omschrijving van de inbreuk in verband met persoonsgegevens, met inbegrip van het aantal betrokken betrokkenen en de getroffen categorieën van persoonsgegevens;
2. De naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
3. De waarschijnlijke gevolgen van de inbreuk;
4. De maatregelen die zijn getroffen om de inbreuk aan te pakken, waaronder maatregelen die de eventuele nadelige gevolgen van de inbreuk beperken.

De verwerkingsverantwoordelijke is bovendien verplicht om alle inbreuken in verband met persoonsgegevens te documenteren, inclusief informatie over de gevolgen daarvan en de genomen corrigerende maatregelen.

Indien een inbreuk in verband met persoonsgegevens een hoog risico oplevert voor betrokkenen, is de verwerkingsverantwoordelijke bovendien verplicht om de betrokkenen te informeren over deze inbreuk. Deze melding dient minimaal punt 2 t/m 4 van de verplichte informatie aan de toezichthoudende autoriteit te bevatten.

Een verwerkingsverantwoordelijke is uitgezonderd van deze meldingsplicht indien:

- Er passende technische en organisatorische beschermingsmaatregelen genomen zijn en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, zoals bijvoorbeeld versleuteling van de data.
- Achteraf maatregelen genomen zijn om ervoor te zorgen dat de bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen.
- De mededeling onevenredige inspanningen zou vergen.

11. De verwerkingsverantwoordelijke dient in elk geval een functionaris voor gegevensbescherming aan te wijzen indien hij hoofdzakelijk is belast met grootschalige verwerking van bijzondere persoonsgegevens.

12. Indien een soort verwerking van persoonsgegevens, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van

12. Formats voor gegevensbeschermingseffectbeoordelingen:

Van de ICO: https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf
Van de CNIL: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf
Het Rijksoverheid Model: https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia

betrokkenen, dient de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit te voeren van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Een dergelijke beoordeling wordt een **gegevensbeschermingseffectbeoordeling** genoemd. Dit is een degelijk instrument om vooraf privacyrisico's van de voorgenomen verwerkingsactiviteit(en) in kaart te brengen.

Een gegevensbeschermingseffectbeoordeling is in ieder geval vereist indien het een grootschalige verwerking van bijzondere persoonsgegevens betreft.

Een beoordeling bevat tenminste de volgende punten:

- een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;

	• beoogde maatregelen om de risico's aan te pakken. Wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien geen maatregelen genomen worden om het risico te beperken, dient de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit te raadplegen.		
	Verplichtingen verwerker		
Artikel 28 t/m 33, 37	Op partijen die de rol van **verwerker** vervullen rusten diverse **verplichtingen**. 1. Een verwerker mag alleen persoonsgegevens verwerken op basis van gedocumenteerde instructies van een verwerkingsverantwoordelijke. Tussen de verwerkingsverantwoordelijke en de verwerker dient een verwerkersovereenkomst afgesloten te worden. 2. Een verwerker moet de beveiliging van de persoonsgegevens die hij verwerkt garanderen aan de verwerkingsverantwoordelijke. 3. De verwerker moet ervoor zorgen dat alle persoonsgegevens die hij verwerkt vertrouwelijk worden behandeld. De	In artikel 8 van de Deelnemersovereenkomst zijn, aanvullend op de AVG, verantwoordelijkheden van een deelnemer jegens derden, waaronder verwerkers van persoonsgegevens, opgenomen.	**Algemeen:** Ook voor verwerkers (bijvoorbeeld de *Dienstverlener aanbieder* of subverwerkers van dienstverleners) is het belangrijk om in een verwerkersovereenkomst duidelijke afspraken te maken met een verwerkingsverantwoordelijke over de verwerkingen die zij uit zullen gaan voeren. Zij kunnen zelf het initiatief nemen om een verwerkersovereenkomst af te sluiten mocht de verwerkingsverantwoordelijke dit initiatief niet tonen.

verwerkersovereenkomst tussen de verwerkingsverantwoordelijke en de verwerker moet van de verwerker eisen dat hij ervoor zorgt dat alle personen die gemachtigd zijn om de persoonsgegevens te verwerken, een passende geheimhoudingsplicht hebben.

4. Een verwerker mag slechts sub-verwerkers inschakelen indien de verwerkingsverantwoordelijke hier, vooraf, schriftelijk toestemming voor heeft gegeven. Wanneer de verwerkingsverantwoordelijke instemt met de aanstelling van sub-verwerkers, moeten die sub-verwerkers op dezelfde voorwaarden worden aangesteld als zijn vastgesteld in de verwerkersovereenkomst tussen de verwerkingsverantwoordelijke en de verwerker.

5. Een verwerker dient een register van de verwerkingsactiviteiten, ook wel **verwerkingsregister** genoemd, bij te houden. Dit register dient minimaal de volgende gegevens te bevatten:

- De naam en contactgegevens van:
  - de verwerkingsverantwoordelijke
  - indien van toepassing, de gezamenlijke verwerkingsverantwoordelijken en/of vertegenwoordiger van de verwerkingsverantwoordelijke, en

van de functionaris voor gegevensbescherming;
- De verwerkingsdoeleinden;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- De categorieën van ontvangers aan wie de persoonsgegevens zijn óf zullen worden verstrekt;
- Indien van toepassing: doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of internationale organisatie en de passende waarborgen;
- De van toepassing zijnde bewaartermijnen;
- Een omschrijving van de geïmplementeerde beveiligingsmaatregelen.

6. Verwerkers (en hun vertegenwoordigers, indien aanwezig) zijn verplicht om op verzoek samen te werken met toezichthoudende autoriteiten bij de uitvoering van haar taken.

7. De verwerker moet **passende technische en organisatorische beveiligingsmaatregelen** treffen om persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging of verlies, wijziging, ongeautoriseerde openbaarmaking of toegang. Afhankelijk

7. Passende technische en organisatorische beveiligingsmaatregelen. In het MedMij Afsprakenstelsel is een Normenkader informatiebeveiliging opgenomen waarin de informatiebeveiliging binnen het MedMij-netwerk uiteen is gezet. In de Deelnemersovereenkomst is aangegeven dat de Deelnemer de voor hem geldende afspraken uit het MedMij Afsprakenstelsel in dit kader doorvertaalt naar (sub)verwerkers. De Deelnemer staat er jegens de Stichting MedMij voor in dat de door hem ingeschakelde derde voor zijn Diensten en/of *Gegevensdiensten* alle verplichtingen uit de Deelnemersovereenkomst nakomt, onder andere dus de uitvoering van de afspraken in het MedMij Afsprakenstelsel, en is aansprakelijk voor het

van de verwerkingsactiviteiten kunnen de beveiligingsmaatregelen het volgende omvatten:

- pseudonimisering en versleuteling van persoonsgegevens;
- doorlopende beoordelingen van de beveiligingsmaatregelen;
- redundantie en back-up-mogelijkheden;
- regelmatig testen, beoordelen en evalueren van de beveiligingsmaatregelen.

Wat een passend niveau van beveiliging is, dient te worden getoetst aan de hand van de verwerkingsrisico's die met de verwerkingsactiviteit gepaard gaan.

8. De verwerker is verplicht om een inbeuk in verband met persoonsgegevens, ook wel **datalek** genoemd, zonder onredelijke vertraging te melden aan de verwerkingsverantwoordelijke.

9. Indien de verwerkingsverantwoordelijke waarvoor de verwerker persoonsgegevens verwerkt verplicht is om een **functionaris voor de gegevensbescherming** aan te stellen, werkt deze verplichting door op de verwerker.

NB. Indien een verwerker, in strijd met de AVG, zelf doeleinden en middelen van een verwerkingsactiviteit vaststelt, wordt de

handelen op grond van deze Overeenkomst van de door hem ingeschakelde derde.

9. Functionaris voor de gegevensbescherming. We raden verwerkers aan zelf te onderzoeken of zij een functionaris voor de gegevensbescherming aan moeten stellen doordat de verwerkingsverantwoordelijke hiertoe ook verplicht is.

	verwerker met betrekking tot die verwerking als de verwerkingsverantwoordelijke beschouwd.		

Architectuur en technische specificaties

1. Inleiding

Een onmisbaar deel van het MedMij Afsprakenstelsel betreft de verantwoordelijkheden die de deelnemers in het afsprakenstelsel hebben, elk in zijn eigen rol, tijdens het feitelijk verzorgen van het informatieverkeer tussen het Persoonsdomein en het Zorgaanbiedersdomein. Deze verantwoordelijkheden zijn opgenomen in de architectuur en de technische specificaties van het MedMij Afsprakenstelsel, die in deze pagina's uiteen worden gezet.

Vaak wordt er in de verantwoordelijkheden verwezen naar een specificatie. Dit kan een specifiek voor MedMij gespecificeerde usecase zijn, maar is vaak ook een standaard, vooral voor informatie. De specificatie zal niet in de verantwoordelijkheid zelf staan uitgeschreven; er zal naar verwezen worden.

De rollen en verantwoordelijkheden zijn om te beginnen bondig en stellig als regel geformuleerd. Pas in tweede instantie zijn ze voorzien van toelich-ting. De opzet is dus niet die van een verhalende uiteenzetting van het stelsel, maar die van een set afspraken, artikelsgewijs. Dat maakt de architectuur geschikt om als verlengstuk van de deelnemersovereenkomst te worden gebruikt. De allereerste vraag is: *Wat is de afspraak?* In tweede instantie spelen vragen als: *Waarom is hiervoor gekozen?* en *Wat betekent die afspraak?*

Waar in de beschrijving van de architectuur, de daarin bevatte rollen en verantwoordelijkheden en de toelichtingen daarop, met een naam wordt gerefereerd aan architectuurcomponenten, zoals die voorkomen bij het onderwerp horende diagrammen, wordt de naam *italiek* en met Beginkapitaal geschreven. Dat geldt ook voor de pad-expressies in de invarianten bij de Informatiemodellen. Variabelen in die pad-expressies staan ook *italiek*, maar beginnen met een kleine letter.

Sommige architectuurcomponenten worden ook vertegenwoordigd door een klasse, attribuut, element of type in de Informatiemodellen. Omdat de spelling van de namen in de Informatiemodellen formeler is, kan de naamgeving daar iets afwijken van die in de rest van de architectuur, in het gebruik van spaties en hoofdletters. In de Informatiemodellen beginnen alle namen met een hoofdletter. Midden in de namen verschijnen bovendien hoofdletters wanneer, en alleen wanneer, het daar resterende deel van de naam ook als aparte naam voorkomt.

Technische code-fragmenten worden in `monospace` geciteerd.

2. Coördinatie, regie en uitwisseling

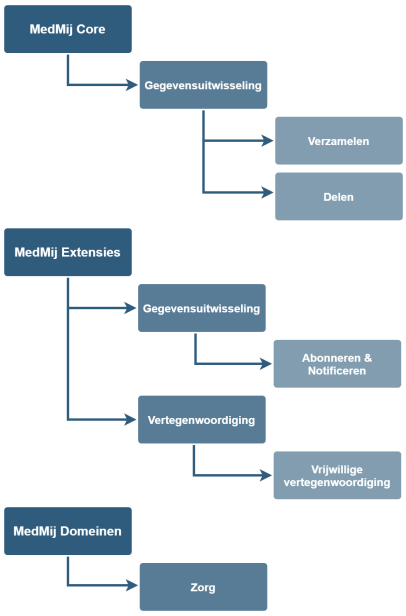
Het MedMij Afsprakenstelsel scheidt drie hoofdfuncties: *Regie*, *Uitwisseling* en *Coördinatie*. Al het gedrag van de betrokken rollen op deze lagen hoort bij één van deze drie hoofdfuncties. De hoofdfuncties hebben een onderlinge relatie. Aan de hoofdfuncties zijn beginselkeuzes verbonden.

3. MedMij Core, Extensies en Domeinen

MedMij is opgedeeld in de MedMij Core en MedMij Extensies. Domeinen gelden als aspecten over de Core en Extensies heen.

1. MedMij Core
    a. Gegevensuitwisseling
        i. Verzamelen en delen
2. MedMij Domeinen
    a. Zorg
3. MedMij Extensies
    a. Gegevensuitwisseling
        i. Abonneren & notificeren

b. Vertegenwoordiging
    i. Vrijwillige vertegenwoordiging



3.1. MedMij Core

De basis van de architectuur van het MedMij afsprakenstelsel wordt gevormd door de MedMij Core. Hierin staan rollen, functies en verantwoordelijkheden beschreven die voor het gehele afsprakenstelsel van belang zijn. Alles dat in de MedMij Core beschreven staat is verplicht. Als deelnemer moet je je aan deze regels houden. Hiermee wordt uitwisseling van gezondheidsgegevens vanuit de MedMij Core mogelijk gemaakt.

3.2. MedMij Extensies

Alle in de MedMij Core beschreven onderwerpen vormen de essentie van het MedMij afsprakenstelsel. Deze onderwerpen zijn noodzakelijk om de *Persoon* in de regie te stellen over de eigen gezondheidsgegevens. Extensies vormen een uitbreiding van functionaliteiten, waarmee de regie van de gebruiker uitgebouwd.

3.3. MedMij Domeinen

MedMij ondersteunt domeinen als aspecten over de MedMij Core en Extensies heen. Dit betekent dat per domein rollen en verantwoordelijkheden worden beschreven waaraan iedere deelnemer moet voldoen die in een domein werkzaam is.

> Als een deelnemer bijvoorbeeld *Dienstverlener Aanbieder* in het domein *Zorg*, dan geldt voor deze deelnemer een combinatie. In het domein *Zorg* staat de rol *Dienstverlener Zorgaanbieder* beschreven, met de bijbehorende verantwoordelijkheden. Deze moeten gecombineerd worden met de verantwoordelijkheden die beschreven staan in de *MedMij Core*, voor de rol *Dienstverlener Aanbieder*.

3.4. Abstractieniveaus

De onderwerpen worden beschreven volgens de basislagen van een architectuur.

3.4.1. Business

Om te beginnen moeten deelnemers er samen voor zorgen dat zich zekere bedrijfsprocessen voltrekken tussen het Persoonsdomein en het Zorgaanbiedersdomein. Deze bedrijfsprocessen gaan vooral over het verzamelen en delen van gezondheidsinformatie. Op dit abstractieniveau is nog geen sprake van geautomatiseerde afhandeling van deze processen, maar zijn de verantwoordelijkheden enkel nog

geformuleerd in termen van de inhoud van die processen en van de gezondheidsinformatie die daarin omgaat.

3.4.2. Applicatie

Op het volgende abstractieniveau, de applicatielaag, komt ter sprake dat, en hoe, deze bedrijfsprocessen met de erin omgaande gezondheidsinformatie, geautomatiseerd moeten worden uitgevoerd, in samenwerking tussen de rollen. Het is de meest complexe laag.

3.4.3. Technologie

Op het onderste abstractieniveau, de technologielaag, zijn de verantwoordelijkheden opgenomen op het gebied van de netwerkinfrastructuur. Hierbij worden de verschillende generieke type nodes beschreven.

4. Informatiemodellen

Een aparte pagina Informatiemodellen, met drie subpagina's, specificeert de conceptuele structuur van (een deel van) het begrippenapparaat van de architectuur van het MedMij Afsprakenstelsel en vertaalt die via logische modellen naar technische modellen van enkele componenten. Zo wordt tot op technisch niveau de interoperabiliteit op het MedMij-netwerk geborgd.

Coördinatie, regie en uitwisseling

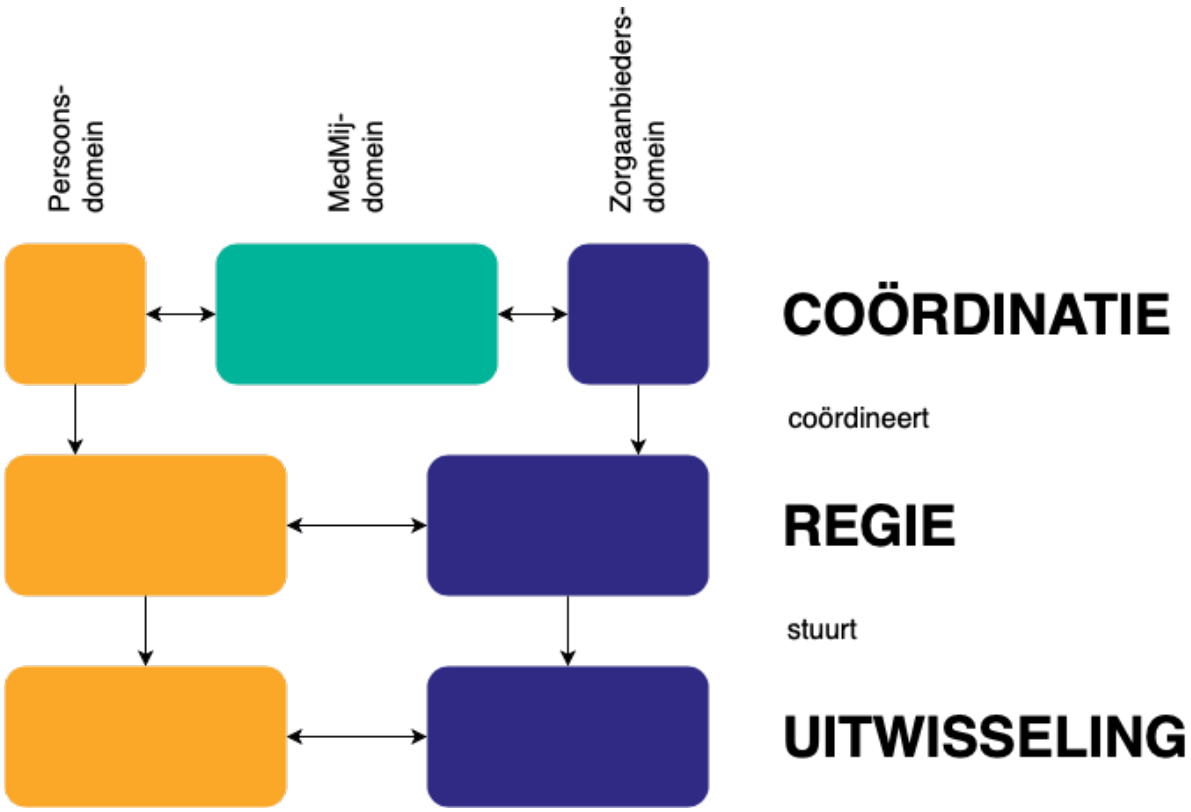
Scheiding tussen Regie, Uitwisseling en Coördinatie

Het MedMij Afsprakenstelsel scheidt drie hoofdfuncties: *Regie*, *Uitwisseling* en *Coördinatie*. Al het gedrag van de betrokken rollen op deze lagen hoort bij één van deze drie hoofdfuncties. De hoofdfuncties hebben een onderlinge relatie. Aan de hoofdfuncties zijn beginselkeuzes verbonden.

Centraal staat de *Regie*; hiermee voert de *Persoon* regie, in interactie met de *Aanbieder*, over (de uitwisseling van) zijn gezondheidsinformatie. Onder deze hoofdfunctie vallen bijvoorbeeld het geven van toestemming van de *Persoon* aan de *Aanbieder*, het authenticeren van de *Persoon* door de *Aanbieder*, het autoriseren van de *Dienstverlener persoon* door de *Aanbieder* en het aangaan, beëindigen en onderhouden van abonnementen. *Regie* leidt zo steeds tot overeenkomsten tussen *Persoon*, *Aanbieder* en *Dienstverlener persoon*, en is gebaseerd op vertrouwen in de identiteit van de anderen in de overeenkomst. De *Dienstverlener aanbieder* is geen partij in deze overeenkomsten, omdat deze geen verwerkingsverantwoordelijke is zoals wel de *Dienstverlener persoon*. De *Dienstverlener aanbieder* speelt wel een belangrijke uitvoerende rol in de totstandkoming van de overeenkomsten, als verwerker namens de *Aanbieder.*

Regie stuurt *Uitwisseling*. *Uitwisseling* geeft uitvoering aan de *Regie*. Deze tweede hoofdfunctie voert het feitelijke verkeer van gezondheidsinformatie uit, van *Aanbieder* naar *Dienstverlener persoon* (*Verzamelen* en *Notificeren*) of andersom (*Delen*). Alle uitwisseling vindt plaats conform gestandaardiseerde *Gegevensdiensten* en in het kader van een *Regie*-overeenkomst. *Regie* en *Uitwisseling* worden, conform principe 10, alleen uitgevoerd door partijen die onder de volledige verantwoordelijkheid vallen van een *Dienstverlener persoon* of *Dienstverlener aanbieder*, en dus decentraal. MedMij is zelf niet betrokken in de uitvoering van *Regie* of *Uitwisseling*.

Toch is een voorbereidende rol van MedMij nodig om de partijen in staat te stellen de onderlinge *Regie* tot stand te brengen. *Coördinatie* is de derde hoofdfunctie, die zorgt voor het vertrouwen tussen het Persoonsdomein en het Aanbiedersdomein, zodat deze van elkaar kunnen weten wat zij kunnen en mogen op het MedMij-netwerk. Deze functie wordt uitgevoerd met de *Catalogus*, die zegt welke *Gegevensdiensten* op enig moment op het MedMij-netwerk van kracht zijn, en vier lijsten (*Gegevensdienstnamenlijst*, *OAuth Client List*, *Whitelist* en *Aanbiederslijst*), die zeggen welke *Deelnemers* er zijn, en wat zij kunnen en mogen.



Business-laag

Op deze laag zijn worden de drie hoofdfuncties door de volgende rollen uitgevoerd.

hoofdfunctie	Persoonsdomein	MedMij-domein	Aanbiedersdomein
Coördinatie	• *Dienstverlener persoon*	• *MedMij Beheer*	• *Dienstverlener aanbieder*
Regie	• *Persoon* • *Dienstverlener persoon*	-	• *Dienstverlener aanbieder*
Uitwisseling	• *Persoon* • *Dienstverlener persoon*	-	• *Dienstverlener aanbieder*

Op deze laag worden de drie hoofdfuncties in de volgende usecases uitgevoerd.

hoofdfunctie	Persoonsdomein	MedMij-domein	Aanbiedersdomein
Coördinatie	• *Opvragen Gegevensdienstnamenlijst* • *Opvragen Aanbiederslijst*	• Opvragen Gegevensdienstnamenlijst • Opvragen Aanbiederslijst	• *Opvragen Gegevensdienstnamenlij* • Opvragen OAuth Client l

		• Opvragen OAuth Client List	
Regie	• *Verzamelen* (*authorization interface* en *token interface*) • *Delen* (*authorization interface* en *token interface*) • *Abonneren* • *Notificeren* (voor abonnements-*Notificaties*) • *Portabiliteitsrapport*	-	• *Verzamelen* (*authorization interface e token interface*), inclusief de beschikbaarheidsvoorwa • *Delen* (*authorization interface e token interface*), inclusief de ontvankelijkheidsvoorwa • *Abonneren* • *Notificeren* (voor abonnements-*Notificaties*)
Uitwisseling	• *Verzamelen (resource interface)* • *Delen (resource interface)* • *Notificeren* (voor *inhoudelijke Notificaties*)	-	• *Verzamelen (laatste fase* • *Delen (resource interfac* • *Notificeren* (voor *inhoudelijke Notificaties*)

Applicatielaag

Op deze laag zijn worden de drie hoofdfuncties door de volgende rollen uitgevoerd.

hoofdfunctie	Persoonsdomein	MedMij-domein	Zorgaanbiedersdomein
Coördinatie	• *DVP Server*	• *MedMij Registratie*	• *Authorization Server*
Regie	• *Persoon* • *User Agent* • *DVP Server* • *Notification Server* (voor subscription notifications) • *OAuth Resource Owner* • *OAuth Client*		• *Authorization Server* • *Subscription Server* • *Notification Client* (voor subscription notifications) • *OAuth Authorization Server* • *Authentication Client* • *Authentication Server*
Uitwisseling	• *Persoon* • *User Agent* • *DVP Server*		• *Resource Server* • *OAuth Resource Server* • *Notification Client* (voor resource notifications)

	• *Notification Server* (voor resource notifications) • *OAuth Resource Owner* • *OAuth Client*		

Op deze laag worden de drie hoofdfuncties op de volgende interfaces uitgevoerd. Elk interface hoort bij één hoofdfunctie.

hoofdfunctie	interface
Coördinatie	• Gegevensdienstnamenlijst interface • OAuth Client List interface • Aanbiederslijst interface
Regie	• user interface (Verklaringen) • authorization interface • token interface • subscription interface • subscription notification interface
Uitwisseling	• resource interface • resource notification interface

Beginselen

De architectuur van het MedMij Afsprakenstelsel hanteert de volgende beginselen ten aanzien van de hoofdfuncties.

1. **Eén interface, één hoofdfunctie.** Een interface hoort bij precies één hoofdfunctie. Bij voorkeur horen ook een rol en een usecase bij precies één hoofdfunctie. Deze voorkeur is sterker op de Applicatie-laag dan op de Business-laag. Deze voorkeur is bovendien minder sterk bij de gebruikersrollen in beide domeinen.
2. **Decentrale regie en uitwisseling.** Noch *MedMij Beheer* noch enige andere partij heeft een centrale of intermediaire rol in *Regie* of *Uitwisseling* tussen het Persoonsdomein en het Zorgaanbiedersdomein. Die intermediaire rol is er voor MedMij Beheer wel in *Coördinatie*. Dit beginsel is een uitwerking van principe 7.
3. **Geen sector-specifieke standaarden of oplossingen voor *Coördinatie* en *Regie*.** Voor *Coördinatie* en *Regie* gebruikt het MedMij Afsprakenstelsel geen sector-specifieke oplossingen of standaarden. Sector-specificiteit moet hier niet alleen qua inhoud begrepen worden, maar ook qua governance (van een standaard). Gezondheid houdt zich niet aan sectorale verkavelingen; de *Regie* erop moet niet sectoraal verkaveld worden, omdat dat de regie zou beperken. Voor *Uitwisseling* heeft sector-specificiteit evenmin de voorkeur, maar vraagt de realiteit erom sector-specifieke uitwisselstandaarden te gebruiken (zoals HL7 voor de zorgsector en bijvoorbeeld StUF voor het gemeentelijke veld). Verreweg de meeste informatie-inhoudelijke standaardisatie vindt binnen sectoren plaats. Dit beginsel laat principe 19 onverlet.
4. **Geen uitwisseling zonder regie.** Er vindt geen *Uitwisseling* plaats waaraan geen *Regie*-overeenkomst ten grondslag ligt. Mochten er *Uitwisselingen* in het MedMij Afsprakenstelsel moeten worden opgenomen die een andere legitimatie vereisen dan waarin *Regie* op enig moment voorziet,

moet die nieuwe legitimatie dus onder de hoofdfunctie *Regie* worden toegevoegd. *Regie* bieden aan *Personen* op hun gezondheid(sinformatie) is het hoofddoel van MedMij. *Coördinatie* voorziet slechts in wat noodzakelijk is om dat doel te bereiken.

5. **Uitwisseling gestandaardiseerd en gecoördineerd.** Al het verkeer in het kader van *Uitwisseling* vindt plaats op basis van gestandaardiseerde *Gegevensdiensten*, die in de *Catalogus* zijn opgenomen.
6. **Gegevensdienst als eenheid van *Regie.*** De eenheid van *Regie* tussen *Persoon* en *Aanbieder* is een hele *Gegevensdienst*. Een *Uitwisseling*, bijvoorbeeld een *Notificatie*, kan echter een kleinere eenheid betreffen, maar wel altijd als onderdeel van één *Gegevensdienst*. Ook elk Abonnement betreft één *Gegevensdienst.*
7. **Eén taal voor *Coördinatie.*** Alle functionaliteit van de hoofdfunctie *Coördinatie* is gestoeld op één gezamenlijke set informatiemodellen, die geordend zijn in drie lagen: conceptueel (metamodel), logisch (logische modellen) en technisch (XML-schema's). Deze informatiemodellen zijn onderdeel van het MedMij Afsprakenstelsel. Dat geldt niet voor de informatiestandaarden die voor de *Gegevensdiensten* gebruikt worden. Die zijn weliswaar per *Gegevensdienst* gestandaardiseerd, maar niet over alle *Gegevensdiensten* heen, op *Catalogus*-niveau, gestandaardiseerd, omdat dat MedMij zou invangen in één sector (zie beginsel 3).
8. **Toekomstvaste scheiding.** De scheiding tussen de drie hoofdfuncties vertegenwoordigt een structureel aspect van het evoluerende MedMij Afsprakenstelsel. Dat betekent dat, ondanks de grote implementatievrijheid van *Deelnemers*, zij hun implementatielast van nieuwe releases kunnen beperken door deze scheiding ook in hun implementatie-architectuur aan te brengen. De scheiding tussen de hoofdfuncties maakt de evolutie van het afsprakenstelsel voor *Deelnemers* voorspelbaarder.

MedMij Core

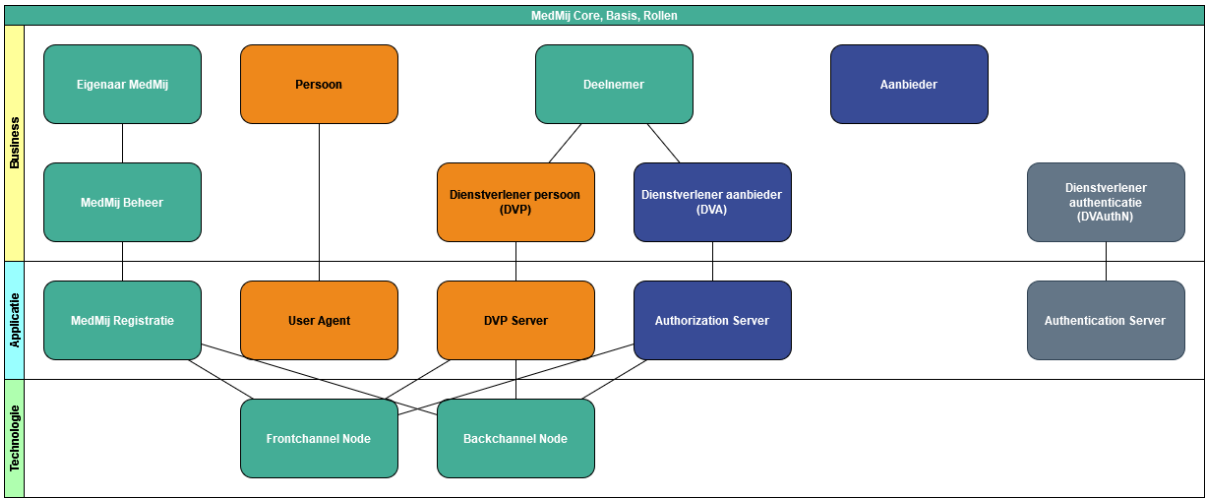
1. Inleiding

De basis van de architectuur van het MedMij afsprakenstelsel wordt gevormd door de MedMij Core. Hierin staan rollen, functies en verantwoordelijkheden beschreven die voor het gehele afsprakenstelsel van belang zijn. Alles dat in de MedMij Core beschreven staat is verplicht. Als deelnemer moet je je aan deze regels houden. Hiermee wordt uitwisseling van gezondheidsgegevens vanuit de MedMij Core mogelijk gemaakt.

2. Rollen

Het onderstaande diagram toont de rollen die vanuit de MedMij Core in de verschillende onderwerpen gebruikt worden. De rollen staan uitgewerkt in drie lagen van een Enterprise Architectuur, namelijk Business, Application en Technologie. De rollen in het MedMij Afsprakenstelsel zijn bijeen horende setjes verantwoordelijkheden. Rollen kunnen, over de lagen heen, aan elkaar gekoppeld zijn. Een rol gaat gepaard met één of meerdere onderliggende rollen.

Dat wil zeggen dat een rol in het algemeen wordt ingevuld met één of meer verbonden onderliggende rollen, al-dan-niet op een onderliggende laag. De rolbindingen vormen zo de ruggengraat van de architectuur van het MedMij Afsprakenstelsel.



In de bovenstaande plaat is allereerst de huisstijl van MedMij aangehouden, zodat

- oranje staat voor het Persoonsdomein;
- blauw staat voor het aanbiedersdomein en
- groen staat voor het MedMij-domein en de MedMij algemene elementen.

De grijze kleur staat voor externe rollen waarvan het MedMij Afsprakenstelsel gebruik maakt.

De verticale lijnen in de architectuur leggen de relatie tussen rollen. De relaties leggen de eindverantwoordelijkheid voor de uitvoering van verantwoordelijkheden bij de hogere rol.

3. Functies & gegevens

Onderstaand diagram toont de centrale functies die vanuit de MedMij Core worden aangeboden, welke rollen verantwoordelijk zijn voor het leveren van deze functies en welke gegevens door de functie geleverd worden.

Dit diagram toont alleen de verantwoordelijke rol, behorende bij een aangeboden functie. De rollen die de functie gebruiken worden benoemd in de uitwerking van de functie, bijvoorbeeld in een stroomdiagram.

MedMij Beheer is verantwoordelijk voor de levering van de functies rondom de te gebruiken lijsten. Hierbij gaat het om:

- Opvragen Gegevensdienstnamenlijst
- Opvragen Aanbiederslijst
- Opvragen Whitelist
- Opvragen OAuth Client List

Omdat een *Persoon* de regie voert over de eigen gezondheidsgegevens, moet een *Dienstverlener persoon* de gegevens beschikbaar stellen. Dit gebeurt vanuit de functie Raadplegen Dossier. Omdat deze functie door de *Dienstverlener persoon* zelf in te vullen is, staat deze niet verder uitgewerkt in het afsprakenstelsel. Hierbij moet wel voldaan worden aan de verantwoordelijkheden core.dossier.103 en core.dossier.104.

Dienstverlener aanbieder biedt aan *Dienstverlener persoon* twee functies, namelijk

- Verzamelen
- Delen

4. Verantwoordelijkheden

In de MedMij Core zijn verschillende rollen beschreven, die met elkaar de verschillende functies uitvoeren en gegevens uitwisselen. Hierbij gelden de verantwoordelijkheden, zoals in dit hoofdstuk benoemd.

De verantwoordelijkheden worden beschreven op de drie lagen van de architectuur, waarbij verantwoordelijkheden op de:

- businesslaag getoond worden als gele regels;
- applicatielaag getoond worden als blauwe regels;
- technologielaag getoond worden als groene regels.

Iedere verantwoordelijkheid heeft een unieke code, welke achter de regel wordt getoond. Verwijzingen naar de verantwoordelijkheid worden uitgevoerd vanuit deze unieke codes. De code is opgebouwd uit verschillende onderdelen.

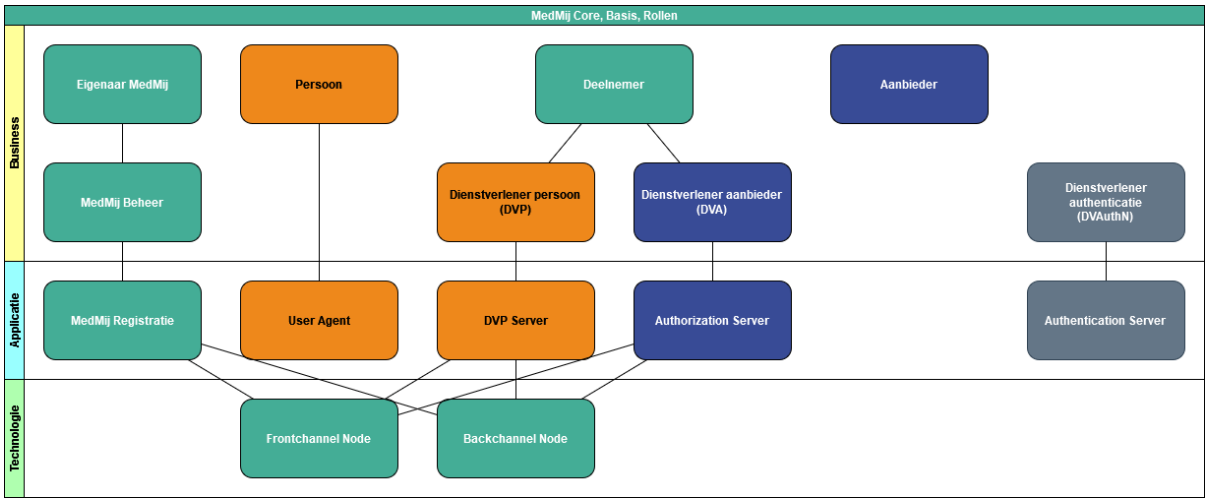
- Het eerste deel bestaat altijd uit 'core', om aan te geven dat het om verantwoordelijkheden gaat die in de MedMij Core beschreven staan.
- Het tweede deel verwijst naar het onderwerp waarop de verantwoordelijkheid van toepassing is.
- Het derde deel is een volgnummer, waarbij verantwoordenheden uit de:
    - businesslaag beginnen met 100;
    - applicatielaag beginnen met 200;
    - technologielaag beginnen met 300.

Rollen, Core

1. Rollenmodel

Het onderstaande diagram toont de rollen die vanuit de MedMij Core in de verschillende onderwerpen gebruikt worden. De rollen staan uitgewerkt in drie lagen van een Enterprise Architectuur, namelijk Business, Application en Technologie. De rollen in het MedMij Afsprakenstelsel zijn bijeen horende setjes verantwoordelijkheden. Rollen kunnen, over de lagen heen, aan elkaar gekoppeld zijn. Een rol gaat gepaard met één of meerdere onderliggende rollen.

Dat wil zeggen dat een rol in het algemeen wordt ingevuld met één of meer verbonden onderliggende rollen, al-dan-niet op een onderliggende laag. De rolbindingen vormen zo de ruggengraat van de architectuur van het MedMij Afsprakenstelsel.



In de bovenstaande plaat is allereerst de huisstijl van MedMij aangehouden, zodat

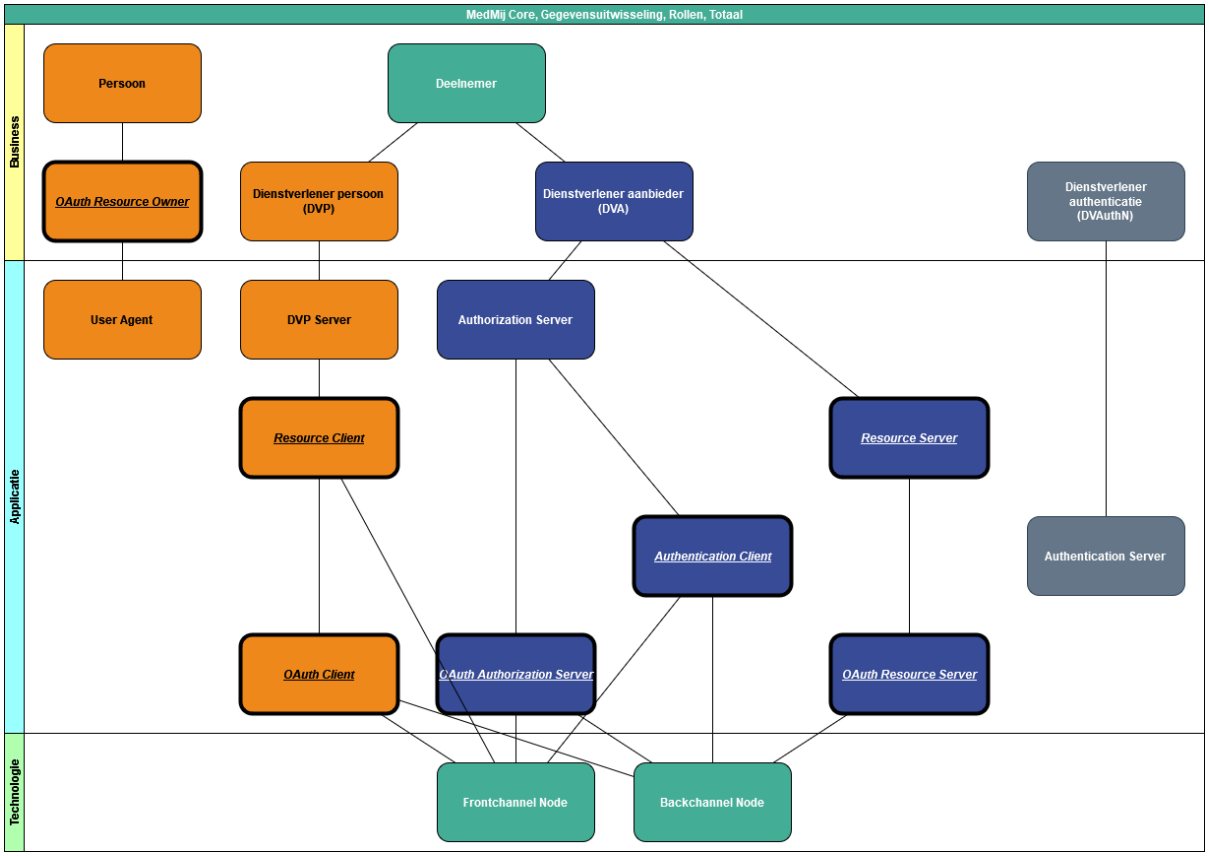
- oranje staat voor het Persoonsdomein;
- blauw staat voor het aanbiedersdomein en
- groen staat voor het MedMij-domein en de MedMij algemene elementen.

De grijze kleur staat voor externe rollen waarvan het MedMij Afsprakenstelsel gebruik maakt.

De verticale lijnen in de architectuur leggen de relatie tussen rollen. De relaties leggen de eindverantwoordelijkheid voor de uitvoering van verantwoordelijkheden bij de hogere rol.

1.1. Gegevensuitwisseling

Voor gegevensuitwisseling wordt het eerder getoonde rollenmodel uitgebreid met rollen die voor gegevensuitwisseling van toepassing zijn.



2. Roldefinities

2.1. Business

- **Eigenaar MedMij**
  De rechtspersoon die (eind)verantwoordelijk is voor de ontwikkeling en het beheer van het afsprakenstelsel en de informatiestandaarden die nodig zijn om gegevens in dezelfde taal te kunnen uitwisselen.
- **MedMij Beheer**
  De rechtspersoon die invulling geeft aan de operationele verantwoordelijkheden in het afsprakenstelsel, zoals het beheren en publiceren van een aanbiederslijst en gegevensdienstnamenlijst.
- **Persoon**
  Degene, 16 jaar of ouder, op wie Gezondheidsgegevens betrekking hebben die via MedMij worden uitgewisseld en tevens de Gebruiker in het Persoonsdomein.
- **Deelnemer**
  Een partij die dienstverlening aanbiedt binnen het MedMij Afsprakenstelsel. De *Dienstverlener persoon* en de *Dienstverlener aanbieder* zijn Deelnemer in het afsprakenstelsel en daarmee gebonden aan de afspraken, bekrachtigd door het tekenen van een deelnemersovereenkomst.
- **Dienstverlener persoon (DVP)**
  Dit betreft een rol in het MedMij Afsprakenstelsel. Levert een Persoonlijke gezondheidsomgeving, een dienst aan de *Persoon* voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de *Aanbieder* mogelijk maakt middels het MedMij Afsprakenstelsel.
- **Dienstverlener aanbieder (DVA)**
  Dit betreft een rol in het MedMij Afsprakenstelsel. Levert Diensten aan de *Aanbieder* gerelateerd aan de uitwisseling tussen *Persoon* en *Aanbieder* en committeert zich hiervoor aan de naleving van de afspraken van het MedMij Afsprakenstelsel.

- **Dienstverlener authenticatie (DVAuthN)**
  De Aanbieder is verplicht bij het verstrekken van gegevens vanuit een gezondheidsdossier de identiteit van de persoon te verifiëren, al dan niet aan de hand van het burgerservicenummer (BSN). MedMij gebruikt hiervoor de door het ministerie van Ministerie van Binnenlandse Zaken en Koninkrijksrelaties toegelaten authenticatiemiddelen. Vooralsnog is DigiD het enige toegelaten middel voor dit doel.
- **Aanbieder**
  Aanbieder is de term waarmee een grote diversiteit aan dienstverleners wordt bedoeld, die vanuit hun diensten gezondheidsinformatie kunnen aanbieden en ontvangen.

- **OAuth Resource Owner**
  Een *OAuth Resource Owner* is een *Persoon* die een *OAuth Client* autoriseert voor toegang tot een *OAuth Resource Server*. De toegang is beperkt tot het bereik van de verleende autorisatie.

2.2. Applicatie

- **MedMij Registratie**
  MedMij Registrati is de applicatie voor de administratie van Deelnemers, de gegevensdiensten die worden aangeboden en de endpoints die hierbij horen. Deze informatie wordt uitgegeven in de verschillende lijsten.
- **User Agent**
  De applicatie die de *Persoon* gebruikt om de MedMij functies uit te voeren.
- **DVP Server**
  De DVP Server verzamelt en deelt gezondheidsgegevens op verzoek van de *Persoon* en stelt hiermee het *Dossier* van de Persoon samen.
- **Authorization Server**
  De Authorization Server controleert of de *Persoon* voor de applicatie toegangsrechten heeft. Indien de *Persoon* toestemming geeft om gegevens uit te wisselen met de *DVP Server*, dan wordt deze toestemming vastgelegd en voor uitwisseling gecontroleerd.
- **Authentication Server**
  De Authentication Server controleert de identiteit van de *Persoon*.

- **Resource Client**
  De *Resource Client* is de applicatie die toegang nodig heeft tot een *Resource Server*.
- **OAuth Client**
  Een *OAuth Client* is een *Resource Client* die gebruik maakt van het OAuth 2.0 raamwerk.
- **Authentication Client**
  Een *Authentication Client* is een applicatie die gebruik maakt van een *Authentication Server* om de identiteit van een *OAuth Resource Owner* vast te stellen.
- **Resource Server**
  De *Resource Server* is de applicatie waar gegevens kunnen worden verzameld, of waarmee gegevens gedeeld kunnen worden.
- **OAuth Resource Server**
  Een *OAuth Resource Server* is een *Resource Server* die gebruik maakt van het OAuth 2.0 raamwerk.

2.3. Technologie

- **Frontchannel Node**
  Een Frontchannel Node communiceert met de *User Agent* van de *Persoon*, waarbij de communicatie internet facing is. De rol van *User Agent* wordt hierbij ingevuld door een webbrowser.
- **Backchannel Node**
  Een Backchannel Node communiceert met andere backchannel nodes, waarbij identificatie geschied door gebruik te maken van de verschillende lijsten die door MedMij Registratie worden geboden.

3. Persoonsdomein

3.1. Business

In het Persoonsdomein is er naast de rol *Dienstverlener persoon* ook de rol *Persoon.* Hoewel *Dienstverlener persoon* namens *Persoon* handelt, kan *Persoon* niet ongenoemd blijven in de afspraken op deze en onderliggende lagen. Dat komt doordat *Persoon* niet enkel de gebruiker van *Dienstverlener persoon* is, maar allereerst het onderwerp van de gezondheidsinformatie die *Deelnemers* ter beschikking moet stellen; daarvoor is authenticatie en autorisatie nodig. In de architectuur van het afsprakenstelsel heeft *Persoon* een operationele rol bij authenticatie en autorisatie van het gegevensverkeer.

3.2. Application

In het persoonsdomein zijn twee rollen onderscheiden: de *User Agent* en de *DVP Server*. Dat is nodig om de verbinding te kunnen leggen met de rollen volgens OAuth. *User Agent* is de front-end-rol voor de *DVP Server* , en kan bijvoorbeeld in een browser zijn geïmplementeerd. Zoals ook elders in het MedMij Afsprakenstelsel gaat het hier om rollen, om setjes verantwoordelijkheden dus, niet om implementatiecomponenten.

4. Aanbiedersdomein

4.1. Business

In het Aanbiedersdomein is er naast de rol *Dienstverlener aanbieder* ook de rol *Aanbieder*. Deze rol wordt operationeel geheel vertegenwoordigd door de *Dienstverlener aanbieder*.

4.2. Application

Waar een *Persoon* zelf operationeel betrokken wordt in het informatieverkeer — namelijk om zich te laten authenticeren, en het verkeer te laten autoriseren — laat de *Aanbieder* zich operationeel geheel vertegenwoordigen door zijn *Dienstverlener* en diens *Authorization Server* en *Resource Server*. Ook al zal in veel gevallen de gezondheidsinformatie uiteindelijk uit een achterliggend systeem worden betrokken, voor het MedMij Afsprakenstelsel is dat geen kwestie. Het is voldoende om bij de *Authorization Server* en *Resource Server* de eindverantwoordelijkheid neer te leggen (black box).

De genoemde servers treden op namens alle eventuele achterliggende systemen in het Aanbiedersdomein, zoals xIS'en. Die achterliggende complexiteit is een black box. Het is mogelijk dat een individuele xIS optreedt voor beide servers, maar dan moeten ook alle met deze rollen verbonden verantwoordelijkheden zijn ingevuld, zowel de direct verbonden verantwoordelijkheden (op de Applicatielaag) als de indirect verbonden verantwoordelijkheden (op de lagen erboven en eronder).

Hoezeer ook alle eindverantwoordelijkheden gedragen worden door de *Dienstverleners* die deelnemer zijn in het MedMij Afsprakenstelsel, zij kunnen ervoor kiezen de uitvoering van die verantwoordelijkheden deels of zelfs geheel uit te besteden. In een mogelijke systeemarchitectuur maken meerdere *Resource Server*-systemen gebruik van een-zelf-de (al dan niet uitbesteed) *Authorization Server*-systeem. Het is mogelijk dat die *Resource Server*-systemen samen onder de eindverantwoordelijkheid van één *Dienstverlener aanbieder* vallen, met de uitvoering al dan niet uitbesteed. Het is ook mogelijk dat twee verschillende *Dienstverlener aanbieders* voor de *Authorization Server* gebruik maken van eenzelfde onderaannemer.

De architectuur heeft zo maximale ruimte aan de eigen businessmodellen en architecturen van *Dienstverlener aanbieder* willen geven zonder daarbij de interoperabiliteit en strakke eindverantwoordelijkheden geweld aan te doen.

> Een rol is nadrukkelijk geen component of systeem. Menige rol wordt weliswaar door componenten en systemen gerealiseerd, maar hoe dat precies gebeurt, en hoeveel en welke componenten- of systeemarchitectuur daarvoor wordt gebruikt is aan de *Dienstverlener*, zolang deze zijn rollen, op

alle lagen, naar behoren speelt, dat wil zeggen, de verantwoordelijkheden van die rollen draagt. Zo wordt aan *Dienstverleners*, in beide domeinen, volop ruimte geboden een businessmodel naar eigen inzicht te kiezen, waarin volop ruimte is voor onderaannemers, zolang de eindverantwoordelijkheid jegens het MedMij Afsprakenstelsel maar onvervreemdbaar bij de *Dienstverlener* blijft liggen.

5. MedMij-Verkeer

Al het *MedMij-verkeer* is over domeingrenzen. Verkeer binnen het *Persoonsdomein* of het *Aanbiedersdomein* maakt geen deel uit van *MedMij-verkeer*. Ook authenticatieverkeer is uitgesloten, omdat het MedMij Afsprakenstelsel geen eisen oplegt over welke (externe) *Authentication Server* wordt gebruikt. Het MedMij Afsprakenstelsel vereist dát er een passende authenticatie door *Aanbieder* moet plaatsvinden, maar het verkeer dat daarvoor nodig is — tussen *Authorization Server*, *Authentication Server* en *User Agent* — is geen MedMij-verkeer. Het is de *Aanbieder* die niettemin als verwerkingsverantwoordelijke verantwoordelijk blijft voor een passende keuze van een *Authentication Server* en voor het laten inrichten van het authenticatieverkeer.

Functies en gegevens, Core

1. Inleiding

Onderstaand diagram toont de centrale functies die vanuit de MedMij Core worden aangeboden, welke rollen verantwoordelijk zijn voor het leveren van deze functies en welke gegevens door de functie geleverd worden.

Dit diagram toont alleen de verantwoordelijke rol, behorende bij een aangeboden functie. De rollen die de functie gebruiken worden benoemd in de uitwerking van de functie, bijvoorbeeld in een stroomdiagram.

MedMij Beheer is verantwoordelijk voor de levering van de functies rondom de te gebruiken lijsten. Hierbij gaat het om:

- Opvragen Gegevensdienstnamenlijst
- Opvragen Aanbiederslijst
- Opvragen Whitelist
- Opvragen OAuth Client List

Omdat een *Persoon* de regie voert over de eigen gezondheidsgegevens, moet een *Dienstverlener persoon* de gegevens beschikbaar stellen. Dit gebeurt vanuit de functie Raadplegen Dossier. Omdat deze functie door de *Dienstverlener persoon* zelf in te vullen is, staat deze niet verder uitgewerkt in het afsprakenstelsel. Hierbij moet wel voldaan worden aan de verantwoordelijkheden core.dossier.103 en core.dossier.104.

Dienstverlener aanbieder biedt aan *Dienstverlener persoon* twee functies, namelijk

- Verzamelen
- Delen

1.1. Lijsten

In het MedMij Afsprakenstelsel worden, ten behoeven van de hoofdfunctie *Coördinatie*, vier lijsten gebruikt voor de interoperabiliteit en het vertrouwen tussen het Persoonsdomein en het Aanbiedersdomein.

lijst	afkorting	wordt opgehaald en gebruikt door		informatie-inhoud
		Dienstverlener Persoon	Dienstverlener Aanbieder	
Aanbiederslijst	ZAL	X		welke *Aanbieders* welke *Gegevensdiensten* aanbieden, en eventueel ook *Abonnementen* daarop, en op welke adressen zij die laten laten ontsluiten, gegeven een zekere *Interfaceversie*
OAuth Client List	OCL		X	de namen van *Dienstverlener persoon*, welke *Gegevensdiensten* zij mogen gebruiken en naar welke adressen mogelijk *Notificaties* in het kader van *Abonnementen* op die *Gegevensdiensten* kunnen worden gestuurd, gegeven een zekere *Interfaceversie*
Gegevensdienstnamenlijst	GNL	X	X	de gebruiksvriendelijke namen van *Gegevensdiensten*
Whitelist	WHL	X	X	welke *Nodes* actief mogen zijn op het MedMij-netwerk

2. Beschikbaarheids- en ontvankelijkheidsvoorwaarde

Hieronder worden de vroege en de late variant vergeleken vanuit de perspectieven van dataminimalisatie en gebruiksvriendelijkheid. Beide aspecten moeten vanuit het perspectief van de gehele usecase en alle

betrokken rollen beschouwd worden: een keuze tussen de vroege en de late variant heeft effecten op meerdere plaatsen tegelijk. De afweging onderscheidt vier situaties, afhankelijk van twee vragen:

- Acht de *Aanbieder* (zich voor) de informatie (uitein-delijk) beschikbaar/ontvankelijk?
- Geeft de *Persoon* (uiteinde-lijk) toestemming?

De late varianten verschillen overigens subtiel tussen zowel de functies Verzamelen en Delen. In Delen is de late variant in vergelijking nog een stap vroeger dan in de functie Verzamelen. Dat komt omdat anders een verwerking (namelijk: plaatsing) van gezondheidsinformatie zou gebeuren door de *Resource Server* nog voordat zou blijken dat de *Aanbieder* hiervoor niet ontvankelijk is. In de functie Verzamelen kan het een stapje later, omdat de te voorkomen actie pas de uitwisseling met de *DVP Server* is.

De twee varianten laten zich als volgt vergelijken inzake dataminimalisatie.

<table>
<tr><th></th><th>(uiteindelijk) wel beschikbaar /ontvankelijk</th><th>(uiteindelijk) niet beschikbaar/ontvankelijk</th></tr>
<tr><td>(uiteindelijk) wel toestemming</td><td rowspan="2">Voor zover er aparte geautoma-ti-seerde logica worden ge-bruikt voor een toets op beschikbaarheid of ontvankelijkheid vraagt de vroege variant ex-tra ver-keer ten opzichte van de late variant, namelijk tussen Autho-ri-zation Ser-ver en de com-ponent-(en) die zij voor het uitvoe-ren van die toets aan-spreekt. Dat ver-keer speelt zich wel geheel binnen de verantwoordelijkheid van een enkele verwerkingsverantwoordelijke af; er vindt geen verstrekking plaats.
De Authorization Server komt alleen in de vroege variant extra te weten dat behandel-relatie en leef-tijd in orde zijn. In de late variant komt alleen de Resource Server dat te weten. Dat laat onverlet dat beide onder dezelfde eindverantwoordelijke Dienstverlener aanbieder vallen.</td><td>In de late variant vindt, in tegenstelling tot in de vroege, al het verkeer na de au-thenti-catie (de toe-stem-mingsvraag, het uit-de-len van authoriza-tion code en ac-cess to-ken en het aan-spreken van de Resour-ce Ser-ver) onnodig plaats. Dit verkeer strekt zich uit over verantwoordelijkheidsgrenzen.
In de late variant krijgt de DVP Server, onnodig, meer over de beschikbaarheid /ontvankelijkheid, en dus over de Persoon, te weten van de Resource Server dan in de vroege variant van de Authorization Server. In de vroege variant kan de betreffende uitzondering immers, vanuit de DVP Server bezien, ook door falende authenticatie of weigering van toestemming veroorzaakt zijn. In de late variant komt de DVP Server echter wel te weten, door het ontvangen van de onnodige authorization code, dat er sprake is van zowel een behandelrelatie als een toereikende leeftijd.</td></tr>
<tr><td>(uiteinde-lijk) geen toestemming</td><td>In de late variant vindt, in tegenstelling tot in de vroege, een overbodige toe-stemmingsvraag plaats. Dit verkeer vindt plaats over het relatief onveilige frontchannel.</td></tr>
</table>

De twee varianten laten zich als volgt vergelijken inzake gebruiksvriendelijkheid.

	(uiteindelijk) wel beschikbaar /ontvankelijk	(uiteindelijk) niet beschikbaar/ontvankelijk
(uiteindelijk) wel	geen verschil	In de vroege variant is de *Persoon* onmiddellijk op de hoogte, zodat deze:

toestemming		• geen onnodige en verwarrende handeling (betekenisloze toestemming) met rechtsgevolgen hoeft uit te voeren, zoals in de late variant; • preciezer dan in de late variant op de hoogte raakt van waarom een uitwisseling faalt. In de late variant kan dat falen andere redenen hebben, zodat de *Persoon* voor opheldering op ondersteuningsvragen aangewezen zou zijn, die wellicht zelfs aan de *Aanbieder* gericht worden. In de vroege variant zijn Uitzonderingen 2, 3 en 4 in *Verzamelen* en *Delen* weliswaar samengenomen in één melding naar de *DVP Server*, zodat deze het onderscheid tussen falende authenticatie, falende autorisatie en falende beschikbaarheid /ontvankelijkheid niet kan maken. De *Persoon* zelf echter kent vanwege zijn/haar voorafgaande rechtstreekse interactie met de *Authorization Server* het resultaat van de authenticatie en de autorisatie wel, en kan dus alsnog uit deze gecombineerde melding, buiten medeweten van de *DVP Server*, afleiden of er sprake was van falende beschikbaarheid/toegankelijkheid.
(uiteindelijk) geen toestemming		In de vroege variant is de *Persoon* onmiddellijk op de hoogte en hoeft deze geen onnodige en verwarrende handeling (holle afwijzing) uit te voeren, zoals in de late variant.

De gevallen waarin de *Aanbieder* (zich voor) de informatie beschikbaar/ontvan-kelijk acht zijn, uitgaande van redelijk gedrag van de *DVP Server*, waarschijnlijk talrijker dan die waarin dat niet het geval is. Anderzijds wegen de nadelen van de vroege variant voor eerstgenoemde gevallen licht, omdat het zorgaanbiedersdomein en de *Authorization Server* om andere redenen al afdoende beveiligd moeten zijn, al is het maar vanwege het gebruik van het BSN. Bovendien is er alleen sprake van extra verkeer voor zo-ver geautomatiseerde logica wordt ingezet en daarvoor rollen anders dan de *Authorization Server*, en dus buiten het MedMij Afsprakenstelsel, worden aangesproken.

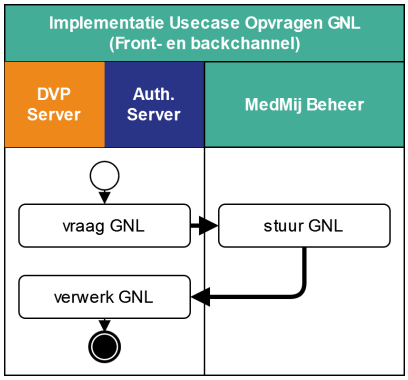
In deze release adviseert het MedMij Afsprakenstelsel daarom de vroege variant, vanwege bovengenoemde analyse. Het MedMij Afsprakenstelsel staat echter ook de late variant toe, om *Dienstverleners aanbieder* zowel de gelegenheid te geven snel aan te sluiten als de tijd om te overwegen hoe de vroege variant op termijn geïmplementeerd zou kunnen worden.

Opvragen Gegevensdienstnamenlijst

1. Inleiding

In de stroomdiagrammen, en op andere plekken in dit afsprakenstelsel wordt met de afkorting GNL verwezen naar de Gegevensdienstnamenlijst.

2. Applicatie- en technologielaag



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen. In de linkerbaan betekent dat: één *DVP Server* of één *Authorization Server*.

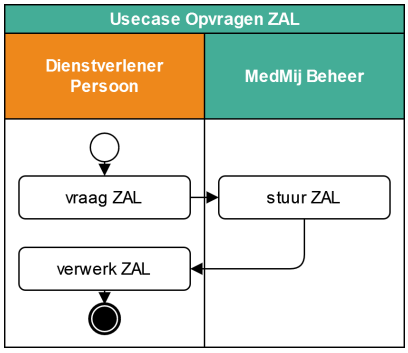
Beide interacties met *MedMij Registratie* zijn backchannel-verkeer.

Opvragen Aanbiederslijst

1. Inleiding

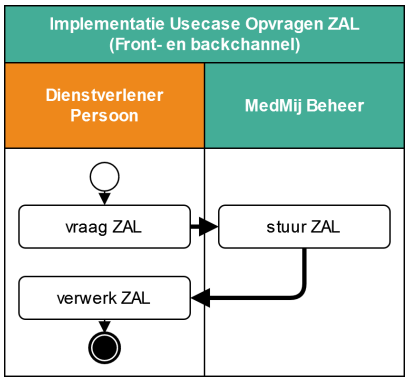
In de stroomdiagrammen, en op andere plekken in dit afsprakenstelsel wordt met de afkorting ZAL verwezen naar de Aanbiederslijst

2. Businesslaag



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

3. Applicatie- en technologielaag



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

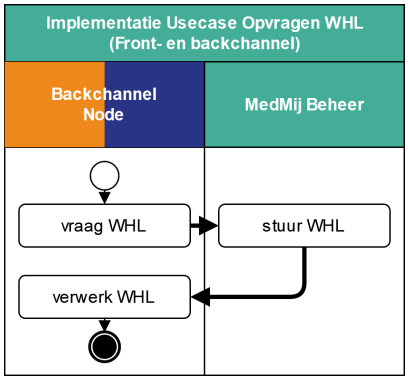
Beide interacties met *MedMij Registratie* zijn backchannel-verkeer.

Opvragen Whitelist

Inleiding

In de stroomdiagrammen, en op andere plekken in dit afsprakenstelsel wordt met de afkorting WHL verwezen naar de Whitelist.

Applicatie en technologielaag



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

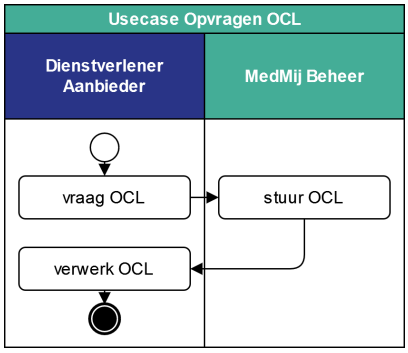
Beide interacties met *MedMij Registratie* zijn backchannel-verkeer.

Opvragen OAuth Client List

1. Inleiding

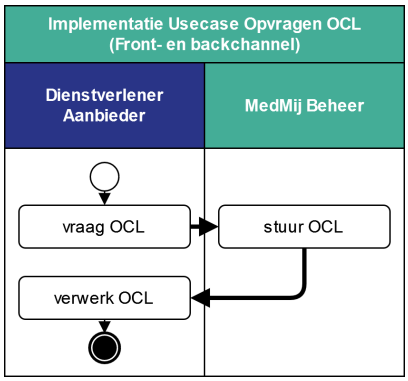
In de stroomdiagrammen, en op andere plekken in dit afsprakenstelsel wordt met de afkorting OCL verwezen naar de OAuth Client List.

2. Businesslaag



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

3. Applicatie- en technologielaag



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

Beide interacties met *MedMij Registratie* zijn backchannel-verkeer.

Verzamelen

1. Inleiding

In de platen hieronder staat het stroomdiagram van de functie *Verzamelen*:

- De happy flow van de usecase verzamelen
- De implementatie van de usecase verzamelen
- De implementatie van het front- en backchannelverkeer.

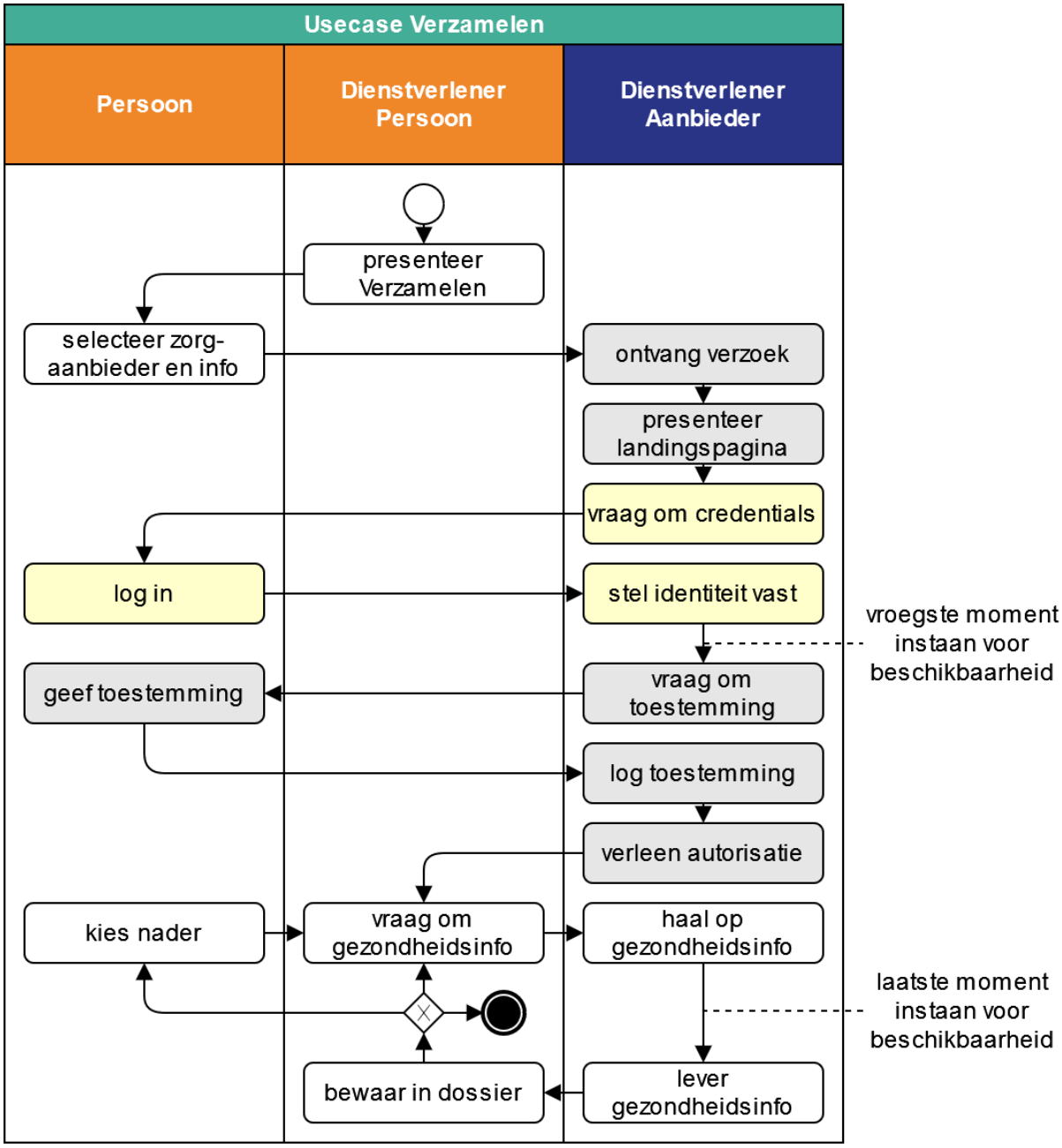
De stroomdiagrammen tonen alleen de situatie waarin alle acties slagen tot en met het uiteindelijke verzamelen van de gezondheidsinformatie (de zogenaamde happy flow). De oranje banen horen, conform de MedMij-huisstijl tot het Persoonsdomein, de blauwe tot het Aanbiedersdomein.

2. Businesslaag

Menig actie in het stroomdiagram is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow; de zachtgeel gekleurde acties vormen samen de authenticatieflow.

Omdat het stroomdiagram alleen de happy flow bevat, worden daarna de uitzonderingen beschreven.

2.1. Stroomdiagram



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De totale procesgang van de usecase *Verzamelen* kent de volgende stappen:

- De *Dienstverlener persoon* presenteert aan de *Persoon* de mogelijkheid om te verzamelen.
- De *Persoon* kiest expliciet de *Aanbieder*, waarbij hij de informatie wenst te verzamelen, en de specifiek e *Gegevensdienst(en)*. Daarvoor kunnen desgewenst de *Gegevensdienstnamen* worden gebruikt uit de *Gegevensdienstnamenlijst*. Het verzoek gaat naar de passende *Dienstverlener aanbieder*.
- De *Dienstverlener aanbieder* ontvangt de *Persoon*.
- De *Dienstverlener aanbieder* laat de *Persoon* zich authenticeren.
- Wanneer de *Persoon* de authenticatie heeft afgebroken geeft de *Dienstverlener aanbieder* de mogelijkheid alsnog te authenticeren of de flow af te breken.

- Dan breekt het moment aan waarop de *Dienstverlener aanbieder* op zijn vroegst ervoor instaat dat de *Aanbieder* voor tenminste één van de gevraagde *Gegevensdiensten* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft, of anders de happy flow afbreekt. Het MedMij Afsprakenstelsel adviseert de beschikbaarheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. In deze release staat het MedMij Afsprakenstelsel het toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment.
- De *Dienstverlener aanbieder* vraagt aan de *Persoon* of hij toestemming geeft tot het verstrekken van de gevraagde informatie aan de *Dienstverlener persoon*. Deze vraag staat op de pagina Toestemmingsverklaring.
- De *Dienstverlener aanbieder* logt die toestemming en geeft een autorisatie af aan de *Dienstverlener persoon*.
- Nu kan de *Dienstverlener persoon* de *Dienstverlener aanbieder* vragen om de gezondheidsinformatie.
- Uiterlijk na de ontvangst van het verzoek zal de *Dienstverlener aanbieder* ervoor instaan dat de *Aanbieder* voor de betreffende *Gegevensdienst(en)* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft, of anders de happy flow afbreken.
- Bij ontvangst slaat de *Dienstverlener persoon* die informatie op in het persoonlijke dossier.
- Mocht een *Gegevensdienst* waartoe de *Dienstverlener persoon* is geautoriseerd uit meerdere *Transacties* bestaan (zie hiervoor de Catalogus), dan bevraagt de *Dienstverlener persoon* de *Dienstverlener aanbieder* daarna mogelijk opnieuw voor de nog resterende *Transacties*, eventueel na nieuwe interactie met de *Persoon*. Hetzelfde geldt wanneer de *Dienstverlener persoon* is geautoriseerd voor meerdere *Gegevensdiensten* van de betreffende Aanbieder.
- Bij de informatie wordt ook de meta-informatie opgeslagen die wordt bedoeld in verantwoordelijkheid core.logging.100 en core.logging.101

De beschikbaarheidsvoorwaarde hoort bij *Regie*, niet bij *Uitwisseling*. De voorwaarde geeft de *Aanbieder* ruimte om deel te nemen in aan de *Persoon* gegeven *Regie*. Omdat echter bestaande implementatie-architecturen veelal uitwisseling centraal zetten, en niet *Regie*, hebben zij moeite de beschikbaarheidsvoorwaarde in de regiefase te implementeren. Daarom biedt het MedMij Afsprakenstelsel vooralsnog de gelegenheid om deze in de uitwisselingsfase te implementeren.

2.2. Uitzonderingen op de Happy flow van de usecase

In onderstaande tabel staan de uitzonderingssituaties beschreven. Alle worden door de *Dienstverlener aanbieder* ontdekt. Om te voorkomen dat de *Dienstverlener persoon* informatie over het bestaan van behandelrelaties verkrijgt zonder dat daarvoor (al) toestemming is gegeven, moet het onderscheid tussen de uitzonderingen 2, 3 en 4 niet te maken zijn door de *Dienstverlener persoon*.

Op de Applicatielaag zullen, bij de usecase-implementatie Verzamelen, deze uitzonderingen opnieuw ter sprake komen, maar nu ook met hun precieze implementatie en formaat van de foutmeldingen.

Of de *Aanbieder* de gevraagde gezondheidsinformatie beschikbaar stelt aan de *Persoon*, is om te beginnen een zaak tussen de *Aanbieder* en *Persoon*, die daarvoor een behandelrelatie moeten hebben. Gegeven zo'n behandelrelatie is er wetgeving van toepassing op deze ter beschikkingstelling. Daarbinnen is eigen beslisruimte voor de *Aanbieder*. Omdat *Aanbieder* en *Persoon* evenwel geen *Deelnemers* in het MedMij Afsprakenstelsel zijn, specificeert het MedMij Afsprakenstelsel niet de exacte logica van de beslissing om de gezondheidsinformatie al dan niet ter beschikking te stellen. Om privacy-redenen vereist het MedMij Afsprakenstelsel echter wel dat er een behandelrelatie moet (hebben) bestaan waarbij de betreffende gezondheidsinformatie hoort én dat de *Persoon* minstens zestien jaar oud is (zie uitzondering Verzamelen 3).

Voor het verstrekken van gegevens aan een minder dan zestienjarige moet toestemming of een machtiging tot toestemming worden verleend door degene die de ouderlijke verantwoordelijkheid of de wettelijke verantwoordelijkheid voor de minder dan zestienjarige draagt. Omdat in dergelijke toestemmingen of machtigingen nog niet is voorzien in deze versie van het MedMij afsprakenstelsel, kan deze controle

vooralsnog als onderdeel van de beschikbaarheidsvoorwaarde worden opgevat. Wanneer een toekomstige release van het MedMij afsprakenstelsel wel zulke toestemmingen of machtigingen omvat, zal de leeftijdsvoorwaarde gescheiden moeten worden van de beschikbaarheidsvoorwaarde.

nr.	uitzondering	actie	vervolg
Verzamelen 1	*Dienstverlener aanbieder* vindt het ontvangen verzoek ongeldig.	*Dienstverlener aanbieder* informeert *Dienstverlener persoon* over deze uitzondering. *Dienstverlener persoon* informeert daarop *Persoon* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
Verzamelen 2	*Dienstverlener aanbieder* kan de identiteit van de *Persoon* niet vaststellen.	*Dienstverlener aanbieder* informeert *Dienstverlener persoon* dat verzoek niet wordt ingewilligd.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
Verzamelen 3	*Dienstverlener aanbieder* stelt op enig moment vast dat van *Persoon* bij *Aanbieder* geen gezondheidsinformatie voor die *Gegevensdienst* beschikbaar is. Hiervan is in elk geval sprake indien hetzij: • er geen behandelrelatie is aan te wijzen als grondslag voor het verzamelen; • *Persoon* nog geen zestien jaar oud is. Zie de toelichting op Beschikbaarheids- en ontvankelijkheidsvoorwaarde.		
Verzamelen 4	De voorgelegde Toestemmingsverklaring wordt niet afgegeven.		
Verzamelen 5	*Dienstverlener aanbieder* kan het antwoord op de toestemmingsvraag niet vaststellen.	*Dienstverlener aanbieder* informeert *Dienstverlener persoon* over deze uitzondering. *Dienstverlener persoon* informeert daarop *Persoon* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
Verzamelen 6	*Dienstverlener aanbieder* kan, zelfs na toestemming, de gezondheidsinformatie alsnog niet ter beschikking stellen aan de *Dienstverlener persoon*.	*Dienstverlener aanbieder* informeert *Dienstverlener persoon* over deze uitzondering. *Dienstverlener persoon*	Mocht de gezondheidsinformatie deels wel (geautoriseerd) ter beschikking staan, dan kan de flow dat nog verzorgen.

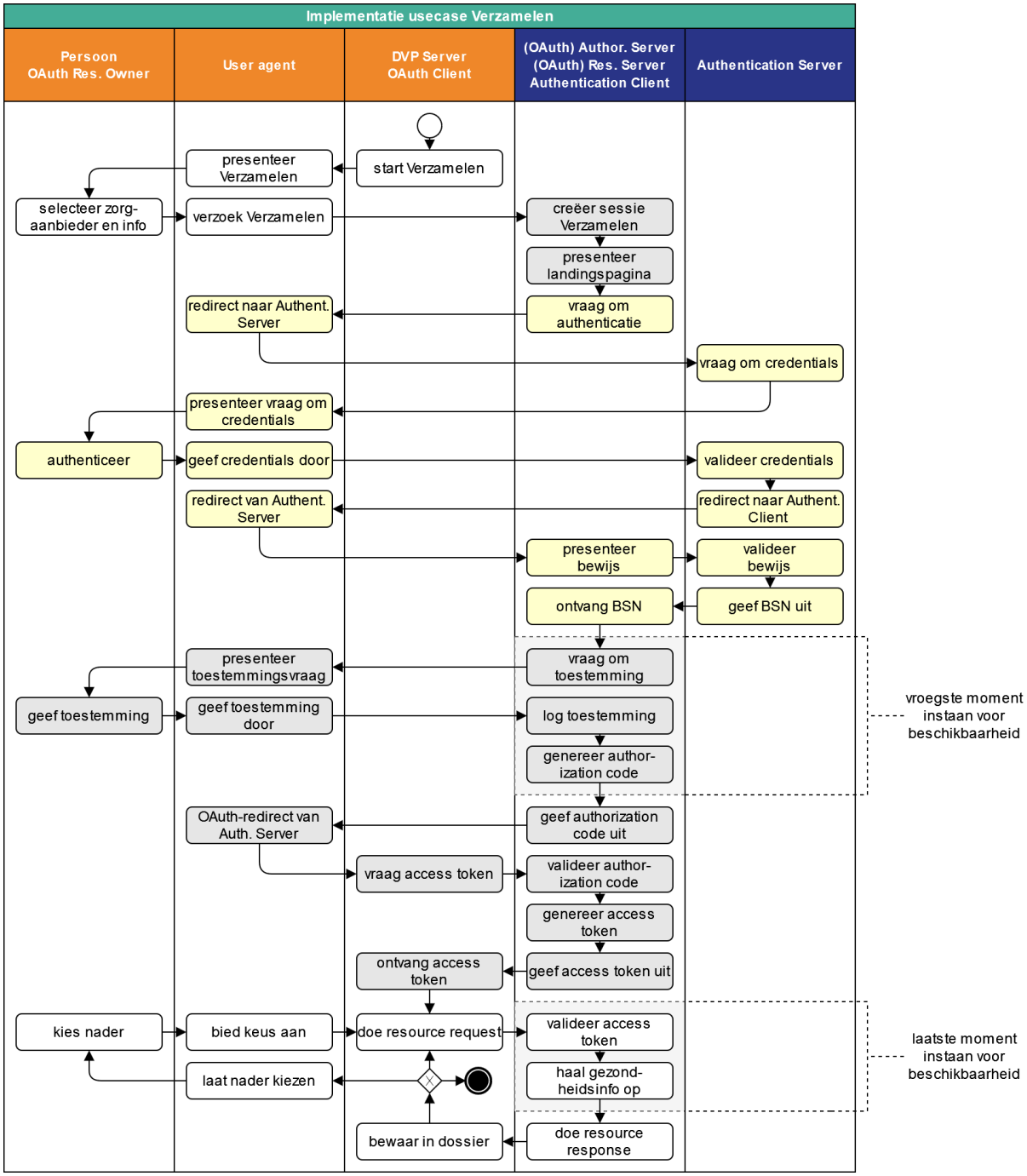
		informeert daarop *Persoon* hierover, met opgave van oorzaak.	
Verzamelen 7	*Persoon* annuleert het inloggen.	*Dienstverlener aanbieder* presenteert een annuleringspagina en biedt *Persoon* de optie om toch in te loggen.	Indien *Persoon* kiest niet in te willen loggen, kan het scherm gesloten worden. *Persoon* kan er ook voor kiezen toch in te loggen. In dat geval vraagt *Dienstverlener aanbieder* weer om credentials.

3. Applicatielaag

Menige actie in het stroomdiagram is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow volgens OAuth 2; de zachtgeel gekleurde acties vormen samen de authenticatieflow. Deze kleuren verwijzen dus alleen maar naar de gebruikte standaarden en zeggen niets over welke component de stap zou moeten uitvoeren. Authenticatie is dus ingebed in autorisatie.

Verantwoordelijkheden inzake uitzonderingen op de happy flow zijn opgenomen bij de respectievelijke interface, waar de uitzonderingen bij de usecases zijn genoemd.

3.1. Stroomdiagram



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De flow kent de volgende stappen:

1. De *DVP Server* start de flow door in de *User Agent* van de *Persoon* de mogelijkheid te presenteren om één of meerdere *Gegevensdiensten* bij een zekere *Aanbieder* te verzamelen. Uit de *Aanbiederslijst* weet de *DVP Server* welke *Gegevensdiensten* door een *Aanbieder* aangeboden worden. Desgewenst worden de *Gegevensdienstnamen* uit de *Gegevensdienstnamenlijst* gebruikt.

2. De *Persoon* maakt expliciet zijn selectie en laat de *User Agent* een authorization request sturen naar de *Authorization Server*. Het adres van het authorization endpoint komt uit de *Aanbiederslijst*. De `redirect_uri` geeft aan waarnaartoe de *Authorization Server* de *User Agent* verderop moet redirecten (met de authorization code). Het authorization request mag desgewenst, onder voorwaarden, meerdere *Gegevensdiensten* van de *Aanbieder* bevatten.

   Toestemming voor meerdere Gegevensdiensten van een Aanbieder

   In een authorization request mogen meerdere *Gegevensdiensten* van eenzelfde *Aanbieder* worden gecombineerd wanneer:

   a. de gegevensdiensten worden aangeboden binnen één zelfde interfaceversie, EN
   b. de FQDN van de in de ZAL, voor deze gegevensdiensten, opgenomen AuthorizationEndpoints met elkaar overeenkomen, EN
   c. de FQDN van de in de ZAL, voor deze gegevensdiensten, opgenomen TokenEndpoints met elkaar overeenkomen.

3. Daarop begint de *Authorization Server* de OAuth-flow (in zijn rol als *OAuth Authorization Server*) door een sessie te creëren.
4. De *Authorization Server* vraagt de *Persoon* via zijn *User Agent* in te loggen.
5. Dan start de *Authorization Server* (nu in de rol van *Authentication Client*) de authenticatieflow door de *User Agent* naar de *Authentication Server* te redirecten, onder meegeven van een `redirect_uri`, die aangeeft waarnaartoe de *Authentication Server* straks de *User Agent* moet terugsturen, na het inloggen van de *Persoon*.
6. De *Authentication Server* vraagt de *Persoon* via zijn *User Agent* om inloggegevens.
7. Wanneer deze juist zijn, redirect de *Authentication Server* de *User Agent* terug naar de *Authorization Server*, onder meegeven van een ophaalbewijs. Wanneer het inloggen is afgebroken geeft de *Authorization Server* de *Persoon* alsnog de mogelijkheid via zijn *User Agent* in te loggen.
8. Met dit ophaalbewijs haalt de *Authorization Server* rechtstreeks bij de *Authentication Server* het BSN op.
9. Dan breekt het vroegste moment aan waarop de *Authorization Server* ervoor instaat dat de *Aanbieder* voor de betreffende *Gegevensdienst(en)* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft, of anders de happy flow afbreekt. Daarvan maakt deel uit dat de *Persoon* daarvoor minstens 16 jaar oud moet zijn.
10. Indien de *Aanbieder* kan instaan voor de beschikbaarheid van tenminste één *Gegevensdienst*, of wanneer géén gebruik wordt gemaakt van dit vroegste moment, dan presenteert de *Authorization Server* via de *User Agent* aan *Persoon* in een *Toestemmingsverklaring*, de vraag of *Persoon* de *Aanbieder* toestaat de gevraagde persoonlijke gezondheidsinformatie aan de *DVP Server* (als *OAuth Client*) te sturen. Indien op dit moment al bekend is dat een bepaalde *Gegevensdienst* niet beschikbaar is voor de *Persoon*, dan mag deze niet worden opgenomen in de *Toestemmingsverklaring* .
11. Bij akkoord logt de *Authorization Server* dit als toestemming, genereert een authorization code en stuurt dit als ophaalbewijs, door middel van een *User Agent* redirect met de in het authorization request ontvangen `redirect_uri`, naar de *DVP Server*. De *Authorization Server* stuurt daarbij de local state-informatie mee die hij in het authorization request van de *DVP Server* heeft gekregen. Laatstgenoemde herkent daaraan het verzoek waarmee hij de authorization code moet associëren.
12. De *DVP Server* vat niet alleen deze authorization code op als ophaalbewijs, maar leidt er ook uit af dat de toestemming is gegeven en logt het verkrijgen van het ophaalbewijs.
13. Met dit ophaalbewijs wendt de *DVP Server* zich weer tot de *Authorization Server*, maar nu zonder tussenkomst van de *User Agent*, voor een access token.
14. Daarop genereert de *Authorization Server* een access token en stuurt deze naar de *DVP Server*.
15. Nu is de *DVP Server* gereed om één of meerdere verzoeken om de gezondheidsinformatie naar de *Resource Server* te sturen, nadat hij de *Persoon* eventueel nog nadere keuzes heeft laten maken. Het adres van de juiste resource endpoints haalt hij uit de *Aanbiederslijst*. Hij plaatst telkens het access token in het bericht en zorgt ervoor dat in het bericht geen BSN is opgenomen.

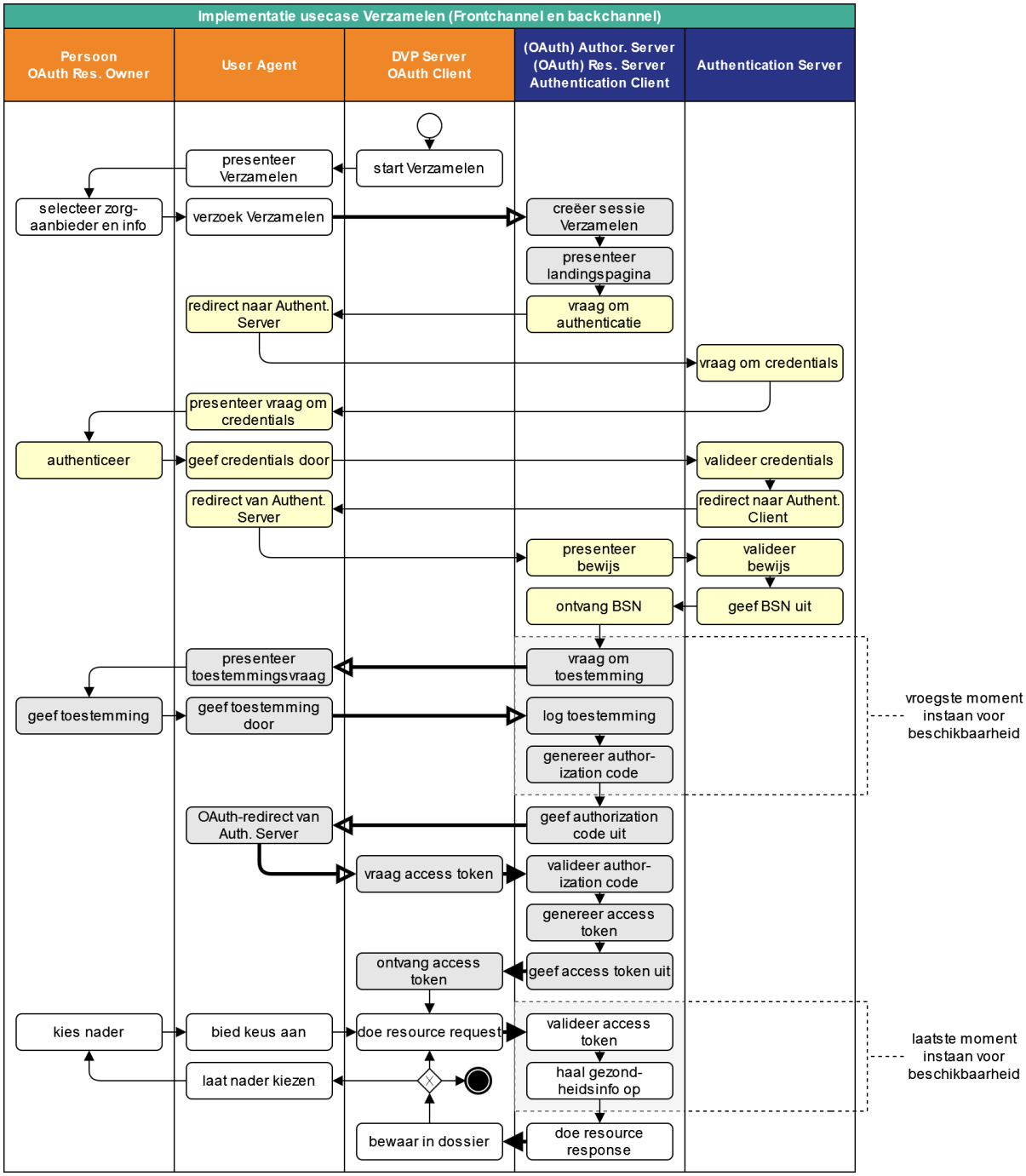
16. De *Resource Server* controleert bij ieder verzoek of het ontvangen token recht geeft op de gevraagde resources en haalt deze (al dan niet) bij achterliggende bronnen op. Dan breekt het uiterste moment aan waarop de *Resource Server* ervoor moet instaan dat voor de *Gegevensdienst* waartoe een verzoek behoort de *Aanbieder* de gezondheidsgegevens beschikbaar heeft. Is dat zo, dan verstuurt de *Resource Server* deze ze in een resource response naar de *DVP Server*.
17. De *DVP Server* bewaart de ontvangen gezondheidsinformatie in het persoonlijke dossier. De *DVP Server* bevraagt de *Resource Server* daarna mogelijk opnieuw, eventueel na nieuwe interactie met de *Persoon*. Zolang het access token geldig is, kan dat.

In de regel worden bij een eenmalig gebruik van *Verzamelen* het authorization interface, het token interface en het resource interface allemaal aangesproken, in die volgorde. Mocht de *DVP Server* echter nog beschikken over een nog niet verlopen access token voor de betreffende *Aanbieder-Gegevensdienst*-combinatie, dan kan het onmiddellijk het resource interface aanspreken.

Het MedMij Afsprakenstelsel adviseert de beschikbaarheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. Vooralsnog staat het MedMij Afsprakenstelsel toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment.

Bij de implementatie van de voorwaarde op beschikbaarheid bij de *Aanbieder* voor de te verzamelen gezondheidsgegevens is het zaak rekening te houden met privacy-vereisten. Wanneer de *Dienstverlener aanbieder* ten behoeve van de beschikbaarheidsvoorwaarde nieuwe gegevensverzamelingen zou aanleggen, vindt een verwerking altijd onder de verantwoordelijkheid van één *Aanbieder* plaats. Het combineren van verwerkingen of het onvoldoende segregeren moet worden vermeden. Afwijking hiervan is alleen mogelijk onder expliciete instructie van de *Aanbieder(s)* en vereist een zorgvuldige voorafgaande afweging, vanwege de daaraan verbonden privacyrisico's.

3.2. Technologielaag



In het bovenstaande stroomschema geven de dikke pijlen het *MedMij-verkeer* weer en zijn daarbinnen de vijf gevallen van frontchannel-verkeer (open pijlpunt) en vier gevallen van backchannel-verkeer (gesloten pijlpunt) aangegeven.

Delen

1. Inleiding

Op deze pagina staan de stroomdiagrammen behorende bij de functie *Delen*. De functie is een spiegelbeeld van de functie *Verzamelen*. Daarom is er een aantal wezenlijke verschillen. Op het niveau van de usecase zijn dat de volgende:

- Voor de start van de usecase zou de *Persoon* moeten kunnen volstaan met het aanwijzen van die informatie in zijn *Dossier* die hij zou willen delen met een nader te benoemen *Persoon*, en er daarbij vanuit mogen gaan dat de *Dienstverlener persoon* daarbij weet welke *Gegevensdienst* daarbij aan de orde is.
- In tegenstelling tot in de functie *Verzamelen* moet *Persoon* in de gelegenheid worden gesteld om zich al dan niet open te stellen voor ontvangst van de betreffende informatie. De *Dienstverlener aanbieder* moet na authenticatie van de *Persoon* kunnen bepalen of de betreffende informatie welkom is bij de betreffende *Aanbieder*. Deze controle op de ontvankelijkheid zal geautomatiseerd plaatsvinden, met het oog op de synchrone gebruikservaring, maar de wijze van implementatie wordt vrijgelaten.
- Juridisch gezien is er geen expliciete toestemming van de *Persoon* vereist aan de *Aanbieder* voor het mogen ontvangen van de gezondheidsinformatie; die volgt uit de verstrekking door de *Persoon*. Er zijn wel toestemmingsvereisten in de relatie *Persoon*-*Dienstverlener persoon* (inzake het mogen verstrekken van de gezondheidsinformatie), maar daarop ziet reguliere wet- en regelgeving toe. Niettemin wordt er, net als in de functie *Verzamelen*, om een bevestiging gevraagd van de *Persoon*.
- Aan het eind van de usecase wordt, indien de *Aanbieder* ervoor ontvankelijk bleek, de betreffende informatie door de *Dienstverlener persoon* geplaatst bij de *Aanbieder,* via de *Dienstverlener aanbieder* . Net zoals in de functie *Verzamelen* geen nadere eisen worden gesteld aan hoe het ophalen van de informatie door de *Dienstverlener aanbieder* bij de *Aanbieder* geschiedt, geldt dat in de functie *Delen* ook voor de plaatsing. Van belang is slechts dat de *Persoon* ervan kan uitgaan dat de *Aanbieder* kennis kan hebben genomen van de betreffende informatie. Hoe dat wordt geborgd is niet triviaal, maar wordt gelaten aan de voorzieningen die de *Dienstverlener aanbieder* treft en de *Dienstverleningsovereenkomst* die hij dienaangaande aangaat met de *Aanbieder*.

In de platen hieronder staat het stroomdiagram van de functie *Delen*:

- De happy flow van de usecase Delen;
- De implementatie van de usecase Delen;
- De implementatie van het front- en backchannelverkeer.

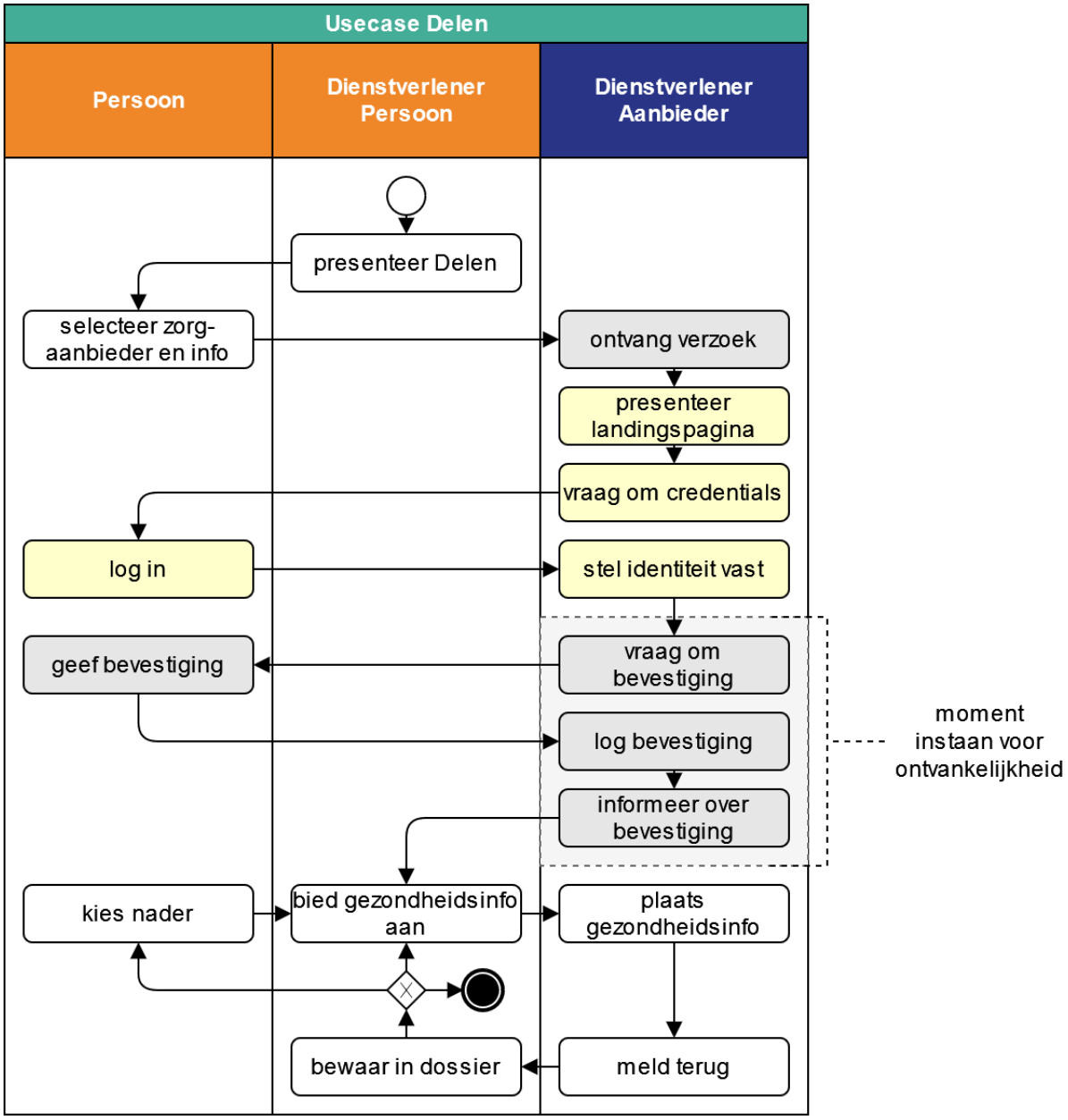
De stroomdiagrammen tonen alleen de situatie waarin alle acties slagen tot en met het uiteindelijke verzamelen van de gezondheidsinformatie (de zogenaamde happy flow). De oranje banen horen, conform de MedMij-huisstijl tot het Persoonsdomein, de blauwe tot het Aanbiedersdomein.

2. Businesslaag

Menige actie in het stroomdiagram is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow; de zachtgeel gekleurde acties vormen samen de authenticatieflow.

Omdat het stroomdiagram alleen de happy flow bevat, worden zijn daarna de uitzonderingen beschreven.

2.1. Stroomdiagram



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De totale procesgang van de UC Delen kent de volgende stappen:

- De *Dienstverlener persoon* presenteert aan de *Persoon* de mogelijkheid om te delen.
- De *Persoon* kiest de *Aanbieder* waarmee hij de informatie wenst te delen en de *Gegevensdienst*. Daarvoor kunnen desgewenst de *Gegevensdienstnamen* worden gebruikt uit de *Gegevensdienstnamenlijst*. Het verzoek gaat naar de passende *Dienstverlener aanbieder*.
- De *Dienstverlener aanbieder* ontvangt de *Persoon*.
- De *Dienstverlener aanbieder* laat de *Persoon* zich authenticeren.
- Wanneer de *Persoon* de authenticatie heeft afgebroken geeft de *Dienstverlener aanbieder* de mogelijkheid alsnog te authenticeren of de flow af te breken.

- Dan breekt het moment aan waarop de *Dienstverlener aanbieder* op zijn vroegst ervoor instaat dat de *Aanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* wenst te ontvangen, of anders de happy flow afbreekt. Het MedMij Afsprakenstelsel adviseert de ontvankelijkheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. Vooralsnog staat het MedMij Afsprakenstelsel het toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment.
- De *Dienstverlener aanbieder* vraagt aan de *Persoon* of hij de wens bevestigt de informatie te laten verstrekken aan de *Aanbieder*. De vraag die hiervoor aan de *Persoon* gesteld moet worden staat op de pagina Bevestigingsverklaring.
- De *Dienstverlener aanbieder* logt die bevestiging en laat de *Dienstverlener persoon* weten of die geslaagd is.
- Voordat de flow dan wordt overgegeven aan de *Dienstverlener persoon* zal de *Dienstverlener aanbieder* ervoor instaan dat de *Aanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* wenst te ontvangen, of anders de happy flow afbreken.
- Nu kan de *Dienstverlener persoon* de gezondheidsinformatie plaatsen bij de *Dienstverlener aanbieder*.
- Mocht de *Gegevensdienst* waartoe de *Persoon* heeft geautoriseerd uit meerdere *Transacties* bestaan (zie hiervoor de Catalogus), plaatst de *Dienstverlener persoon* daarna mogelijk opnieuw bij de *Dienstverlener aanbieder* voor de nog resterende *Transacties*, eventueel na nieuwe interactie met de *Persoon*.
- De *Dienstverlener persoon* tekent bij de informatie ook de meta-informatie aan die wordt bedoeld in verantwoordelijkheid 19 van de Processen- en Informatielaag.

De ontvankelijkheidsvoorwaarde is een aspect van de regie, niet van de uitwisseling. De voorwaarde geeft de *Aanbieder* ruimte om deel te nemen in aan de *Persoon* gegeven regie. Omdat echter bestaande implementatie-architecturen veelal uitwisseling centraal zetten, en niet regie, hebben zij moeite de beschikbaarheidsvoorwaarde in de regiefase te implementeren. Daarom biedt het MedMij Afsprakenstelsel vooralsnog de gelegenheid om deze in de uitwisselingsfase te implementeren. *Deelnemers* wordt echter aangeraden om, met het oog op de toekomst, in hun implementatie-architecturen een passend onderscheid tussen regie en uitwisseling te maken en de eerste geleding de tweede te laten sturen.

2.2. Uitzonderingen op de Happy flow van de usecase

In onderstaande tabel staan de uitzonderingssituaties beschreven. Alle worden door de *Dienstverlener aanbieder* ontdekt. Om te voorkomen dat de *Dienstverlener persoon* informatie over het bestaan van behandelrelaties verkrijgt zonder dat (al) bevestiging is gegeven, moet het onderscheid tussen de uitzonderingen 2, 3 en 4 niet te maken zijn door de *Dienstverlener persoon*.

nr.	uitzondering	actie	vervolg
nr.	uitzondering	actie	vervolg
UC Delen 1	*Dienstverlener aanbieder* vindt het ontvangen verzoek ongeldig.	*Dienstverlener aanbieder* informeert *Dienstverlener persoon* over deze uitzondering. *Dienstverlener persoon* informeert daarop *Persoon* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Delen 2	*Dienstverlener aanbieder* kan de identiteit van de *Persoon* niet vaststellen.	*Dienstverlener aanbieder* informeert *Dienstverlener persoon* dat delen niet toegelaten wordt.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Delen 3	*Dienstverlener aanbieder* stelt op enig moment vast dat betreffende informatie van		

	Persoon bij *Aanbieder* niet welkom is. Hiervan is in elk geval sprake indien hetzij: • er geen behandelrelatie is aan te wijzen als grondslag voor het delen; • *Persoon* nog geen zestien jaar oud is. Zie de toelichting op Beschikbaarheids- en ontvankelijkheidsvoorwaarde.		
UC Delen 4	De bevestiging wordt niet gegeven.		
UC Delen 5	*Dienstverlener aanbieder* kan het antwoord op de bevestigingsvraag niet vaststellen.	*Dienstverlener aanbieder* informeert *Dienstverlener persoon* over deze uitzondering. *Dienstverlener persoon* informeert daarop *Persoon* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Delen 6	*Dienstverlener persoon* kan, zelfs na bevestiging, de gezondheidsinformatie alsnog niet plaatsen bij *Dienstverlener aanbieder*.	*Dienstverlener persoon* informeert daarop *Persoon* hierover, met opgave van oorzaak.	Mocht gezondheidsinformatie deels wel (geautoriseerd) geplaatst kunnen worden, dan kan de flow dat nog verzorgen.
UC Delen 7	*Persoon* annuleert het inloggen.	*Dienstverlener aanbieder* presenteert een annuleringspagina en biedt *Persoon* de optie om toch in te loggen.	Indien *Persoon* kiest niet in te willen loggen, kan het scherm gesloten worden. *Persoon* kan er ook voor kiezen toch in te loggen. In dat geval vraagt *Dienstverlener aanbieder* weer om credentials.

Of de *Aanbieder*, in de controle op ontvankelijkheid, zich ontvankelijk verklaart voor de door de *Persoon* aangeboden gezondheidsinformatie, is om te beginnen een zaak tussen de *Aanbieder* en *Persoon*, die daarvoor een behandelrelatie moeten hebben. Gegeven zo'n behandelrelatie is er wetgeving van toepassing op deze ontvankelijkheid. Daarbinnen is eigen beslisruimte voor de *Aanbieder*. Omdat *Aanbieder* en *Persoon* evenwel geen *Deelnemers* in het MedMij Afsprakenstelsel zijn, specificeert het MedMij Afsprakenstelsel niet de exacte logica van de beslissing om al dan niet ontvankelijk te zijn voor de gezondheidsinformatie. Om privacy-redenen vereist het MedMij Afsprakenstelsel echter wel dat er een behandelrelatie moet (hebben) bestaan waarbij de betreffende gezondheidsinformatie hoort én dat de *Persoon* minstens zestien jaar oud is (zie uitzondering UC Delen 3).

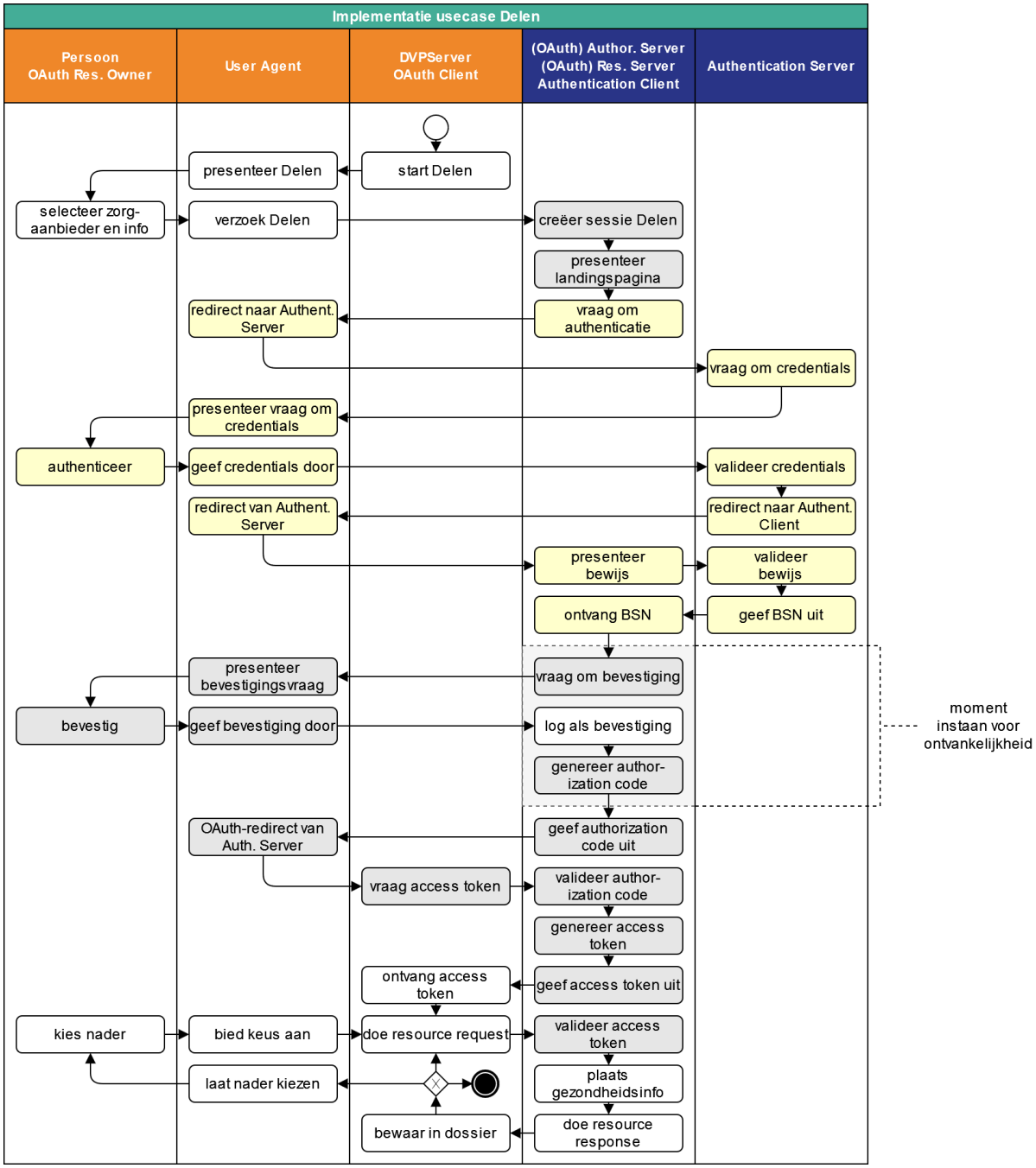
Voor het laten delen van gegevens door een minder dan zestienjarige moet toestemming of een machtiging tot toestemming worden verleend door degene die de ouderlijke verantwoordelijkheid of de wettelijke verantwoordelijkheid voor de minder dan zestienjarige draagt. Omdat in dergelijke toestemmingen of machtigingen nog niet is voorzien in deze versie van het MedMij Afsprakenstelsel, kan deze controle vooralsnog als onderdeel van de ontvankelijkheidsvoorwaarde worden opgevat. Wanneer een toekomstige release van het MedMij Afsprakenstelsel wel zulke toestemmingen of machtigingen omvat, zal de leeftijdsvoorwaarde gescheiden moeten worden van de ontvankelijkheidsvoorwaarde.

3. Applicatielaag

Menige actie in het stroomdiagram is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow volgens OAuth 2; de zachtgeel gekleurde acties vormen samen de authenticatieflow. Deze kleuren verwijzen dus alleen maar naar de gebruikte standaarden en zeggen niets over welke component de stap zou moeten uitvoeren. Authenticatie is dus ingebed in autorisatie.

Verantwoordelijkheden inzake uitzonderingen op de happy flow zijn opgenomen bij de respectievelijke interface, waar de uitzonderingen bij de usecases zijn genoemd.

3.1. Stroomdiagram



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De flow kent de volgende stappen:

1. De *DVP Server* start de flow door in de *User Agent* van de *Persoon* de mogelijkheid te presenteren om een bepaalde *Gegevensdienst* met een zekere *Aanbieder* te delen. Het gaat altijd om precies één *Gegevensdienst* (één scope, in OAuth-termen). Uit de *Aanbiederslijst* weet de *DVP Server* welke *Gegevensdiensten* door een *Aanbieder.*
2. aangeboden worden. Desgewenst worden de *Gegevensdienstnamen* uit de *Gegevensdienstnamenlijst* gebruikt.

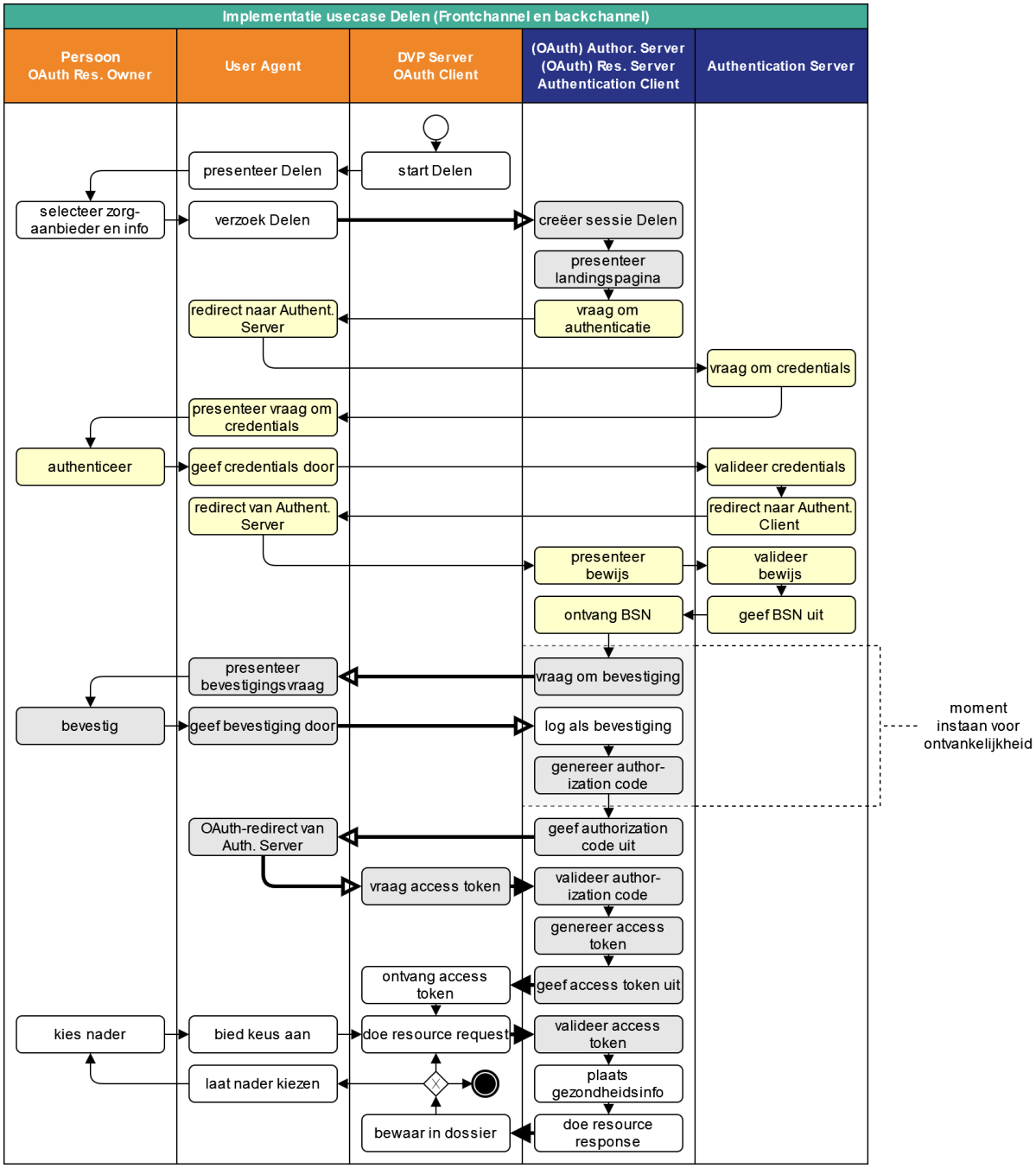
3. De *Persoon* maakt expliciet zijn selectie en laat de *User Agent* een deel-verzoek sturen naar de *Authorization Server*. Het adres van het authorization endpoint komt uit de *Aanbiederslijst*. De redirect URI geeft aan waarnaartoe de *Authorization Server* de *User Agent* verderop moet redirecten (met de authorization code).
4. Daarop begint de *Authorization Server* de OAuth-flow (in zijn rol als *OAuth Authorization Server*) door een sessie te creëren.
5. De *Authorization Server vraagt de Persoon via zijn User Agent in te loggen.*
6. Dan start de *Authorization Server* (nu in de rol van *Authentication Client*) de authenticatieflow door de *User Agent* naar de *Authentication Server* te redirecten, onder meegeven van een redirect URI, die aangeeft waarnaartoe de *Authentication Server* straks de *User Agent* moet terugsturen, na het inloggen van de *Persoon*.
7. De *Authentication Server* vraagt van de *Persoon* via zijn *User Agent* om inloggegevens.
8. Wanneer deze juist zijn, redirect de *Authentication Server* de *User Agent* terug naar de *Authorization Server*, onder meegeven van een ophaalbewijs. Wanneer het inloggen is afgebroken geeft de *Authorization Server* de *Persoon* alsnog de mogelijkheid via zijn *User Agent* in te loggen.
9. Met dit ophaalbewijs haalt de *Authorization Server* rechtstreeks bij de *Authentication Server* het BSN op.
10. Dan breekt het vroegste moment aan waarop de *Authorization Server* ervoor instaat dat de *Aanbieder* voor de betreffende *Gegevensdienst* überhaupt ontvankelijk is voor de gezondheidsinformatie van die *Persoon*, of anders de happy flow afbreekt. Daarvan maakt deel uit dat de *Persoon* daarvoor minstens 16 jaar oud moet zijn.
11. Zo ja, dan presenteert de *Authorization Server* via de *User Agent* aan *Persoon* de vraag of laatstgenoemde bevestigt de gevraagde persoonlijke gezondheidsinformatie door de *DVP Server* (als *OAuth Client*) te laten aanbieden. Onder het stroomdiagram staat gespecificeerd welke informatie, waarvandaan, de *OAuth Authorization Server* verwerkt in de aan *Persoon* voor te leggen bevestigingsvraag.
12. Bij akkoord logt de *Authorization Server* dit als bevestiging, genereert een authorization code en stuurt dit als ophaalbewijs, door middel van een browser redirect met de in stap 1 ontvangen redirect URI, naar de *DVP Server*. De *Authorization Server* stuurt daarbij de local state-informatie mee die hij in de eerste stap van de *DVP Server* heeft gekregen. Laatstgenoemde herkent daaraan het verzoek waarmee hij de authorization code moet associëren.
13. De *DVP Server* vat niet alleen deze authorization code op als ophaalbewijs, maar leidt er ook uit af dat de bevestiging is gegeven en logt het verkrijgen van het ophaalbewijs.
14. Met dit ophaalbewijs wendt de *DVP Server* zich weer tot de *Authorization Server*, maar nu zonder tussenkomst van de *User Agent*, voor een access token.
15. Daarop genereert de *Authorization Server* een access token. Dan breekt het uiterste moment aan waarop de *Authorization Server* ervoor moet instaan dat voor de betreffende *Gegevensdienst* de *Aanbieder* ontvankelijk is voor de gezondheidsgegevens van de betreffende *Persoon*. Is dat zo, dan verstuurt de *Authorization Server* het access token naar de *DVP Server*. Is dat niet zo, dan breekt de *Authorization Server* de happy flow af en stuurt zij geen access token naar de *DVP Server*.
16. Nu is de *DVP Server* gereed om de gezondheidsinformatie aan de *Resource Server* aan te bieden, nadat hij de gebruiker eventueel nog nadere keuzes heeft laten maken. Het adres van het resource endpoint haalt hij uit de *ZAL*. Hij plaatst het access token in het bericht en zorgt ervoor dat in het bericht geen BSN is opgenomen.
17. De *Resource Server* controleert of het ontvangen token recht geeft op het aanbieden van de informatie, plaatst deze (al dan niet) bij achterliggende bestemmingen en verstuurt een antwoord in een FHIR-response naar de *DVP Server*.
18. Deze maakt hierover een aantekeningen bij de aangeboden gezondheidsinformatie in het persoonlijke dossier. Mocht de *Gegevensdienst* waartoe de *Persoon* heeft geautoriseerd uit meerdere *Transacties* bestaan (zie hiervoor de Catalogus), plaatst de *DVP Server* daarna mogelijk opnieuw bij de *Resource Server* voor de nog resterende *Transacties*, eventueel na nieuwe interactie met de *Persoon*. Dat geldt ook voor de situatie waarin één *Transactie*, blijkens de betreffende *Informatiestandaard*, uit meerdere FHIR creates bestaat. Zolang het access token geldig is, kan dat.

In de regel worden bij een eenmalig gebruik van de functie *Delen* het authorization interface, het token interface en het resource interface allemaal aangesproken, in die volgorde. Mocht de *DVP Server* echter nog beschikken over een nog niet verlopen access token voor de betreffende *Aanbieder-Gegevensdienst*-combinatie, dan kan het onmiddellijk het resource interface aanspreken.

Het MedMij Afsprakenstelsel adviseert de ontvankelijkheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. In release 1.1.1 staat het MedMij Afsprakenstelsel toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment.

Bij de implementatie van de toets op ontvankelijkheid van de *Aanbieder* voor de te delen gezondheidsgegevens is het zaak rekening te houden met privacy-vereisten. Wanneer de *Dienstverlener aanbieder* ten behoeve van de ontvankelijkheidstoets nieuwe gegevensverzamelingen zou aanleggen, vindt een verwerking altijd onder de verantwoordelijkheid van één *Aanbieder* plaats. Het combineren van verwerkingen of het onvoldoende segregeren moet worden vermeden. Afwijking hiervan is alleen mogelijk onder expliciete instructie van de *Aanbieder(s)* en vereist een zorgvuldige voorafgaande afweging, vanwege de daaraan verbonden privacyrisico's.

3.2. Technologielaag



In bovenstaand stroomschema geven de dikke pijlen het *MedMij-verkeer* weer en zijn daarbinnen de vijf gevallen van frontchannel-verkeer (open pijlpunt) en vier gevallen van backchannel-verkeer (gesloten pijlpunt) aangegeven.

Verantwoordelijkheden, Core

1. Inleiding

In de MedMij Core zijn verschillende rollen beschreven, die met elkaar de verschillende functies uitvoeren en gegevens uitwisselen. Hierbij gelden de verantwoordelijkheden, zoals in dit hoofdstuk benoemd.

De verantwoordelijkheden worden beschreven op de drie lagen van de architectuur, waarbij verantwoordelijkheden op de:

- businesslaag getoond worden als gele regels;
- applicatielaag getoond worden als blauwe regels;
- technologielaag getoond worden als groene regels.

Iedere verantwoordelijkheid heeft een unieke code, welke achter de regel wordt getoond. Verwijzingen naar de verantwoordelijkheid worden uitgevoerd vanuit deze unieke codes. De code is opgebouwd uit verschillende onderdelen.

- Het eerste deel bestaat altijd uit 'core', om aan te geven dat het om verantwoordelijkheden gaat die in de MedMij Core beschreven staan.
- Het tweede deel verwijst naar het onderwerp waarop de verantwoordelijkheid van toepassing is.
- Het derde deel is een volgnummer, waarbij verantwoordenheden uit de:
  - businesslaag beginnen met 100;
  - applicatielaag beginnen met 200;
  - technologielaag beginnen met 300.

2. Rollen

1.	*Eigenaar MedMij* neemt de functionele rol van *MedMij Beheer* op zich. Er is één *Eigenaar MedMij* die één *MedMij Beheer* speelt.	core. rollen. 100
2.	Een *Deelnemer* neemt de functionele rol van *Dienstverlener persoon* en/of *Dienstverlener aanbieder* op zich. Hierbij speelt één *Deelnemer* één of meerdere dienstverleners en wordt elke dienstverlener gespeeld door één *Deelnemer.*	core. rollen. 101
3.	*Dienstverlener persoon* biedt aan *Persoon,* in het kader van de toepasselijke *Dienstverleningsovereenkomst*, een geautomatiseerde rol ter gebruik, hier genoemd: *DVP Server*. Eén *Dienstverlener persoon* biedt één of meerdere *DVP Servers* en elke *DVP Server* wordt door één *Dienstverlener persoon* geboden.	core. rollen. 200
4.	*Dienstverlener aanbieder* biedt een geautomatiseerde rol *Authorization Server*, voor het namens *Aanbieders* uitwisselen van gezondheidsinformatie met *DVP Server*. Deze rol wordt altijd in combinatie met een *Resource Server*.	core. rollen. 201
5.	*Dienstverlener aanbieder* biedt een geautomatiseerde rol *Resource Server*, voor het namens *Aanbieders* uitwisselen van gezondheidsinformatie met *DVP Server*. Eén *Dienstverlener aanbieder* biedt één of meer combinaties van één *Authorization Server* en één *Resource Server* en elke combinatie van één *Authorization Server* en één *Resource Server* wordt door één *Dienstverlener aanbieder* geboden.	core. rollen. 202
6.	*Persoon* gebruikt één geautomatiseerde rol *User Agent* voor toegang tot de functionaliteit van *DVP Server* en *Authorization Server. User Agent* presenteert de functionaliteit aan *Persoon*, spreekt *DVP Server* aan en verwijst de *Persoon* naar de *Authorization Server*.	core. rollen. 203

7.	*MedMij Beheer* ontsluit ten behoeve van alle betrokkenen een geautomatiseerde rol, hier genoemd: *MedMij Registratie*.	core. rollen. 204
8.	Ten behoeve van het authenticeren van *Persoon*, zal de betrokken *Authorization Server*, in de rol van *Authentication Client*, gebruikmaken van de Authentication Server van een *Dienstverlener authenticatie.*	core. rollen. 205
9.	Ten behoeve van het autoriseren van *DVP Server* voor toegang tot *Resource Server*, in het kader van de functies *Verzamelen* en *Delen*, zullen de betrokken *User Agent*, *DVP Server, Authorization Server* en *Resource Server* gebruik maken van OAuth 2.0, waarbij als grant type gebruik wordt gemaakt van Authorization Code en waarbij: a. de rol van *OAuth Resource Owner* wordt verzorgd door de *Persoon*; b. de rol van *OAuth Client* wordt verzorgd door de *DVP Server*; c. de rol van *OAuth Resource Server* wordt verzorgd door de *Resource Server*; d. de rol van *OAuth Authorization Server* wordt verzorgd door de *Authorization Server.* De keuze, in OAuth, voor de grant type Authorization Code past bij de typische software-architectuur die in MedMij in het Persoonsdomein wordt aangetroffen: toegang tot een PGO-dienst via componenten die niet onder controle van de *OAuth Client* vallen en als betrekkelijk onveilig moeten worden gezien.	core. rollen. 206
10.	Als *MedMij-verkeer* is gedefinieerd: al het gegevensverkeer in het kader van enige usecase-implementatie, onmiddellijk tussen twee verschillende van de vier volgende soorten rollen, namelijk: • ten eerste *DVP Server*, • ten tweede *User Agent*, • ten derde *Authorization Server* of *Resource Server* en • ten vierde *MedMij Registratie*, met dien verstande dat: • in deze rollen telkens begrepen zijn de door hen eventueel verzorgde respectievelijke Autorisatie-rollen, • van deze rollen telkens uitgesloten zijn de door hen eventueel verzorgde Authenticatie-rollen, en • in deze rollen, met betrekking tot de usecase-implementaties, telkens inbegrepen zijn de Nodes waarop zij functioneren.	core. rollen. 207

11.	In het *MedMij-netwerk* functioneert:
	
	• iedere rol uit de applicatie-laag op één of meer *Frontchannel* en/of *Backchannel Nodes*, met uitzondering van:
	  • Voor al diens frontchannel-verkeer gebruikt elke *DVP Server* één *Frontchannel Node* , en wel met een hostname die voor die *DVP Server* voorkomt op de *OAuth Client List*.
	  • *MedMij Registratie* functioneert op precies één node, welke bekend staat onder de naam 'Stelselnode'. Zonder de MedMij Stelselnode is er geen MedMij-netwerk.
	
	Het is toegestaan om een *Authorization Server* en een *Resource Server* te verdelen over verschillende *Nodes*, maar ook te combineren op dezelfde. De afsprakenset staat het zelfs toe dat *Authorization Server* en *Resource Server* elk apart op meerdere *Nodes*
		core.
		rollen.
		300

	worden geprojecteerd. Het kan dan voorkomen dat, bij de betreffende *AanbiederGegevensdiensten* in de *Aanbiederslijst*, hostnames in de endpointadressen staan die verschillen tussen het authorization endpoint, het token endpoint en het resource endpoint, zelfs bij eenzelfde *Interfaceversie*. Een belangrijke eis blijft evenwel dat al deze hostnames bij *Nodes* van eenzelfde *Dienstverlener aanbieder* horen. De hele flow behorend bij een zekere *AanbiederGegevensdienst* moet namelijk onder de eindverantwoordelijkheid van één zo'n *Dienstverlener* vallen, namelijk van de *Dienstverlener* die die *AanbiederGegevensdienst* ontsluit. Zo blijft die integrale eindverantwoordelijk-heid ook op net-werk-niveau toetsbaar. Zie de drie (ingewikkelde) invarianten bij *Aanbie-derGegevensdienst*van het soort “niet-lokale afhankelijkheid”. De uitzondering daarop inzake het frontchannel-verkeer is noodzakelijk om de *OAuth Client List* te laten functioneren. Het is dus mogelijk voor een *DVP Server* om verschillende certificaten te hanteren voor frontchannel- en backchannel-verkeer, zolang op de *OAuth Client List* maar de hostname in het certificaat voor frontchannelverkeer voorkomt die tevens voorkomt in de redirect URI inzake OAuth. --- In het Aanbiedersdomein treden alleen de *Nodes* op in het *MedMij-netwerk*. Dat wil zeggen dat bijvoorbeeld achterliggende xIS'en niet over het *MedMij-netwerk* communiceren met de *Node*. Dat verkeer is verborgen achter de *Node*. Alle daarvoor benodigde routering wordt afgehandeld door de server-implementaties en speelt zich buiten het zicht van het MedMij Afsprakenstelsel af.	
12.	Op één *Node* functioneert hetzij één *Authorization Server*, hetzij één *Resource Server*, hetzij een combinatie van voorgaande rollen.	core.rollen.301

3. Functies & gegevens

De interpretatie door een *Persoon* van zorg- en gezondheidsinformatie die hij heeft verzameld bij een *Aanbieder*, en de interpretatie door een *Aanbieder* van zulke informatie die met hem/haar gedeeld is door een *Persoon,* hangt niet alleen af van de inhoud van die informatie, maar ook van de partij die de betreffende informatie oorspronkelijk heeft geregistreerd. De oorspronkelijke herkomst van de gegevens (de auteur) kent geen rol in het MedMij afsprakenstelsel. Dat betekent niet alleen dat er binnen de grenzen van het MedMij Afsprakenstelsel momenteel geen basis is om auteursauthenticiteit (met bijvoorbeeld certificaten) te arrangeren, maar het brengt ook met zich mee dat informatie over de auteur, hoe wezenlijk ook, voor het MedMij Afsprakenstelsel een *gegevens-inhoudelijke* aangelegenheid is. Die informatie wordt immers ook gebruikt voor de interpretatie van de gedeelde zorg- en gezondheidsinformatie. Omdat, conform principe 1, het MedMij Afsprakenstelsel gegevensneutraal wil zijn, wordt de auteursinformatie een onderdeel geacht van de inhoud van een *Gegevensdienst*.

3.1. Algemeen

1.	*MedMij Beheer* onderhoudt een archief van alle ooit verspreide versies van de *Aanbiederslijst*, de *OAuth Client List*, de *Whitelist* en de *Gegevensdienstnamenlijst*. De bewaartermijn, gerekend vanaf het einde van de geldigheid van de betreffende versie, is niet korter dan die van de logbestanden als bedoeld in verantwoordelijkheid core.logging.101.	core.algemeen.100

3.2. Dossier

1.	*Dienstverlener persoon* biedt *Persoon* de functie *Verzamelen* om bij *Dienstverlener aanbieder* gezondheidsinformatie te verzamelen van *Aanbieder*, indien deze die informatie	

	beschikbaar stelt, die op deze *Persoon* betrekking heeft en laat deze in een persoonlijk gezondheidsdossier (kortweg *Dossier*) van *Persoon* bewaren. Bij deze functie betrokken rollen gebruiken hiertoe het betreffende stroomdiagram. Deze verantwoordelijkheid introduceert ook de notie van een persoonlijk gezondheidsdossier. Voor het voldoen aan deze regel is het dus niet voldoende aan de *Persoon* alleen inkijk in gezondheidsinformatie te bieden. Hij/zij moet het ook kunnen opslaan en beheren. Omdat deze functie zich over verschillende functionele rollen uitstrekt, is om interoperabiliteitsredenen de specificatie van het stroomdiagram aangehaald.	core.dossier.100
2.	*Dienstverlener persoon* biedt *Persoon* de functie *Delen* om bij *Dienstverlener aanbieder* ten behoeve van een *Persoon*, indien deze daartoe ontvankelijk is, gezondheidsinformatie te plaatsen die op deze *Persoon* betrekking heeft en die afkomstig is uit het *Dossier*. Bij deze usecase betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.	core.dossier.101
3.	*Dienstverlener persoon* draagt ervoor zorg dat in het *Dossier* bij alle bij *Dienstverlener aanbieder* in het kader van een *Gegevensdienst* verzamelde informatie onlosmakelijk deze *Dienstverlener aanbieder* en *Gegevensdienst* als bron en verzamelcontext worden aangetekend. *Dienstverlener persoon* draagt ervoor zorg dat, in geval van het delen van informatie met een (andere) *Aanbieder* deze bron- en context-informatie wordt meegeleverd aan de *Dienstverlener aanbieder*. Voor de benoeming van de bron wordt daarbij gebruik gemaakt van de *Aanbiedersnaam*. Voor de benoeming van de context wordt daarbij gebruik gemaakt van de betreffende *Gegevensdienstnaam* uit de *Gegevensdienstnamenlijst*. Hiermee wordt geborgd dat bij de uitgewisselde zorg- en gezondheidsinformatie altijd duidelijk is bij welke bron (*Dienstverlener aanbieder*) en in welke context (*Gegevensdienst*) deze is verzameld. Een ontvanger van deze informatie kan deze meta-informatie gebruiken voor een betere interpretatie van de betreffende informatie. Mochten hieruit alsnog interpretatievragen komen, kan de ontvanger zich vervoegen bij betreffende bron.	core.dossier.102
4.	*Dienstverlener persoon* biedt *Persoon* de functie *Raadplegen dossier* om het persoonlijk gezondheidsdossier te raadplegen. Omdat deze functie zich niet over meerdere domeinen uitstrekt, is zij niet nader gespecificeerd in een stroomdiagram. Het is aan de vrijheid van de *Deelnemer* om deze naar behoefte van haar klanten in te richten. Maar zij mag niet ontbreken, omdat dan de *Persoon* geen *Regie* over het dossier zou kunnen voeren.	core.dossier.103
5.	In het kader van de functie *Raadplegen dossier* zal *Persoon* te allen tijde moeten kunnen nagaan: • welke inhoud van het *Dossier* wel, en welke niet, via MedMij-verkeer van *Dienstverlener aanbieder* is betrokken van welke *Aanbieder,* en sindsdien niet is veranderd; • welke inhoud van het *Dossier* wel, en welke niet, via MedMij-verkeer bij *Dienstverlener aanbieder* is geplaatst ten behoeve van welke *Aanbieder*. Hiermee is het voor de *Persoon* duidelijk op welk deel van de inhoud van zijn dossier hij de aan het MedMij Afsprakenstelsel verbonden vertrouwen kan verbinden. Het is immers goed mogelijk dat een PGO alleen op bepaalde onderdelen deelneemt, en dus voldoet, aan het MedMij Afsprakenstelsel.	core.dossier.104

3.3. Opvragen gegevensdienstnamenlijst

1.	*MedMij Beheer* beheert en publiceert de *Gegevensdienstnamenlijst*. Deze beschrijft welke gebruikersvriendelijke namen horen bij welke *Gegevensdiensten.* De *Gegevensdienstnamenlijst* voldoet aan wat over haar is bepaald in de Informatiemodellen.	core.gnl.100
2.	*MedMij Beheer* biedt aan *Deelnemers* de functie *Opvragen Gegevensdienstnamenlijst* om de actuele versie van die *Gegevensdienstnamenlijst* op te vragen. Betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.	core.gnl.101
3.	*MedMij Registratie*, *DVP Server en Authorization Server* implementeren de functie *Opvragen Gegevensdiensnamenlijst*, door middel van het bepaalde inzake het Gegevensdienstnamenlijstinterface op Interfaces lijsten. Zij gebruiken hiervoor het betreffende stroomdiagram.	core.gnl.200
4.	*DVP Server en Authorization Server* betrekken minstens elke vijftien minuten (900 seconden) de meest recente *Gegevensdienstnamenlijst* van *MedMij Registratie*.	core.gnl.201
5.	*DVP Server en Authorization Server* valideren elke nieuwe verkregen *Gegevensdienstnamenlijst* tegen het XML-schema van de Gegevensdienstnamenlijst.	core.gnl.202

3.4. Opvragen Aanbiederslijst

1.	*MedMij Beheer* beheert en publiceert een *Aanbiederslijst*, namens de deelnemende *Dienstverlener aanbieder*. De gepubliceerde *Aanbiederslijst* bevat steeds en slechts alle actuele entries, en beschrijft van elke *Aanbieder*: • welke *Gegevensdiensten* deze momenteel aanbiedt, en welke technische adressen daarvoor moeten worden aangesproken bij de *Dienstverlener aanbieder*, gegeven een zekere *Interfaceversie*; Deze afspraak wijst *MedMij Beheer* de verantwoordelijkheid toe om ten behoeve van alle *Dienstverleners persoon* een lijst te verspreiden van *Aanbieders* en de door hen aangeboden *Gegevensdiensten*. Zonder deze functie zou het stelsel niet functioneren.	core.alst.100
2.	*MedMij Beheer* beheert en publiceert, in de *Aanbiederslijst*, unieke en gebruikersvriendelijke namen van *Aanbieders*, van het formaat `<aanbieder>@medmij.` Daarop is naamgevingsbeleid van toepassing. *Aanbieders* kunnen in hun directe of indirecte contact met *Personen* deze naam meegeven als hun "MedMij-naam". *MedMij Beheer* zorgt voor uniciteit en heeft het laatste woord bij het vaststellen ervan.	core.alst.101
3.	*MedMij Beheer* biedt aan *Dienstverleners persoon* een functie (*Opvragen Aanbiederslijst*) om de actuele versie van die *Aanbiederslijst* op te vragen. Betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.	core.alst.102
4.	*MedMij Registratie* en elke *DVP Server* implementeren de functie *Opvragen Aanbiederslijst*, door middel van het bepaalde inzake het Aanbiederslijstinterface op Interfaces lijsten. Zij gebruiken hiertoe het betreffende stroomdiagram.	core.alst.200
5.	*DVP Server* betrekt minstens elke vijftien minuten (900 seconden) de meest recente *Aanbiederslijst* van *MedMij Registratie*.	

		core.alst.201
6.	*DVP Server* valideert elke nieuw verkregen *Aanbiederslijst* tegen het XML-schema van de *Aanbiederslijst*.	core.alst.202

3.5. Opvragen Whitelist

1.	*MedMij Beheer* beheert en publiceert een actuele *Whitelist*, namens de deelnemende *Dienstverleners aanbieder* en *Dienstverleners persoon*. De *Whitelist* beschrijft welke *Nodes* in MedMij-verkeer mogen deelnemen. De *Whitelist* voldoet aan wat over haar is bepaald in de Informatiemodellen.	core.whl.100
2.	*MedMij Beheer* biedt aan *Deelnemers* de functie *Opvragen Whitelist* om de actuele versie van die *Whitelist* op te vragen. Betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.	core.whl.101
3.	De *MedMij Stelselnode* biedt aan *Nodes* de functie *Opvragen Whitelist* om de actuele versie van de *Whitelist* op te vragen. Betrokken rollen gebruiken hiervoor het betreffende stroomdiagram.	core.whl.300
4.	Het aandeel van de *MedMij Stelselnode* in de functie *Opvragen Whitelist* is voor minstens 99,9% van de tijd beschikbaar. *MedMij Registratie* laat, na het niet beschikbaar raken van het aandeel van *MedMij Stelselnode* in de usecase, maximaal acht uren (480 minuten) verstrijken voordat het weer beschikbaar is.	core.whl.301
5.	*Nodes* betrekken minstens elke vijftien minuten (900 seconden) de meest recente *Whitelist* van *MedMij Registratie*.	core.whl.302
6.	*MedMij Registratie* heeft `stelselnode.medmij.nl` als hostname. Door op deze manier de *MedMij Stelselnode* te autoriseren voor MedMij-verkeer wordt ervoor gezorgd dat ook in foutsituaties of bootstrap-situaties een *Backchannel Node* de *MedMij Stelselnode* kan aanspreken om een *Whitelist* op te halen.	core.whl.303
7.	*Nodes* valideren elke nieuw verkregen *Whitelist* tegen het XML-schema van de Whitelist. Alle hostnames op de *Whitelist* zijn fully-qualified domain names, conform RFC3696, sectie 2.	core.whl.304
8.	Ten behoeve van de technische beveiliging van het gegevensverkeer, dat zich voltrekt in het kader van de functie *Opvragen Whitelist,* maken betrokken rollen gebruik van *Versleuteling*, *Server Authentication* en *Server Authorization.*	core.whl.305
9.	*Backchannel Nodes* laten, elk hunnerzijds, backchannel-verkeer over het *MedMij-netwerk* dan en alleen dan doorgang vinden, nadat zij hebben vastgesteld dat de hostname van de andere *Node,* waarmee verbinding gemaakt zou worden, op de meest actuele *Whitelist* voorkomt. In geval van frontchannel-verkeer vindt er geen Server Authorization plaats.	core.whl.306
10.	De *Node* die	

	• de TLS-client zou worden voert de in verantwoordelijkheid core.whl.306 bedoelde controle tegen de *Whitelist* uit voorafgaand aan de start van de TLS-handshake. Indien die controle niet kan wor-den uitge-voerd of een negatief resultaat oplevert, wordt de TLS-handshake niet gestart. • de TLS-server is, voert de in verantwoordelijkheid core.whl.306 bedoelde controle tegen de *Whitelist* geheel uit voordat enige volgende stap wordt gezet door de *OAuth Authorization Server* of *OAuth Resource Server*, volgens de specifi-ca-ties van de functies *Verzamelen* en *Delen*. Deze vereiste wordt volgordelijkheid genoemd. Indien de contro-le tegen de *Whitelist* niet kan worden uit-gevoerd, of een negatief resultaat ople-vert, wordt de proces-gang onmiddellijk af-gebroken en komt het niet tot een start van de uit-voering van die eerstvolgende stap. De con-trole tegen de*Whitelist* slaagt in dit geval dan en slechts dan als op de *Whitelist* tenmin-ste een van de vol-gende namen uit het de door de TLS-client aange-boden certificaat voorkomen: de`Com-mon Name`of een van de eventuele `Subject Alterna-tive Names`	core.whl.307
11.	Voor zover de *Dienstverlener aanbieder* ervoor kiest de controle tegen de *Whitelist* na af-loop van de TLS-handshake uit te voeren, is deze controle logisch geschei-den van de bedoelde eerstvolgende stap. De vereiste volgordelijkheid kan wor-den aange-toond door middel van code-inspec-ties, penetratietesten en inspecties van logs. In geval van uitgaand verkeer kan de voorziene TLS-client de controle tegen de *Whitelist* al uitvoeren voordat hij de TLS-handshake initieert, omdat hij de voorziene TLS-server al heeft geïdentificeerd, om te weten wie hij überhaupt moet aanspreken. In geval van inkomend verkeer echter, kan de TLS-server de zich aandienende TLS-client pas identificeren gedurende of na de TLS-handshake, aan de hand van het certificaat dat hij, conform verantwoordelijkheid 2, moet ontvangen. Daarop moet een hostname voorkomen die op de *Whitelist* is terug te vinden. Door toe te staan dat niet alleen de `Common Name` de voor MedMij geautoriseerde hostname mag bevatten, maar ook een `Subject Alternative Name`, biedt het MedMij Afsprakenstelsel aan deelnemers de mogelijkheid tot hergebruik van certificaten voor meerdere MedMij-nodes, of voor meerdere doelen dan alleen deelname in MedMij. Het vroegste, en op het eerste gezicht dus meest veilige, moment om de controle tegen de *White-list*uit te voeren is in dat geval gedurende de TLS-handshake, tussen de ontvangst van het certificaat van de TLS-client en de voorziene ver-zending van de `Finished` message. Indien die controle niet kan wor-den uitge-voerd, of een ne-ga-tief resultaat oplevert, wordt dan in plaats van de `Finished message` de uitzondering `access_denied` verzonden. Hoewel sectie 7.2.2 van de TLS-spe-cifi-catievoorziet in deze mogelijkheid, voorzien veel standaardimplementaties er niet in. In-grepen in die standaard-im-plementaties zijn soms wel mogelijk, maar kunnen nieuwe beveili-gingsrisico's met zich meebren-gen, bijvoorbeeld vanwege de complexiteit van het beheren van maatwerk-aanpassingen aan stan-daardimplementa-ties. Daarom wil het MedMij Afsprakenstelsel implementatievrijheid bieden, zonder evenwel het risico te accepteren dat er inhoudelijke informatie gaat worden verwerkt die afkomstig is van een TLS-client, voordat de controle tegen de *Whitelist* heeft verzekerd dat die TLS-client tot MedMij-verkeer geauto-riseerd was. Omdat er meerdere manieren zijn om dat ook na afloop van de TLS-hand-shake te imple-men-teren, vereist het MedMij Afspraken-stelsel hiervoor geen vaste architectuur-va-riant (zoals met een re-verse proxy), maar stelt het de vereiste van vol-gordelijkheid, naast een logische scheiding. Deze moe-ten kunnen worden aangetoond door middel van code-inspectie, penetratietesten en in-specties van logs.	core.whl.308

12.	Indien een *Whitelist*-controle, in het kader van verantwoordelijkheid core.whl.307 en core.whl.308, niet kan worden uitgevoerd, of een negatief resultaat oplevert, breekt dit de voortgang af van de uitvoering van de functie en stellen de betrokken Applicatie-rollen elkaar hiervan niet op de hoogte. Omdat het niet slagen van de *Whitelist*-controle duidt op een niet te vertrouwen tegenpartij, wordt deze daarvan niet op de hoogte gesteld.	core.whl.309

3.6. Opvragen OAuth Client List

1.	*MedMij Beheer* beheert en publiceert een actuele *OAuth Client List*, namens de deelnemende *Dienstverleners persoon*. De gepubliceerde *OAuth Client List* bevat steeds en slechts alle actuele entries, en beschrijft van elke *OAuth Client*: • wat de gebruikersvriendelijke namen zijn die voor de *Dienstverleners persoon* worden gebruikt in de Toestemmingsverklaring , de Bevestigingsverklaring; *De OAuth Client List bevat dus geen namen voor Dienstverleners aanbieder.* Dat is niet nodig, omdat deze niet voorkomen in de *Toestemmingsverklaring.*	core.ocl.100
2.	De *OAuth Client List* voldoet aan wat over haar is bepaald in de Informatiemodellen.	core.ocl.101
3.	*MedMij Beheer* biedt aan *Deelnemers* de functie *Opvragen OAuth Client List* om de actuele versie van die *OAuth Client List* op te vragen. Betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.	core.ocl.102
4.	*MedMij Registratie* en *Authorization Server* implementeren de functie *Opvragen OAuth Client List*, door middel van het bepaalde inzake het interface voor OAuth Client List op Interfaces lijsten. Zij gebruiken hiervoor het betreffende stroomdiagram.	core.ocl.200
5.	*Authorization Server* betrekt minstens elke vijftien minuten (900 seconden) de meest recente OAuth Client List (OCL) van *MedMij Registratie*.	core.ocl.201
6.	*Authorization Server* valideert elke nieuwe verkregen OAuth Client List (OCL) tegen het XML-schema van de *OAuth Client List*.	core.ocl.202
7.	De *OAuth Client List* bevat voor elke *DVP Server* alleen die *Node* waarmee de betreffende *DVP Server* het frontchannelverkeer afhandelt. Conform het bepaalde onder core.rollen.300, mag een *DVP Server* meerdere *Nodes* gebruiken, maar mag de *DVP Server* maar één *Node* gebruiken voor al haar frontchannelverkeer, op het authorization interface dus. De inhoud van de *OAuth Client List* wordt alleen gebruikt op dat authorization interface, voor twee doelen: • het kennisnemen van de *Gegevensdiensten* waarop de *DVP Server* is erkend, zodat de *Authorization Server* een authorization request kan weigeren wanneer de *DVP Server* niet is erkend op de Gegevensdienst waarvoor hij autorisatie vraagt; • het kennisnemen van de naam van de *Dienstverlener persoon* die moet verschijnen in de Toestemmingsverklaring en de Bevestigingsverklaring.	core.ocl.300

	Daarom hoeft, voor een *DVP Server*, in de *OAuth Client List* alleen die ene *Node* te worden opgenomen die deze *DVP Server* voor haar frontchannelverkeer gebruikt. Om geen overbodige gegevens te verspreiden, worden alle andere eventuele *Nodes* van de *OAuth Client List* geweerd.	

3.7. Gegevensdiensten

1.	*Dienstverlener persoon* laat *Persoon* met een *Gegevensdienst* uit de *Gegevensdienstnamenlijst* gezondheidsinformatie verzamelen bij een *Dienstverlener aanbieder* of, ten behoeve van een *Aanbieder*, plaatsen bij een *Dienstverlener aanbieder*. Een *Gegevensdienst* is een op een specifieke en gestandaardiseerde set gezondheidsinformatie gerichte dienst waarmee *Dienstverlener aanbieder* zulke informatie ontsluit naar *Dienstverlener persoon* in het kader van de functie *Verzamelen* of *Dienstverlener aanbieder* zulke informatie geplaatst krijgt ten behoeve van een *Aanbieder*. In de *Gegevensdienstnamenlijst* zijn de *Gegevensdiensten* opgenomen die op enig moment worden aangeboden, maar de *Catalogus* is de autoriteit daarvoor.	core.gegevensdiensten.100
2.	Elke *Dienstverlener aanbieder* ontsluit op elk moment minstens één *Gegevensdienst*. Het ontsluiten van een *Gegevensdienst* door een *Dienstverlener aanbieder* is, in deze versie van het MedMij Afsprakenstelsel, hetzij in het kader van *Verzamelen* of in het kader van *Delen* van zekere gezondheidsinformatie. De term 'ontsluiten' wordt hier gebruikt in plaats van de term 'aanbieden', omdat als aanbieder van een *Gegevensdienst* de *Aanbieder* wordt gezien, niet de *Deelnemer* (*Dienstverlener aanbieder*). De *Deelnemer* ontsluit de *Gegevensdienst* dus namens de *Aanbieder* die die *Gegevensdienst* aanbiedt. De termen 'aanbieden' en 'ontsluiten' vertegenwoordigen een tweedeling in de verantwoordelijkheid voor een geleverde *Gegevensdienst*. De *Aanbieder* is, ook als verwerkingsverantwoordelijke in de zin der AVG, verantwoordelijk voor het aanbieden van een *Gegevensdienst* aan de *Dienstverlener persoon*; de *Dienstverlener aanbieder* is, ook als verwerker in de zin der AVG, verantwoordelijk voor het ontsluiten van diezelfde *Gegevensdienst* aan diezelfde *Dienstverlener persoon*. Aanbieden en ontsluiten zijn dus niet achter elkaar geschakeld: de *Aanbieder* biedt de *Gegevensdienst* niet zozeer aan de *Dienstverlener aanbieder* aan, maar aan de *Dienstverlener persoon* . Aanbieden en ontsluiten zijn aspecten van eenzelfde geleverde *Gegevensdienst*: het eerste het verwerkingsverantwoordelijke, het tweede het verwerkende.	core.gegevensdiensten.101
3.	*MedMij Beheer* zal alleen in de *Aanbiederslijst* opnemen dat een zekere *Gegevensdienst* door een zekere *Aanbieder* via een *Dienstverlener aanbieder,* wordt aangeboden, indien zij (*Stichting MedMij*) heeft vastgesteld dat de *Dienstverlener aanbieder* voldoet aan de specifiek op die *Gegevensdienst* toepas-selij-ke eisen. Omdat er een indirectie speelt, via de *Dienstverlener aanbieder* naar de *Aanbieder*, moet gezegd worden dat één *Aanbieder* genoeg is (die een bepaalde *Gegevensdienst* ontsluit) om ervoor te zorgen dat de	core.gegevensdiensten.102

	Dienstverlener aanbieder zich voor die *Informatiestandaard* moet kwalificeren in het MedMij Afsprakenstelsel.	
4.	Voor elke *Gegevensdienst* waarvan de *Aanbiederslijst* aan-geeft dat een zekere *Aanbieder* deze aanbiedt, zal een *Dienstverlener aanbieder* ervoor zorgdragen dat die *Gegevensdienst* ook geleverd wordt. Daarbij wordt geen enkel onderscheid gemaakt tussen *Dienstverleners persoon*, tenzij het MedMij Afsprakenstelsel daartoe uitdrukkelijk verplicht. Dit geldt ook voor de mogelijke andere *Gegevensdienst(en)* die in de *Catalogus* staan genoemd als *Vereist* bij eerstgenoemde *Gegevensdienst*. Net als verantwoordelijkheid core.gegevensdiensten.102, moet ook vanuit deze verantwoordelijkheid rekening houden met de indirectie via *Dienstverlener aanbieder* naar de *Aanbieder* zelf. Deze regel legt het bij de *Dienstverlener aanbieder* om ervoor zorg te dragen dat de *Aanbieder* met wie hij een dienstverleningsovereenkomst heeft, ook de *Gegevensdienst* levert die hij toegezegd heeft.	core.gegevensdiensten.103
5.	Het in verantwoordelijkheid core.gegevensdiensten.103 bepaalde is ook van toepassing zolang de geldigheid van de toepasselijke vermelding in de *Aanbiederslijst* niet langer dan één uur (3600 seconden) geleden is verstreken. Zo wordt ervoor ruimte geboden dat na-ijlende sessies, die nog gebruik maken van de verstrijkende versie van de *Aanbiederslijst*, nog kunnen worden afgemaakt.	core.gegevensdiensten.104
6.	Als een *Dienstverleners persoon* een zekere *Gegevensdienst* ontsluit ten behoeve van zijn *Personen* en daartoe laat leveren door een *Dienstverlener aanbieder*, zullen de *DVP Server* van die *Dienstverlener persoon* en de *Authorization Server* en *Resource Server* van die *Dienstverlener aanbieder* daarvoor de bij de *Gegevensdienst* horende functie implementeren en de bij de *Gegevensdienst* horende *Systeemrollen* gebruiken, zoals deze in de *Catalogus* zijn opgenomen, en zich daarbij te conformeren aan de specificaties van die *Systeemrollen* zoals die zijn gepubliceerd op de plaats(en) waarnaar de *Catalogus* verwijst met *Functionelespecificatieverwijzing* en *Technischespecificatieverwijzing*. Zo wordt geborgd dat de juiste functie-implementaties en informatiestandaarden worden gebruikt. Ook wordt het correcte gebruik geborgd, wat bijdraagt aan interoperabiliteit en vertrouwen.	core.gegevensdiensten.200

4. Autorisatie

1.	*Dienstverlener aanbieder* vergewist zich ervan, elke keer opnieuw voordat hij *Persoon* gezondheidsinformatie van *Aanbieder* laat verzamelen door middel van de functie *Verzamelen*, dat deze *Persoon* uitdrukkelijk *Toestemming* heeft gegeven aan *Aanbieder* om de in de *Gegevensdienst* betrokken gezondheidsinformatie aan *Dienstverlener persoon* ter beschikking te laten stellen. De vraag om *Toestemming* heeft een vaste formulering, die is opgenomen in de functie *Verzamelen*. Deze *Toestemming* is slechts van kracht binnen één doorloping van de usecase. Het is dus de *Dienstverlener aanbieder* die de *Toestemming* ophaalt bij de *Persoon*. De tweede zin van deze verantwoordelijkheid maakt de toestemming functioneel zo eenvoudig mogelijk, omdat in deze release van het MedMij Afsprakenstelsel alleen	core.autorisatie.100

	met een eenmalige vraag gezondheidsinformatie verzameld kan worden. De toestemming, hoe expliciet ook, heeft precies dezelfde reikwijdte als die eenmalige vraag.	
2.	*Dienstverlener aanbieder* vergewist zich ervan, elke keer opnieuw voordat hij *Persoon* gezondheidsinformatie ten behoeve van *Aanbieder* laat plaatsen, dat deze *Persoon* uitdrukkelijk heeft bevestigd om de in de *Gegevensdienst* betrokken gezondheidsinformatie aan *Aanbieder* ter beschikking te willen stellen. De vraag om *Bevestiging* heeft een vaste formulering, die is opgenomen in de functie *Delen*. Deze bevestiging geldt niet buiten één doorloping van de functie *Delen*. Deze verantwoordelijkheid is welbewust niet geïntegreerd met verantwoordelijkheid 1 omdat de hier bedoelde bevestiging niet de juridische status heeft van de in verantwoordelijkheid 1 bedoelde *Toestemming*.	core.autorisatie.101
3.	In de implementatie van de functies *Verzamelen* en *Delen* handelen *DVP Server* enerzijds en *Authorization Server* en *Resource Server* anderzijds, hun onderlinge verkeer af conform de standaard OAuth 2.0. Conform wettelijke verplichting geeft *Persoon*, in de functie *Verzamelen*, actief toestemming aan de *Aanbieder.* In de functie *Delen* is deze verplichting niet aan de orde, maar vindt op dit moment evengoed een bevestiging door de *Persoon* plaats. De *User Agent* presenteert een venster waarin de *Persoon* deze toestemming, respectievelijk bevestiging, kan geven. Aangezien in het persoonsdomein niet met BSN gewerkt mag worden, moet er een vervangende identificatie van de *Persoon* gebruikt worden.	core.autorisatie.200
4.	Van de vier soorten authorization grants die OAuth 2.0 biedt, beperken de OAuth-rollen zich tot Authorization Code. Met deze ene soort kunnen alle situaties die in het MedMij Afsprakenstelsel voorkomen worden bediend. Voor het maximaliseren van de interoperabiliteit kiest MedMij ervoor de andere drie soorten uit te sluiten.	core.autorisatie.201
5.	De *OAuth Client* en *OAuth Resource Server* zullen slechts tokens van het type Bearer-token uitwisselen, conform RFC6750. De OAuth-standaard laat het (access) token type vrij. Token types verschillen in het vertrouwen waarmee de *OAuth Resource Server* aan de *OAuth Client* de gevraagde resources kan prijsgeven als laatstgenoemde het access-token aan eerstgenoemde overlegt. Bij de eenvoudigste vorm (bearer-token) geeft de *OAuth Resource Server* eenvoudigweg aan elke *OAuth Client* die een geldig access-token overlegt, de resources die daarbij horen. "Aan toonder", net zoals een bank een cheque kan verzilveren aan toonder. Daaraan kleven evenwel veiligheidsrisico's, omdat het access-token na uitgifte gestolen kan zijn, of anderszins vervreemd van de *OAuth Client* aan wie het uitgedeeld was. Andere token types kunnen daarom vragen om meer garanties, zoals een identiteit van de *OAuth Client* of een client-secret. Bearer-token is echter het enige goed gestandaardiseerde en breed gebruikte token type. Het legt wel veel verantwoordelijkheid voor beheersing van de veiligheidsrisico's bij *OAuth Client* en *OAuth Authorization Server*. In hoofdstuk 5 van de specificatie van de standaard RFC6750 is daarom expliciete aandacht voor die beveiligingsrisico's en maatregelen om die het hoofd te bieden.	core.autorisatie.202
6.		

	De *OAuth Client* maakt alleen gebruik van één scope tegelijk. De *OAuth Authorization Server* genereert authorization-codes en access-tokens met een enkelvoudige scope die geheel vervat moet zijn in de *Gegevensdienst* waarom de *OAuth Client* heeft gevraagd. Bij het genereren van codes en tokens is de OAuth-scope meegenomen. Deze is gerelateerd aan de *Gegevensdienst*. Hoewel het technisch mogelijk is om meerdere scopes mee te geven is de scope beperkt tot één *Gegevensdienst* per keer.	core.autorisatie.203
7.	De *OAuth Authorization Server* stelt van elke uitgegeven authorization-code en elk uitgegeven access-token de geldigheidsduur op exact 15 minuten (900 seconden). Zij geeft bovendien geen refresh-tokens uit. Dit is een maatregel tegen de beveiligingsrisico's 4.4.1.1 en 4.4.1.3 uit RFC 6819. Bovendien wordt de hele flow van de functie *Verzamelen* ononderbroken uitgevoerd. De 900 seconden moeten dan voldoende zijn voor de *OAuth Client* om het access-token aan de *OAuth Authorization Server* aan te bieden. Een refresh-token is dan niet nodig.	core.autorisatie.204
8.	De *OAuth Authorization Server* genereert authorization-codes en access-tokens zodanig, dat de kans op het raden ervan niet groter is dan 2^{-128} en de daarvoor gebruikte random number generators cryptografisch veilig zijn.	core.autorisatie.205

7.	In de authorization-codes en access-tokens is het desgewenst toegestaan één of meer van de informatie-elementen uit de volgende limitatieve lijst op te nemen:
	
	• een identifier van de authorization-code, respectievelijk het access-token, indien die identifier op zichzelf voldoet aan de in verantwoordelijkheid 6 genoemde eisen;
	• een verloopmoment van de geldigheid van het token, onder de voorwaarden dat zowel:
	  • de waarde daarvan in overeenstemming is met de verantwoordelijkheden in het MedMij Afsprakenstelsel en
	  • uit het verstreken zijn daarvan wél de ongeldigheid van de authorization-code of het access-token mag worden geconcludeerd door de *OAuth Authorization Server* of de *Resource Server*, maar uit het nog niet verstreken zijn daarvan **niet** diens geldigheid, waarvoor namelijk een validatie van het gehele token tegen de interne administratie van de *OAuth Authorization Server* de enige autoriteit is;
	• een identificatie van de service die het token heeft uitgegeven;
	• de `scope` waarvoor de authorization-code of het access-token is uitgegeven, in de vorm van een kopie van de `scope`-parameter van de authorization request in antwoord waarop de authorization-code of het access-token is uitgegeven;
	• de naam van het token-formaat;
	• een digitale handtekening.
		core.autorisatie.206

9.	Geen andere informatie dan de in verantwoordelijkheid 7 genoemde mag voorkomen in de authorization-code of het acces-token, ook niet versleuteld. Er mogen t.a.v. informatie-inhoud van het token verschillende keuzes gemaakt worden tussen authorization-code en access-token. De *OAuth Client* mag de inhoud van het token niet interpreteren.	core.autorisatie.207
10.	Met betrekking tot zowel authorization-codes als access-tokens, draagt de *OAuth Authorization Server* die hen uitgeeft ervoor zorg, dat daarvan nooit twee dezelfde geldige in omloop zijn.	core.autorisatie.208

Dit is een maatregel tegen beveiligingsrisico 4.4.1.3 uit RFC 6819. Aan de in omloop gebrachte authorization-codes en access-tokens zijn twee belangrijke eisen te stellen: uniciteit en vertrouwelijkheid. De eis van vertrouwelijkheid weegt in het MedMij Afsprakenstelsel zwaar. Omdat de authorization-code (indirect) en het access-token (direct) toegang geven tot persoonlijke gezondheidsinformatie, kiest MedMij voor een formaat dat vrijwel betekenisloos is en alleen betekenis krijgt door confrontatie met lokale en goed beschermde administraties van de *OAuth Authorization Server*. De maximale raadkans wordt geëist in RFC6749, sectie 10.10 . Er mag door vergelijking van meerdere authorization-codes of access-tokens niet doorschemeren hoe zij gegenereerd worden.

Wanneer een identifier is opgenomen in het access-token, kan dat gebruikt worden als identificatie van de *OAuth Authorization Server*-sessie waarin het token werd uitgegeven, zodat de *OAuth Resource Server* deze sessie kan hervatten wanneer zij het access-token aangeboden krijgt. Het is ook mogelijk dat een dergelijke identifier niet zozeer is opgenomen in de authorization-code, respectievelijk het access-token, maar geheel overeenkomt met de authorization-code, respectievelijk het access-token. Hoe dan ook, verantwoordelijkheid 6 blijft erop van kracht.

Wanneer een verloopmoment is opgenomen in het access-token, wordt het mogelijk om de *OAuth Resource Server* te laten afzien van onnodige raadpleging van de *OAuth Authorization Server*, wanneer deze apart geïmplementeerd zouden zijn. De tweede voorwaarde bij deze mogelijkheid voorkomt dat een eventuele corrumpering, in het *Persoonsdomein*, van de authorization-code of het access-token waarbij het verloopmoment verlaat zou worden, leidt tot onterechte toegang tot, of onterechte plaatsing van gezondheidsinformatie. Het accepteren van een authorization-code of een access-token gebeurt altijd in het licht van de interne administratie van de *OAuth Authorization Server*. Die corrumpering kan het verloopmoment ook vervroegen, maar richt dan weinig schade aan. Overigens kan in de deze versie van het MedMij Afsprakenstelsel, waarin de geldigheidsduur een vaste waarde heeft, de *OAuth Client* zelf ook al uitrekenen wanneer het geen zin meer heeft een authorization-code of access-token nog aan te bieden. De meerwaarde van het opnemen van een verloopmoment in de authorization-code of het access-token zal dus hooguit in mogelijke toekomstige versies kunnen blijken.

De service die het token heeft uitgegeven is al wel in deze versie van het MedMij Afsprakenstelsel een nuttig informatie-element. In situaties waarin een *OAuth Resource Server* samenwerkt met meerdere van hem gescheiden geïmplementeerde *OAuth Authorization Server*, moet deze bij een aangeboden access-token kunnen bepalen welke *OAuth Authorization Server* moet worden aangesproken. Dat aanspreken kan bijvoorbeeld door middel van Token Introspection volgens RFC7662. De geëigende bron voor die informatie is het access-token zelf, dat weet heeft van zijn afkomst. Die afkomstinformatie levert geen extra privacyrisico's op, omdat de *OAuth Client* sowieso op de hoogte is van wie hij het access-token heeft ontvangen.

Verder mag de *OAuth Authorization Server* ook een kopie van de `scope` opnemen in (de authorization-code of) het access-token, de `scope` die hij eerder in de authorization request heeft ontvangen van de *OAuth Client* (zie Authorization interface). Zo hoeft de *OAuth Resource Server* niet apart door de *DVP Server* van de `scope` op de hoogte gebracht te worden. De authorization-code of het access-token draagt zo weliswaar extra betekenis, maar de risico's daarvan wegen niet op tegen de risico's van het apart door de *DVP Server* laten sturen van de scope, die bijvoorbeeld zou kunnen afwijken van die waarvoor de authorization-code of het access-token is uitgegeven.

	De lijst van toegestane informatie-elementen is limitatief. Geen andere informatie, ook niet versleuteld, mag in de authorization-code of het access-token zijn opgenomen. Daaronder vallen zeker ook: • informatie over *Persoon*; • informatie over *Aanbieder of Gegevensdienst*, al dan niet in relatie tot *Persoon*, buiten de `scope`; • benoeming van, en beperkingen aan, de beoogde acceptanten van de authorization-code of het access-token. Op dit punt is namelijk de *Aanbiederslijst* de autoriteit: als de *OAuth Client* een access-token heeft opgehaald op een plek die daartoe in de *Aanbiederslijst* stond, dan moet hij dat access-token kunnen aanbieden aan de plek die daartoe in de *Aanbiederslijst* staat. --- Het verbod op interpretatie door de *OAuth Client* van authorization-code en access-token zorgt ervoor dat er een minimale afhankelijkheid wordt gecreëerd tussen de dienstverleners in het Persoonsdomein enerzijds en die in het Aanbiedersdomein anderzijds, zodat P1 en P7 maximaal worden nageleefd en interne complexiteit en implementatiekeuzes in het Aanbiedersdomein niet doorschemeren in, of invloed uitoefenen op, de implementatie in het Persoonsdomein. De beperkingen van betekenisdragendheid van de authorization-code en het access-token, zelfs indien versleuteld, bevorderen de privacy door middel van dataminimalisatie. Bovendien voorkomen zij nieuwe risico's op compromittering van die informatie-inhoud. Zulke compromittering zou moeilijk te ontdekken en te pareren zijn in het Aanbiedersdomein, ingeval men er daar toe besloten zou hebben van interne autorisatie-administratie af te zien omdat de informatie toch al meereist op de authorization code of het acces token, via de *OAuth Client*.	
11.	Access-tokens worden alleen uitgegeven na controle van de client_id, de opgegeven autorisatie-code en de Common name van het in de TLS verbinding gebruikte certificaat. De controles worden uitgevoerd conform: • IETF RFC 6749, De code moet zijn uitgegeven aan de opgegeven client_id. • IETF RFC 8705, Bij het verzoek naar het token-endpoint wordt gebruikgemaakt van een certificaat, waarvan de Common name geregistreerd is bij de opgegeven client_id. **Controle certificaat optioneel** De controle van het in de TLS verbinding gebruikte certificaat is vooralsnog optioneel. De implementatie van deze controle wordt sterk aangeraden, zodat met een hogere mate van zekerheid de verzoekende partij kan worden vastgesteld.	core.autorisatie.209
12.	Het OAuth-client type van de *OAuth Client* is confidential. Om de privacy te kunnen borgen is het van belang dat de *OAuth Authorization Server* voldoende zekerheid heeft over de identiteit van de *OAuth Client*. Die zekerheid is afhankelijk van hoe goed de *OAuth Client* zijn credentials vertrouwelijk kan houden. Daartoe maakt de OAuth-specificatie onderscheid tussen twee client types: confidential en public. De eerste soort kan een voor de *OAuth Authorization Server* afdoende mate van vertrouwelijkheid van zijn credentials bieden, de tweede	core.autorisatie.210

	niet. Het is een hoofddoel van MedMij om zulk vertrouwen te borgen in een afsprakenstelsel en niet over te laten aan individuele spelers. Daarom verbindt het MedMij Afsprakenstelsel verantwoordelijkheden aan *OAuth Clients* ten behoeve van hun betrouwbaarheid jegens *OAuth Authorization Server*. We verwachten dat een groot deel van de implementaties van de *OAuth Client* (van de *DVP Server* dus) deze vertrouwelijkheid sowieso kunnen bieden, omdat ze de architectuur hebben van wat de OAuth-specificatie web application noemt. Andersoortige *DVP Server*-architecturen, zoals die van een app, zijn ook mogelijk, maar alleen onder de voorwaarde dat de *OAuth Client* al het credentials-verkeer in de achtergrond op een server afhandelt, niet via het user device.	

5. Authenticatie

1.	*Dienstverlener aanbieder* draagt ervoor zorg dat de onder core.gegevensdiensten.103 , core.gegevensdiensten.104, core.autorisatie.100 en core.autorisatie.101 bedoelde vraag om *Toestemming*, respectievelijk bevestiging, slechts plaatsvinden wanneer hij de identiteit van de *Persoon* met passende zekerheid heeft vastgesteld.	core. authenticatie. 100

6. Adressering

1.	De *OAuth Client* stelt conform RFC 3986 de URI samen waarmee hij zichzelf, de *Authorization Server* en de *Resource Server* adresseert.	core. adressering. 200

2.	De URI's een hostname die een fully-qualified domain name is, conform RFC3696, sectie 2, en heeft het patroon `scheme://host path`, waarbij:
	• `scheme` altijd `https` is, in lowercase;
	• `host` een hostname is waarin
	  • slechts de karakters [a-z], [0-9], "." (punt) en "-" (koppelteken) voorkomen;
	  • elke punt twee opeenvolgende segmenten scheidt en van elk der gescheiden segmenten geen deel uitmaakt;
	  • het eerste karakter van een segment geen koppelteken is;
	  • elk segment minstens één karakter lang is;
	  • het laatste segment minstens twee karakters lang is;
	  • het laatste karakter geen koppelteken mag zijn;
	  • maximaal 255 tekens voorkomen;
	  • ten minste twee segmenten voorkomen;
	• `path` de syntax heeft van `path-abempty` uit sectie 3.3 van RFC 3986 (en dus leeg mag zijn), maar niet eindigt op een `/`.
	
	De eis dat `https` in lowercase staat volgt de canonical form zoals gespecificeerd in sectie 3.1 van RFC 3986. De eisen aan de hostname zijn o.a. gebaseerd op RFC 952 en RFC 1123. Het laatste segment is het zogeheten top-level domain.
		core. adressering. 201

3.	In alle adressering op het authorization interface, het token interface en het resource interface is het gebruik van het voor `https` bedoelde poortnummer, zoals opgenomen in de Service Name and Transport Protocol Port Number Registry van IANA, verplicht. Dat geldt dus ook voor de `redirect_uri`. In release 1.1.1 van het MedMij Afsprakenstelsel was deze verantwoordelijkheid alleen van toepassing op frontchannel-verkeer en had de *Dienstverlener aanbieder*	core. adressering. 202

	voor back-channelverkeer de vrijheid om een ander poortnummer te kiezen dan dat conform de IANA-lijst bij `https` hoort (443). Dat zorgt echter voor een extra beveiligingsbeheerlast bij de *DVP Server* die rekening houden met meerdere bestemmingspoortnummers bij uitgaand verkeer. Die beheerst brengt indirect ook extra beveiligingsrisico's met zich mee. Daartegenover staat dat de in deze release aangebrachte aanscherping naar verwachting geen wezenlijke beperking voor *Dienstverleners aanbieder* zal zijn, omdat zij toch al gebruik maken van het voor `https` bedoelde poortnummer uit de IANA-lijst. Een mogelijke uitzondering vormt de situatie waarin de *Authorization Server* en/of *Resource Server* in een multi-tenant omgeving draaien.	
4.	Voor het samenstellen van alle adressen van het authorization request en het token request, betrekt de *OAuth Client* de eerste onderdelen van de URI, namelijk `host` en `path`, uit de *Aanbiederslijst*, op basis van de van toepassing zijnde *Aanbieder*, *Interfaceversie* en *Gegevensdienst.* Andere elementen van de algemene URI-syntax, zoals `user`, `password`, `query` en `fragment`, zijn afwezig in de adressen. Voor het samenstellen van alle adressen van het resource request, betrekt de *OAuth Client* de base url (het onderdeel van de URI dat is aangeduid als `[base]` in de specificaties van de *Transactie* die behoort bij de van toepassing zijnde combinatie *Aanbieder*, *Gegevensdienst* en *Systeemrol*), uit de *Aanbiederslijst*, op basis van de van toepassing zijnde *Aanbieder*, *Interfaceversie*, *Gegevensdienst* en *Systeemrol*. Wanneer de specificaties een request identificeren maar geen `[base]` aanduiden, mag de *OAuth Client* het resource request alleen indienen als de volledige, absolute URI van het resource request begint met de volledige *ResourceEndpointuri* zoals die is verkregen uit de *Aanbiederslijst*, op basis van de van toepassing zijnde *Aanbieder*, *Interfaceversie*, *Gegevensdienst* en *Systeemrol*.	core.adressering.203
5.	*MedMij Registratie* wordt in de functies Opvragen Aanbiederslijst, Opvragen OAuth Client List en Opvragen Gegevensdienstnamenlijst geadresseerd met de hostname `stelselnode.medmij.nl`.	core.adressering.204

De *Aanbiederslijst* wordt dus gebruikt door de *OAuth Client* om, gegeven een zekere *Interfaceversie*, het endpoint te kennen dat past bij de van toepassing zijnde *Aanbieder, Gegevensdienst* en, voor het resource endpoint, *Systeemrol*. Net zo gebruikt de *Notification Client* de *OAuth Client List* om, gegeven een zekere *Interfaceversie*, het endpoint te kennen dat past bij de van toepassing zijnde *OAuth Client* en *Gegevensdienst*. Daarom moet er uit één zo'n setje één endpoint-adres volgen. Andersom echter is dat geen eis. Het is mogelijk om, in elke door de *Dienstverlener Aanbieder* gewenste combinatie, endpointadressen te hergebruiken voor meerdere van zulke setjes in de *Aanbiederslijst*, respectievelijk door de *Dienstverlener persoon* in de *OAuth Client List*.

7. Beveiliging

1.	In het gegevensverkeer voor de functies *Verzamelen*, *Delen*, Opvragen Aanbiederslijst, *Opvragen OAuth Client List* en *Opvragen Gegevensdienstnamenlijst*, maken betrokken rollen gebruik van de functies *Versleuteling*, *Server Authentication* en *Server Authorization*, zoals beschreven onder TLS en certificaten.	core.beveiliging.200
2.	De *OAuth Client* en *OAuth Authorization Server* gebruiken voor al hun onderlinge verkeer PKI-certificaten, en wel servercertificaten, ten behoeve van de authenticatie van de andere server in een uitwisseling. Dit is een maatregel tegen beveiligingsrisico's 4.4.1.1, 4.4.1.3, 4.4.1.4 en 4.4.1.5 in RFC 6819. De PKI-certificaten worden in deze release van het MedMij	core.beveiliging.201

Afsprakenstelsel gebruik voor twee doelen op de tehnologielaag: authenticatie van servers en versleuteling, waarmee de vertrouwelijkheid en integriteit van de inhoud van het gegevensverkeer wordt geborgd.

3. De *OAuth Client* realiseert de volgende beveiligingsmaatregelen, conform RFC 6819: — core.beveiliging.202

beveiligingsmaatregel	paragraaf in RFC 6819	gemitigeerde risico('s)
Clients should use an appropriate protocol, such as OpenID or SAML to implement user login. Both support audience restrictions on clients.	4.4.1.13	4.4.1.13
All clients must indicate their client ids with every request to exchange an authorization "code" for an access token.		
Keep access tokens in transient memory and limit grants.	5.1.6	
Keep access tokens in private memory.	5.2.2	4.1.3
The "state" parameter should be used to link the authorization request with the redirect URI used to deliver the access token.	5.3.5	4.4.1.8
CSRF defense and the "state" parameter created with secure random codes should be deployed on the client side. The client should forward the authorization "code" to the authorization server only after both the CSRF token and the "state" parameter are validated.	4.4.1.12	

4. De *OAuth Client* realiseert de volgende beveiligingsmaatregelen, conform RFC 6819: — core.beveiliging.203

beveiligingsmaatregel	paragraaf in RFC 6819	gemitigeerde risico('s)
Client applications should not collect authentication information directly from users and should instead delegate this task to a trusted system component, e.g., the system browser.	4.1.4	4.1.4
The client server may reload the target page of the redirect URI in order to automatically clean up the browser cache.	4.4.1.1	4.4.1.1
If the client authenticates the user, either through a single-sign-on protocol or through local authentication, the client should suspend the access by a user account if the number of invalid authorization "codes" submitted by this user exceeds a certain threshold.	4.4.1.12	4.4.1.12
Client developers and end users can be educated to not follow untrusted URLs.	4.4.1.8	4.4.1.8

	For newer browsers, avoidance of iFrames during authorization can be enforced on the server side by using the X-FRAME-OPTIONS header. For older browsers, JavaScript frame-busting techniques can be used but may not be effective in all browsers.	5.2.2.6	4.4.1.9
	Explain the scope (resources and the permissions) the user is about to grant in an understandable way	5.2.4.2	4.2.2

5. De *OAuth Authorization Server* realiseert de volgende beveiligingsmaatregelen, conform RFC 6819:

core.beveiliging.204

beveiligingsmaatregel	paragraaf in RFC6819	gemitigeerde risico('s)
Authorization servers should consider such attacks: Password Phishing by Counterfeit Authorization Server	4.2.1	4.2.1
Authorization servers should attempt to educate users about the risks posed by phishing attacks and should provide mechanisms that make it easy for users to confirm the authenticity of their sites.		
Authorization servers should decide, based on an analysis of the risk associated with this threat, whether to detect and prevent this threat.	4.4.1.10	4.4.1.10
The authorization server may force a user interaction based on non-predictable input values as part of the user consent approval.		
The authorization server could make use of CAPTCHAs.		
The authorization server should consider limiting the number of access tokens granted per user.	4.4.1.11	4.4.1.11
The authorization server should send an error response to the client reporting an invalid authorization "code" and rate-limit or disallow connections from clients whose number of invalid requests exceeds a threshold.	4.4.1.12	4.4.1.12
Given that all clients must indicate their client ids with every request to exchange an authorization "code" for an access token, the authorization server must validate whether the particular authorization "code" has been issued to the particular client.	4.4.1.13	4.4.1.13
Best practices for credential storage protection should be employed.	5.1.4.1	4.4.1.2
Enforce system security measures.	5.1.4.1.1	4.3.2 en 4.4.1.2

	Enforce standard SQL injection countermeasures.	5.1.4.1.2		
	Store access token hashes only.	5.1.4.1.3		
	The authorization server should enforce a one-time usage restriction.	5.1.5.4	4.4.1.1	
	If an authorization server observes multiple attempts to redeem an authorization "code", the authorization server may want to revoke all tokens granted based on the authorization "code".	5.2.1.1		
	Bind the authorization "code" to the redirect URI.	5.2.4.5	4.4.1.3	
	the authorization server associates the authorization "code" with the redirect URI of a particular end-user authorization and validates this redirect URI with the redirect URI passed to the token's endpoint,	4.4.1.7		
6.	*OAuth Client*, *OAuth Authorization Server* en *OAuth Resource Server* implementeren de op deze respectievelijke rollen toepasselijke beveiligingsmaatregelen, volgens paragaaf 5.3 van RFC 6750. Deze verantwoordelijkheid is opgenomen omdat met het bearer token informatie verkregen kan worden zonder dat nogmaals de identiteit wordt gecontroleerd. Daarom moeten maatregelen getroffen worden om te waarborgen dat het token alleen correct gebruikt kan worden.			core.beveiliging.205

Voor het opstellen van bovenstaande verantwoordelijkheden is gebruikgemaakt van RFC 6819 van IETF, dat een uitgebreide inventarisatie van die risico's bevat, inclusief een reeks van maatregelen per risico. Waar het risico van toepassing is op het gebruik van OAuth binnen MedMij, en de maatregelen passen binnen de MedMij-principes, zijn zij opgenomen in het afsprakenstelsel.

Met betrekking tot het gestelde in sectie 3.1 van RFC 6819 kan gesteld worden dat MedMij uitgaat van:

- handles i.p.v. assertions, zodat de *OAuth Resource Server* moet kunnen refereren aan data van de *OAuth Authorization Server;*
- bearer-tokens i.p.v. proof-tokens.

In hoofdstuk 4 van RFC 6819 staat een uitgebreide lijst van beveiligingsrisico's. Niet van toepassing zijn, voor de deze release van het afsprakenstelsel:

- bedreiging 4.1.2: Obtaining Refresh Tokens, omdat het afsprakenstelsel niet met refresh tokens werkt;
- bedreiging 4.2.3: Malicious Client Obtains Existing Authorization by Fraud, omdat in het afsprakenstelsel de autorisatie (vooralsnog) strikt eenmalig mag worden gebruikt;
- bedreiging 4.3.4: Obtaining Client Secret from Authorization Server Database, omdat authenticatie van *OAuth Clients* in MedMij werkt op basis van PKI-servercertificaten, niet op basis van client secrets;
- bedreiging 4.3.5: Obtaining Client Secret by Online Guessing, omdat authenticatie van *OAuth Clients* in MedMij op basis van PKI-servercertificaten wordt gedaan, niet op basis van client secrets .

Wel van toepassing zijn:

- bedreiging 4.1.3: Obtaining Access Tokens;

- bedreiging 4.1.4: End-user Credential Phished Using Comprised or Embedded Browser;
- bedreiging 4.1.5: Open Redirectors on Client;
- bedreiging 4.2.1: Password Phishing by Counterfeit Authorization Server;
- bedreiging 4.2.2: User Unintentionally Grants Too Much Access Scope;
- bedreiging 4.2.4: Open Redirector;
- bedreiging 4.3.1: Eavesdropping Access Tokens;
- bedreiging 4.3.2: Obtaining Access Tokens from Authorization Server Database;
- bedreiging 4.3.3: Disclosure of Client Credentials during Transmission;
- bedreiging 4.1.1: Obtaining Client Secrets;
- bedreiging 4.4.1.1: Eavesdropping or Leaking Authorization Code;
- bedreiging 4.4.1.2: Obtaining Authorization "codes" from Authorization Server Database;
- bedreiging 4.4.1.3: Online Guessing of Authorization "codes";
- bedreiging 4.4.1.4: Malicious Client Obtains Authorization;
- bedreiging 4.4.1.5: Authorization "code" Phishing;
- bedreiging 4.4.1.6: User Session Impersonation;
- bedreiging 4.4.1.7: Authorization "code" Leakage through Counterfeit Client;
- bedreiging 4.4.1.8: CSRF against redirect-URI;
- bedreiging 4.4.1.9: Clickjacking Attack against Authorization;
- bedreiging 4.4.1.10: Resource Owner Impersonation;
- bedreiging 4.4.1.11: DoS Attacks That Exhaust Resources;
- bedreiging 4.4.1.12: DoS Using Manufactured Authorization "codes";
- bedreiging 4.4.1.13: Code Substitution (OAuth Login).

In relatie tot het MedMij Afsprakenstelsel vallen de maatregelen die getroffen moeten worden ter mitigatie van deze risico's uiteen in drie groepen:

- maatregelen waarin al is voorzien door één of meerdere verantwoordelijkheden in het MedMij-afsprakenstelsel, zoals bijvoorbeeld:
  - het gebruik van TLS;
  - het gebruik van een (externe) *Authentication Server*;
  - het beperken van de scope en de geldigheidsduur van authorization codes en access tokens;
  - verantwoordelijkheid 3 op het Token interface;
- maatregelen die weliswaar door RFC 6819 worden gesuggereerd, maar niet worden overgenomen in het MedMij Afsprakenstelsel, omdat zij niet passen bij diens principes of bij andere verantwoordelijkheden in het stelsel;
- overige maatregelen, die alsnog getroffen dienen te worden door *DVP Server*, *OAuth Client* of *OAuth Authorization Server*.

8. Logging en portabiliteit

1.	*Dienstverlener persoon* zal het *Dossier* zo inrichten dat deze ook dienst kan doen als logbestand, zoals bedoeld in de AVG en NEN 7513:2018, van de door enige *Persoon* bij enige *Dienstverlener aanbieder* verzamelde persoonsgege-vens en door enige*Persoon* bij enige *Dienstverlener aanbieder* geplaatste persoonsgegevens. Met de logging wordt beoogd een betrouwbaar overzicht te kunnen leveren van de gebeurtenissen waarbij gezondheidsinformatie over een *Persoon* zijn verwerkt. Die gebeurtenissen kunnen zich over verschillende plaatsen en tijden uitstrekken. Het beoogde overzicht is dus alleen mogelijk als de loggegevens uit verschillende bronnen kunnen worden gecombineerd. Ook zonder direct een virtueel wereldwijd en levenslang patiëntdossier als doel te stellen is duidelijk dat gestandaardiseerde logging een voorwaarde is om het overzicht voor de betreffende *Persoon* mogelijk te maken. Op 18 mei 2018 is een revisie verschenen van de 2010-versie van NEN 7513. Deze norm, met het nummer NEN 7513:2018, is onderdeel van het Normenkader	core. logging. 100

	informatiebeveiliging van het MedMij Afsprakenstelsel. In hoofdstuk 5 van de gereviseerde norm staan de informatiebehoeften, zowel de algemene als die vanuit het specifieke perspectief van cliënten, zorginstellingen en toezichthouders. Hoofdstuk 6 vertaalt deze behoeften naar een overzicht van te loggen gebeurtenissen en hoofdstuk 7 biedt een model van de te loggen gegevens. De voorgaande versie (NEN 7513:2010) is ingetrokken. De term *NEN 7513* in het Besluit elektronische gegevensverwerking door zorgaanbieders wordt daarom geacht naar de 2018-versie te verwijzen.	
2.	De bewaartermijn van de logbestanden is ten minste 24 maanden en niet meer dan 36 maanden. Na de bewaartermijn van de logbestanden moeten deze vernietigd worden. Het maximum van de bewaartermijn is bepaald voor logging binnen de scope van MedMij-verkeer ter voorkoming van onnodige opslag van gegevens en ter bescherming van de privacy van de gebruiker. Deze minimale en maximale bewaartermijnen van logbestanden passen binnen de uitersten die daartoe door NEN7513 (paragraaf 8.5) zijn bepaald.	core.logging.101
4.	*Dienstverlener persoon* biedt *Persoon* de mogelijkheid om een *Portabiliteitsrapport* te verkrijgen. Daarmee kan *Persoon* geautomatiseerd een lijst exporteren, genaamd het *Portabiliteitsrapport,* van alle keren, gedurende een zekere periode, dat *Persoon* deze *Dienstverlener persoon* bij een *Aanbieder* gezondheidsinformatie volgens een zekere *Gegevensdienst* heeft verzameld.	core.logging.102
5.	*Dienstverlener persoon* biedt *Persoon* pro-actief de export van een *Portabiliteitsrapport* aan: • voordat *Dienstverlener persoon*, om welke reden dan ook, haar dienstverlening aan *Persoon* staakt; • voordat *Dienstverlener persoon* de logbestanden zou verwijderen waaruit zij *Portabiliteitsrapporten* voor *Persoon* over een zekere periode zou samenstellen.	core.logging.103
6.	*Dienstverlener persoon* beperkt *Persoon* niet in het gebruik van de *Portabiliteitsrapport* in de relatie van *Persoon* met mogelijke andere en/of latere *Dienstverlener persoon*.	core.logging.104
7.	Het *Portabiliteitsrapport* voldoet aan hetgeen daarover bepaald is in de Informatiemodellen en heeft de technische vorm van een XML-document, dat voldoet aan het XML-schema dat op de pagina XML-schema's te vinden is. Met het *Portabiliteitsrapport* krijgt *Persoon* een middel in handen om een belangrijk deel van de gezondheidsinformatie die hij in het *Dossier* in zijn PGO heeft verzameld, naar believen ook in andere PGO's onder te brengen (portabiliteit, overdraagbaarheid). Ook dat draagt bij aan de *Regie* van de *Persoon* over zijn gezondheidsinformatie, aan zijn voortdurend vrije keuze tussen *Dienstverlener persoon* (principe 7) en aan het beperken van het nadeel dat hij zou ondervinden wanneer zijn *Dienstverlener persoon* haar activiteiten zou staken. Er is geen garantie dat een *Portabiliteitsrapport* geautomatiseerd door een andere PGO dan die het rapport heeft gemaakt zou kunnen worden 'afgespeeld', al is het maar doordat niet alle gebruikte *Gegevensdiensten* nog als geldig in de *Catalogus* hoeven te staan. Het *Portabiliteitsrapport* geeft in dat soort gevallen nog steeds precieze en menselijkerwijs enigszins leesbare informatie waarmee de nieuwe PGO alsnog, desnoods, handmatig gevuld kan worden.	core.logging.105

	Dienstverlener persoon kunnen hun dienstverlening aan *Persoon* kracht bij zetten door een importfunctie voor *Portabiliteitsrapporten* aan te bieden. Dit is echter niet verplicht en moet gezien worden in het licht van principe 3. Een zwaarder middel voor portabiliteit zou een uitwisselstandaard tussen PGO's zijn. Dit zou echter een flinke complexiteit en kosten met zich meebrengen, niet in het minst doordat het rekening zou moeten houden met alle voormalige versies van het MedMij Afsprakenstelsel en met *Gegevensdiensten* die ondertussen niet meer als geldig in de *Catalogus* staan.	
8.	Bij het loggen van verzonden resource requests neemt de *OAuth Client* ook het `MedMij-Request-ID Header Field` op in het logbestand.	core.logging.200
9.	Bij het loggen van ontvangen resource requests neemt de *OAuth Resource Server* ook het `MedMij-Request-ID Header Field` op in het logbestand.	core.logging.201

8.1. Domain Name System

1.	*Dienstverleners persoon*, *Dienstverleners aanbieder* en *MedMij Beheer* zijn, in hun rol als DNS Server of cliënt daarvan, ervoor verantwoordelijk dat de name records behorende bij de hostnames van *Nodes* zijn ondertekend volgens DNSSEC.	core.dns.300
2.	Elke *Node*, in zijn rol als DNS resolver in het Domain Name System, controleert of de ontvangen name records zijn voorzien van ondertekening volgens DNSSEC en valideert deze volgens DNSSEC. Indien deze controle en validatie niet beide slagen, ziet hij af van verbinding met de betreffende hostname. Het gebruik van DNSSEC (RFC 4033, RFC 4034, RFC 4035) vermindert de kwetsbaarheid van het Domain Name System voor bijvoorbeeld DNS spoofing.	core.dns.301

8.2. TLS en certificaten

Onderstaande tabel vat samen hoe in de verantwoordelijkheden op deze laag de beveiligingsfuncties beveiliging, authenticatie en autorisatie worden ingericht. Het onderscheid, bij autorisatie, tussen inkomend en uitgaand verkeer is het gevolg van dat in deze twee gevallen de identificatie van de andere *Node* anders plaatsvindt.

	frontchannel-verkeer	**uitgaand backchannel-verkeer**	**inkomend backchannel-verkeer**
versleuteling volgens TLS	altijd		
identificatie op basis van ...	`redirect_uri` of *Aanbiederslijst*		PKIoverheid-certificaat
authenticatie, op basis van PKI-certificaat, van ...	alleen de TLS-server	TLS-client én TLS-server	
autorisatie op basis van controle tegen de *Whitelist*	niet	voorafgaand aan de TLS-handshake	zie verantwoordelijkheid core.whl.307

1.	Al het verkeer over het *MedMij-netwerk* is beveiligd en versleuteld met Transport Layer Security (TLS).	core.tls.300
2.	Er wordt gebruikgemaakt van TLS-versies en -algoritmen die zijn geclassificeerd als "goed" in de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS), versie 2.1 van het NCSC. Indien meerdere TLS-versies als "goed" geclassificeerd zijn, moet minimaal de laagste TLS-versie worden ondersteund. Hogere TLS-versies mogen worden aangeboden.	core.tls.301
3.	Van verantwoordelijkheid core.tls.301kan in het MedMij Afsprakenstelsel worden afgeweken, indien dit expliciet benoemd wordt in nadere eisen binnen de afsprakenset.	core.tls.302
4.	Gebruik van TLS False Start is verboden. Gebruik van TLS False Start is verboden om te voorkomen dat er inhoudelijke verwerking plaatsvindt van uitgewisselde gegevens voordat voor de betreffende uitwisseling authenticatie en autorisatie geslaagd zijn (zie onder).	core.tls.303
5.	Bij de TLS-handshake moet de hoogste toegestane TLS-versie gekozen worden die beide partijen ondersteunen.	core.tls.304
6.	Als invulling van core.tls.302 geldt, in afwijking van core.tls.301: • TLS 1.2 moet door elke deelnemer ondersteund worden. • TLS 1.3 moet door elke deelnemer ondersteund worden, indien redelijkerwijs mogelijk. **TLS 1.2** TLS 1.3 wordt in de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS), versie 2.1 van het NCSC als enige met "goed" geclassificeerd. Daarmee is dit de enige TLS-versie die volgens eis 1b ondersteund mag worden. Bij deze release van dit afsprakenstelsel kan TLS 1.3 niet door alle deelnemers ondersteund worden, omdat dit niet wordt aangeboden in door sommigen gebruikte componenten. Daarom maken we gebruik van de mogelijkheid die regel 1c biedt om een afwijkende regeling te treffen. De afwijkende regeling bestaat eruit dat TLS 1.3 door iedere deelnemer aangeboden moet worden, indien redelijkerwijs mogelijk. Om redenen van interoperabiliteit moet iedere deelnemer TLS 1.2 blijven ondersteunen. Het voornemen is deze afwijking te schrappen zodra TLS 1.3 breed ondersteund wordt, waardoor verantwoordelijkheid 1b weer onverkort geldt en TLS 1.3 de enige toegestane versie wordt. Dit kan al dan niet met behulp van een snel door te voeren patch op het MedMij Afsprakenstelsel.	core.tls.305
7.	Voor authenticatie en autorisatie bij backchannel-verkeer op het *MedMij-netwerk*, kunnen elke *PGO Node*, elke *ZA Node* en de *MedMij Stelselnode* een PKIoverheid-certificaat overleggen, en wel een G1-certificaat van een *PKIoverheid TSP*.	core.tls.314

- Private Root CA (per medio 2020 de standaard voor m2m)
  - Stamcertificaat
    - Staat der Nederlanden Private Root CA - G1
  - Domein Private Services, maar alleen de volgende:
    - Staat der Nederlanden Private Services CA - G1
    - KPN PKIoverheid Private Services CA - G1
    - QuoVadis PKIoverheid Private Services CA - G1
    - Digidentity BV PKIoverheid Private Services CA - G1

Uitzondering

Partijen die op 25-02-2022 al *Deelnemer* van MedMij waren en gebruikmaken van een publiek certificaat voor de beveiliging van hun backchannel-verkeer, kunnen dit certificaat tot uiterlijk 4 december 2022 gebruiken. Hierna is het gebruik van een privaat (G1) certificaat van *PKIoverheid* ook voor deze deelnemers verplicht voor de beveiliging van al het backchannel-verkeer en zal deze uitzondering verwijderd worden.

- Stamcertificaat
  - Staat der Nederlanden EV Root CA
- Intermediair Domein Server CA 2020
  - QuoVadis PKIoverheid Server CA 2020
  - Digidentity PKIoverheid Server CA 2020
  - KPN PKIoverheid Server CA 2020

8.	Voor authenticatie en autorisatie bij frontchannel-verkeer tussen productieomgevingen op het *MedMij-netwerk*, kunnen elke *PGO Node*, elke *ZA Node* en de *MedMij Stelselnode* een PKI-certificaat overleggen dat aan de volgende eisen voldoet: 1. De vereisten aan de certificaat leverancier voor PKI certificaten zijn: a. De meest up-to-date WebTrust audit is succesvol doorlopen en de certificering is geldig voor de 'Certificatie Authority' op iedere schakel in de keten van ondertekeningen tot en met de uitgifte processen. 2. De technische vereisten zijn: a. De 'private key' moet worden gegenereerd op het doelplatform waar het PKI certificaat wordt toegepast. b. Bij gebruik van publieke PKI certificaten is de toepassing van 'Certification Authority Authorization Resource Record' vereist. c. Het toepassen van DNSSEC op de gebruikte domeinen is vereist onder de voorwaarden van pas-toe-of-leg-uit. Strengere eisen kunnen worden gesteld vanuit aanvullende kaders, zoals aansluitvoorwaarden. d. Het gebruik van wildcard certificaten wordt niet toegestaan. e. Het gebruik van 'multi-domain'-certificaten is toegestaan, onder de voorwaarde dat de eigenaar van het certificaat gelijk is aan de eigenaar van alle domeinen die opgenomen zijn in de Subject Alt Name DNS waarden van het certificaat. 3. Uitgifte: a. Het zekerheidsuitgifte niveau moet minimaal op het OV-niveau (Organisation Validated) of met hogere zekerheid zijn uitgegeven voor publieke PKI webserver certificaten wanneer persoonsgegevens van bijzondere aard worden verwerkt. Dit is relevant voor de aanschaf van het certificaat en dit valt achteraf te controleren op het bestaan van Policy Object Identifiers (OIDs) die markeren welk type certificaat het betreft.	core.tls.315

b. De uitgever van de PKI certificaten is verantwoordingsplichtig aan de AVG en/of GDPR.

4. Beheer:
   a. Veilig beheer moet zijn toegepast zoals toegelicht in ‘Factsheet Veilig beheer van digitale certificaten’.

Uitzondering

Partijen die op 25-02-2022 al *Deelnemer* van MedMij waren en gebruikmaken van een publiek certificaat voor de beveiliging van hun frontchannel-verkeer, kunnen dit certificaat tot uiterlijk 4 december 2022 gebruiken. Hierna is het gebruik van publiek certificaat dat voldoet aan de hierboven genoemde eisen verplicht en zal deze uitzondering verwijderd worden.

- Stamcertificaat
  - Staat der Nederlanden EV Root CA
- Intermediair Domein Server CA 2020
  - QuoVadis PKIoverheid Server CA 2020
  - Digidentity PKIoverheid Server CA 2020
  - KPN PKIoverheid Server CA 2020

9.	Alle certificaathouders verbinden zich aan de op hen toepasselijke eisen van het PKI-stelsel waarvan zij een certificaat afnemen. Een organisatie mag meerdere certificaten hebben. Alle certificaathouders verbinden zich aan de op hen toepasselijke eisen van het PKI-stelsel waarvan zij een certificaat afnemen. Een organisatie mag meerdere certificaten hebben. De keuze voor de PKI-standaard past bij principe 19 van het MedMij Afsprakenstelsel. Er bestaan andere manieren voor, en ideeën over, het borgen van vertrouwen in een netwerk van geautomatiseerde systemen, maar deze zijn nog lang niet zo bewezen als PKI, dat wereldwijd wordt ondersteund, en wereldwijd is beproefd, door overheden en marktspelers. Bij gebruik van de PKI-standaard doet zich de vraag voor van welk(e) PKI-stelsel(s) gebruik gemaakt kan of moet worden. Zo'n PKI-stelsel voorziet in een hiërarchie van organisaties die certificaten uitgeven, zodanig dat de betrouwbaarheid van de certificaten van zo'n organisatie leunt op de betrouwbaarheid van de eerst-hogere organisatie in die hiërarchie, doordat de certificaten van de lagere-in-hiërarchie een handtekening hebben van die van de hogere-in-hiërarchie. Aan de top van zo'n hiërarchie staat een zogenoemde root Certificate Authority (root CA) die zijn betrouwbaarheid niet aan een hogere kan ontlenen, zijn eigen (stam)certificaten tekent, en zo een steunpilaar is van het vertrouwen in het hele betreffende PKI-stelsel. Het MedMij Afsprakenstelsel had ervoor kunnen kiezen een PKI-stelsel specifiek voor MedMij in te richten, maar de kosten daarvan, voor zichzelf en voor haar deelnemers, wegen niet op tegen de voordelen, onder de voorwaarde dat er een ander geschikt PKI-stelsel voorhanden is. Deelnemers zullen met hun services immers ook in andere afsprakenstelsels betrokken kunnen zijn dan dat van MedMij. Zo'n keuze past bovendien niet bij principe P6. Omdat het MedMij-netwerk een nationale en maatschappelijk kritische infrastructuur is, met hoge eisen aan betrouwbaarheid, kiest het MedMij Afsprakenstelsel voor de	core.tls.307

	beveiliging van al het backchannel-verkeer voor het momenteel enige PKI-stelsel waarin de betrouwbaarheid uiteindelijk steunt op een Nederlandse publiekrechtelijke rechtspersoon: PKIoverheid met de Staat der Nederlanden als root CA. Zo is de governance van de root CA transparant en toegankelijk belegd. Het MedMij Afsprakenstelsel bouwt ondermeer voor het door hem aan zijn deelnemers geboden vertrouwen dus mede op het PKIoverheid-stelsel, op het door dat stelsel vastgestelde programma van eisen voor de in dat stelsel betrokken TSP's en op de certificatiehiërarchie voor private G1 certificaten van PKIoverheid. Deelnemers in het MedMij Afsprakenstelsel zullen dus service-certificaten moeten betrekken bij een bij PKIoverheid aangesloten TSP die bij haar past.	
10.	Tijdens de handshake van TLS, wordt door de TLS-server in de `server hello`-stap aan de TLS-client: • in geval van backchannel-verkeer, altijd een verzoek om een certificaat gedaan. Indien de TLS-client daarop geen certificaat overlegt, wordt de handshake onmiddellijk afgebroken. • in geval van frontchannel-verkeer, nooit een verzoek om een certificaat gedaan. Bij backchannel-verkeer vindt dus twee-wegauthenticatie plaats, bij frontchannel-verkeer een-wegauthenticatie.	core.tls.308
11.	Alle *Backchannel Nodes* valideren tijdens de TLS-handshake bij backchannel-verkeer aan het begin van een TLS-sessie of het een PKIoverheid-certificaat is en controleren bij de *Certification Authority* of het ontvangen certificaat geldig is, op basis van CRL of OCSP. In geval van het falen van één van deze controles wordt het certificaat niet geaccepteerd en de TLS-sessie niet gestart.	core.tls.309
12.	In geval van het gebruik van OCSP in het kader van verantwoordelijkheid core.tls.309 mag de OCSP response vastgeniet zitten aan het certificaat (OCSP Stapling). Omdat het vastnieten van OCSP antwoorden (stapling) is toegestaan, zal iedere *Node* welke een certificaat moet controleren het vastnieten in zoverre moeten ondersteunen dat het alleen het feit dat er een vastgeniet OCSP antwoord gebruikt wordt niet mag leiden tot een foutmelding of het anderszins plots beëindigen van de TLS handshake of sessie. Het laten vastnieten van een OCSP-antwoord aan het certificaat is toegestaan in het Afsprakenstelsel MedMij. De ontvanger mag dit OCSP-antwoord gebruiken maar kan de controle of het certificaat ingetrokken is ook op een andere manier uitvoeren. Wanneer ervoor gekozen is om de controle alleen via OCSP uit te voeren kan het voorkomen dat een OCSP responder geen of niet tijdig een antwoord geeft. In dat geval kan ervoor gekozen worden om de TLS sessie toch op te zetten (soft-fail). Het primaire mechanisme binnen het MedMij Afsprakenstelsel om te bepalen of nodes elkaar mogen benaderen is de *Whitelist*-controle. Voor alle eisen gerelateerd aan PKIoverheid-certificaten, zie https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen.	core.tls.310
13.	Met inachtneming van verantwoordelijkheid core.tls.309, accepteren *Backchannel Nodes* PKIoverheid certficaten van elkaar door het stamcertificaat van de hiërarchie 'Staat der Nederlanden Private Root CA - G1', zoals gepubliceerd op https://cert.pkioverheid.nl/, te vertrouwen, zolang de geldigheidsdatum niet is verlopen en het stamcertificaat NIET is ingetrokken;	core.tls.311

	Uitzondering Tot 4 december 2022 moeten alle *Deelnemers* ook de certificaten uit de hiërarchie 'Staat der Nederlanden EV', zoals gepubliceerd op https://cert.pkioverheid.nl/, accepteren. Dit doen zij door ook van deze hiërarchie het stamcertificaat te vertrouwen. Na 4 december 2022 mag dit stamcertificaat niet meer vertrouwd worden.	
14.	PKI-certificaten moeten (in ieder geval op productie en acceptatie omgevingen) als complete keten inclusief alle intermediate certificaten worden verstuurd en gecontroleerd. Een certificaat keten bestaat uit het certificaat zelf, aangevuld met alle intermediate certificaten die worden meegeleverd door de CSP, de uitgevende instantie van het betreffende certificaat. Het root certificaat moet niet meegeleverd worden (dit is al aanwezig in de truststore van de tegenpartij).	core.tls.313

Interfaces, Core

1. Inleiding

Op deze pagina's staan de verantwoordelijkheden die horen bij de interfaces in het MedMij Afsprakenstelsel. In elke functie wordt gebruik gemaakt van één of meer van deze interfaces. Onderstaande tabel laat zien welke functies welke interface gebruiken.

hoofdfunctie	*Regie*			*Uitwisseling*	*Coördina*		
interface	**user interface**	**authorization interface**	**token interface**	**resource interface**	**GNL interface**	**OCL interface**	**int**
geboden door rol		***Authorization Server***		***Resource Server***			***MedMij Registra***
Opvragen Gegevensdienstnamenlijst					X		
Opvragen OAuth Client List						X	
Opvragen Aanbiederslijst							
Opvragen Whitelist							
Verzamelen	X	X	X	X			
Delen	X	X	X	X			

Verantwoordelijkheden over de adressering van deze interfaces komen hieronder aan de orde. Verantwoordelijkheden voor de specifieke interfaces zijn opgenomen in specifieke subpagina's, die klikbaar zijn in bovenstaande tabel.

2. Adressen en interfaces

Op de interfaces in de flows van Verzamelen en Delen adresseren Applicatie-rollen elkaar op basis van een URI. Onderstaande tabel geeft een overzicht.

hoofdfunctie	**interface**	**geadresseerde**	**bericht**	**kanaal**
Regie	authorization interface	*Authorization Endpoint* van de *Authorization Server*	authorization request	frontchannel
		OAuth Client (`redirect_uri`)	authorization response	
	token interface	*Token Endpoint* van de *Authorization Server*	access token request	backchannel
Uitwisseling	resource interface	*Resource Endpoint* van de *Resource Server*	resource request	

In de nu verantwoordelijkheden wordt bepaald hoe de URI's zijn opgebouwd waarmee de adresbepaler de adresgebruiker de geadresseerde laat adresseren, en hoe de parameters worden gevuld. De opbouw van het adres is steeds dezelfde, ook voor frontchannel en backchannel. Desondanks maken we in het logische

informatiemodel, in de *Aanbiederslijst*, wel onderscheid tussen *Frontchanneluri* en *Backchanneluri*. Dat houdt dat model wendbaarder, mocht er ooit wel adresseringsverschillen tussen frontchannel en backchannel ontstaan.

Interfaces lijsten

1	De *Aanbiederslijst* voldoet aan wat over haar is bepaald in de Informatiemodellen.	core. lijsten. 100
2.	De URI van de: • *Aanbiederslijst* is `https://stelselnode.medmij.nl/MedMij_Zorg aanbiederslijst.xml?api=1.5.1` • *OAuth Client List* is `https://stelselnode.medmij.nl /MedMij_OAuthclientlist.xml?api=1.5.1` • *Gegevensdienstnamenlijst* is `https://stelselnode.medmij.nl /MedMij_Gegevensdienstnamenlijst.xml?api=1.5.1` • *Whitelist* is `https://stelselnode.medmij.nl/MedMij_Whitelist.xml?api= 1.5.1` Versies worden van elkaar onderscheiden door een query-parameter in de URI. Vanaf release 1.1.2 van het MedMij Afsprakenstelsel hebben de lijst-interfaces een versienummer. Dat maakt het mogelijk om meerdere versies van deze interfaces tegelijkertijd in productie te hebben. De versies worden, vanaf release 1.1.2, van elkaar onderscheiden door een query-parameter in de URI. Het versienummer is identiek aan dat van de betreffende release. Opeenvolgende versies van de lijst-interfaces kunnen daarom inhoudelijk identiek zijn. bijvoorbeeld: `https://stelselnode.medmij.nl/MedMij_Whitelist.xml?api=1. 1.2`	core. lijsten. 300
3.	Het aandeel van *MedMij Registratie* in elk van de implementaties van de functies *Opvragen Aanbiederslijst*, *Opvragen OAuth Client List*, *Opvragen Gegevensdienstnamenlijst* en *Opvragen Whitelist* is voor minstens 99,9% van de tijd beschikbaar. *MedMij Beheer* laat, na het niet beschikbaar raken van bedoelde aandeel, maximaal acht uren (480 minuten) verstrijken voordat het weer beschikbaar is.	core. lijsten. 301
4.	*MedMij Beheer* brengt, in geval van zo'n incident, *Deelnemers* op de hoogte van het optreden van het incident en van de verwachte down-time. *MedMij Beheer* brengt *Deelnemers* op de hoogte van gepland onderhoud dat leidt tot tijdelijke onbeschikbaarheid.	core. lijsten. 302
5.	Ingeval *MedMij Registratie* in de functies *Opvragen Aanbiederslijst*, *Opvragen OAuth Client List*, *Opvragen Gegevensdienstnamenlijst* en/*of* *Opvragen Whitelist* onbeschikbaar is, mogen betreffende opvragers gedurende maximaal 10 uur gebruik maken van het meest recente exemplaar van de betreffende lijst in de cache. De *Whitelist* is niet bedoeld voor het blokkeren van gecompromitteerde nodes. In die gevallen moet het betreffende certificaat worden ingetrokken, de systemen opgeschoond en een nieuw certificaat worden geïnstalleerd. Daarom is, in geval van de in deze verantwoordelijkheid bedoelde down-time, het gaan achterlopen van de inhoud van de *Whitelist*, geen beveiligingsrisico.	core. lijsten. 303

User interface (Autorisatieserver)

Het user interface hoort bij de hoofdfunctie *Regie*.

`NaamAanbieder`, `NaamGegevensdienst` en `NaamLeverancierPGO` zijn placeholders, zoals opgenomen in de Toestemmingsverklaring en de Bevestigingsverklaring.

1.	Het welkomstscherm dat aan de *Persoon* wordt gepresenteerd bij ontvangst op de Autorisatieserver in de functies Verzamelen en Delen staat gespecificeerd op de pagina Landingspagina. Daarbij geldt dat: • de gebruikersvriendelijke weergave van de identiteit van de *Aanbieder* (`NaamAanbieder`) wordt bepaald door de betreffende *Dienstverlener aanbieder*, in haar dienstverleningsrelatie met de betreffende *Aanbieder*;	core.usrint.100
2.	Het Annuleringsscherm, dat aan de *Persoon* wordt gepresenteerd na afbreken van de authenticatie in de functies Verzamelen en Delen staat gespecificeerd op de pagina Annuleringspagina. Daarbij geldt dat: • de gebruikersvriendelijke weergave van de identiteit van de *Aanbieder* (`NaamAanbieder`) wordt bepaald door de betreffende *Dienstverlener aanbieder*, in haar dienstverleningsrelatie met de betreffende *Aanbieder*;	core.usrint.101
2a.	De vraag die aan de *Persoon* gesteld moet worden om toestemming te verlenen aan de *Aanbieder* in de functie Verzamelen staat gespecificeerd op de pagina Toestemmingsverklaring. Daarbij geldt dat: • de gebruikersvriendelijke weergave van de identiteit van de *Aanbieder* (`NaamAanbieder`) wordt bepaald door de betreffende *Dienstverlener aanbieder*, in haar dienstverleningsrelatie met de betreffende *Aanbieder*; • de gebruikersvriendelijke weergave van een *Gegevensdienst* (`NaamGegevensdienst`) wordt betrokken uit de *Gegevensdienstnamenlijst;* • de gebruikersvriendelijke weergave van de identiteit van de *Dienstverlener persoon* (`NaamLeverancierPGO`) wordt betrokken uit de *OAuth Client List*.	core.usrint.102
2b.	De vraag die aan de *Persoon* gesteld moet worden in de stap "bevestig" in de functie Delen staat gespecificeerd op de pagina Bevestigingsverklaring. Daarbij geldt dat: • de gebruikersvriendelijke weergave van de identiteit van de *Aanbieder* (`NaamAanbieder`) wordt bepaald door de betreffende *Dienstverlener aanbieder*, in haar dienstverleningsrelatie met de betreffende *Aanbieder*; • de gebruikersvriendelijke weergave van een *Gegevensdienst* (`NaamGegevensdienst`) wordt betrokken uit de *Gegevensdienstnamenlijst;* • de gebruikersvriendelijke weergave van de identiteit van de *Dienstverlener persoon* (`NaamLeverancierPGO`) wordt betrokken uit de *OAuth Client List*.	core.usrint.103

Authorization interface

De authorization interface hoort bij de hoofdfunctie *Regie*.

Op deze pagina staan alleen de verantwoordelijkheden inzake de authorization interface die nog niet genoemd staan in de OAuth 2-specificatie.

1. De parameters in de authorization request worden als volgt gevuld:

parameter	vulling	toelichting
`response_type`	letterlijke waarde `code`	Dit is het gevolg van verantwoordelijkheid (
`client_id`	de hostname, die in de *OAuth Client List* is opgenomen, van de *Node* van de *OAuth Client* die de authorization request doet	
`redirect_uri`	1. zodanig dat de erin opgenomen hostname gelijk is aan de `client_id` en er geen poortnummer is opgenomen 2. de `redirect_uri` moet volledig zijn en verwijzen naar een `https`-beschermd endpoint 3. de redirect_uri moet urlencoded zijn (conform RFC 3986)	Zie verantwoordelijkheden core.adresserin adressering.201 en core.adressering.202. De tweede eis is een maatregel tegen bev , 4.2.4, 4.4.1.1, 4.4.1.5 en 4.4.1.6 in RFC 6 Token interface, de toelichting onder veran
`scope`	Voor "verzamelen": • één of meerdere, door een enkele spatie van elkaar gescheiden, aanbieder-gegevensdienst-combinaties, waarbij de *Aanbiedernaam* telkens dezelfde moet zijn. Voor "delen": • één aanbieder-gegevensdienst-combinatie. Een aanbieder-gegevensdienst-combinatie bestaat uit: • één *Aanbiedernaam*, ontdaan van de suffix `@medmij` • gevolgd door een tilde (~)	Er worden geen andere scopes of onderde opgenomen dan de genoemde. Voorbeelden van syntactisch juiste scopes • `"eenofanderezorgaanbieder~42"` afnemen van *Gegevensdienst* 42 bij `eenofanderezorgaanbieder@medm` • `"eenofanderezorgaanbieder~42 eenofanderezorgaanbieder~48"`, afnemen van *Gegevensdiensten* 42 e `eenofanderezorgaanbieder@medm`

		• gevolgd door één *GegevensdienstId* van een *Gegevensdienst* uit de *Gegevensdienstnamenlijst.*	
	`state`	1. conform sectie 4.1.1. van RFC 6749.	Hiermee geeft de *OAuth Client* informatie r *Authorization Server*, waaraan eerstgenoe redirect, kan afleiden bij welk verzoek de a hoort. Deze informatie is verder betekenisl *Authorization Server*. De state MOET • een minimale lengte hebben van 128 k lang om niet raadbaar te zijn). • een maximale lengte hebben van 512 l grens, rekening houdend met standaar maximale lengte uri's).

Conform de OAuth 2- specificatie moeten overige parameters die meegestuurd worden in het request ger

2. De *OAuth Client* zorgt ervoor dat voor het authorization request de http-methode `GET` wordt gebruikt, niet

   In de OAuth-specificatie, sectie 3.1 wordt de *OAuth Authorization Server* verplicht gesteld `GET` te acce optioneel gehouden. Omdat `GET` de verreweg meest in het MedMij Afsprakenstelsel passende http-me authorization request, geldt, om de *OAuth Authorization Server* niet voor onnodige implementatiekoste verantwoordelijkheid. Hoewel deze verantwoordelijkheid een verantwoordelijkheid van de *OAuth Clien* onder de verantwoordelijkheid van een MedMij-deelnemer valt, wordt de request uiteindelijk door de *U*

3. Na ontvangst van een authorization request verifieert de *Authorization Server* dat:

   • de betreffende `client_id` voorkomt op de *OAuth Client List*;
   • de `redirect_uri` geldig is en voorkomt bij de betreffende `client_id` op de *OAuth Client List.*

   Als een van deze verificaties niet slaagt dan behandelt de *Authorization Server* dit als uitzondering 1a volg verantwoordelijkheid core.authint.207.

4. Vervolgens verifieert de *Authorization Server* dat:

   • alle gevraagde *GegevensdienstId's* voorkomen op de *OAuth Client List,* bij de betreffende `client_i` gehanteerde *Interfaceversie*;
   • zij namens deze *Aanbieder*, voor de gehanteerde *Interfaceversie*, deze *Gegevensdienst(en)* ontsluit, i met de gepubliceerde *Aanbiederslijst*;
   • indien in de scope meerdere *GegevensdienstId's* zijn opgenomen:
     • alle *Gegevensdiensten* betrekking hebben op de functie *Verzamelen*;
     • de hostnames van de *AuthorizationEndpoints*, waarop de *Gegevensdiensten* worden aangeboden overeenkomen;
     • de hostnames van de *TokenEndpoints*, waarop de *Gegevensdiensten* worden aangeboden, met e

   Als een van deze verificaties niet slaagt dan behandelt de *Authorization Server* dit als uitzondering 1b volg verantwoordelijkheid core.authint.207.

   Zo voorkomt de *Authorization Server* dat gevolg wordt gegeven aan een verzoek dat blijkens de *OAutl Aanbiederslijst* niet is toegestaan.

5. Tijdens de afhandeling van een authorization request laat de *Authorization Server,* in zijn rol als *Authoriza* de *Persoon* om OAuth-autorisatie vraagt, de *Persoon* authenticeren door de *Authentication Server*.

   Conform stroomdiagram onder 1. De *Aanbieder* in het Aanbiedersdomein, en dus BSN-domein, is verp verstrekken van gegevens vanuit een gezondheidsdossier de identiteit van de persoon te verifiëren aa BSN.

   Het MedMij Afsprakenstelsel brengt het gebruik van de *Authentication Server* onder in de OAuth-flow, verantwoordelijkheid van de *Authorization Server*. Laatstgenoemde handelt in dezen onder verantwoo individuele *Aanbieders*, want die zijn het waarvoor de *Persoon* zich authenticeert.

   De directe interactie van de *Persoon* met de *Authorization Server* is bedoeld om de *DVP Server* te aut *Resource Server* aan te spreken. Die levert de uiteindelijke *Gegevensdienst* pas.

6. Onmiddellijk na authenticatie van de *Persoon*, zoals bedoeld in verantwoordelijkheid core.authint.204, en slaagt, vraagt de *OAuth Authorization Server* de *Persoon* om een *Toestemmingsverklaring* (in het geval v een *Bevestigingsverklaring* (in het geval van *Delen*), volgens het daaromtrent bepaalde op de pagina Use (Autorisatieserver), volgens de standaard OAuth 2.0, op de wijze waarop deze in het MedMij Afsprakenste

7. Voorafgaand aan uitgifte van een authorization code via de in de authorization request opgenomen `redi` administreert de *OAuth Authorization Server* die authorization code en de daarvoor gebruikte `redirect_`

   Dit is een maatregel tegen beveiligingsrisico's 4.4.1.3, 4.4.1.5 en 4.4.1.7 uit RFC 6819 (zie verantwoor beveiliging.205). Zie ook verantwoordelijkheid core.tknint.206.

8. *Authorization Server* en *DVP Server* behandelen uitzonderingssituaties inzake het authorization interface onderstaande tabel.

Nummer	Implementeert uitzonderingen	Uitzondering	Actie	Melding
Authorization interface 1a	Verzamelen 1 Delen 1	*Authorization Server ontvangt een authorization request zonder (geldige)* `redirect_uri` *en/of zonder een (geldige)* `client_id`*.*	*Authorization Server* informeert *User Agent* over deze uitzondering. *Authorization Server* voert geen redirect naar de *Client* uit, ook niet met een foutmelding.	conform OAu 2.0-specificati par. 4.1.2.1
Authorization interface 1b		*Authorization Server* ontvangt een ongeldige authorization request, anders dan uitzondering 1.	*Authorization Server* informeert *DVP Server* over deze uitzondering. *DVP Server*	conform OAu 2.0-specificati par. 4.1.2.1, n de daar genoemde, zo specifiek mogelijke, toepasselijke error code

			informeert *Persoon* daarover.	
Authorization interface 2	Verzamelen 2 Delen 2	*Authorization Server* kan de identiteit van de *Persoon* niet vaststellen.	*Authorization Server* informeert *DVP Server* over deze uitzondering. *DVP Server* informeert *Persoon* dat diens verzoek geen voortgang kan vinden, maar laat de oorzaak daarvan helemaal in het midden.	conform OAut 2.0-specificati par. 4.1.2.1, e code `access denied`, met de error description "`Access denied.`"
Authorization interface 3	Verzamelen 3 Delen 3	*Authorization Server* stelt tijdens de afhandeling van de authorization request vast dat: • in geval van de functie *Verzamelen*: van *Persoon* bij *Aanbieder* voor geen van de gevraagde *Gegevensdiensten* gezondheidsinformatie beschikbaar is; • in geval van de functie *Delen*: *Aanbieder* niet ontvankelijk is voor die *Gegevensdienst* van *Persoon;* Zie de toelichting op Beschikbaarheids- en ontvankelijkheidsvoorwaarde .		
Authorization interface 4	Verzamelen 4 Delen 4	De autorisatievraag wordt ontkennend beantwoord.		
Authorization interface 5	Verzamelen 5 Delen 5	*Authorization Server* kan de autorisatie niet vaststellen.	*Authorization Server* informeert *DVP Server* over deze uitzondering. *DVP Server* informeert daarop *Persoon* hierover.	conform OAut 2.0-specificati par. 4.1.2.1, e code `access denied`, met de error description "`Authorizat failed.`"

De uitzonderingssituaties kunnen gezien worden als de implementatie-tegenhangers van de uitzonde Verzamelen en Delen. Op de Applicatielaag zijn deze echter per interface geordend. Alle uitzonderinge *Authorization Server* ontdekt. In deze versie van het MedMij Afsprakenstelsel is bepaald dat zij altijd le mogelijk afbreken van de flow door alle betrokken rollen. Daartoe moeten echter eerst nog de andere worden. Om te voorkomen dat de *DVP Server* informatie over het bestaan van behandelrelaties verkrij daarvoor (al) toestemming is gegeven, moet het onderscheid tussen de uitzonderingen 2, 3 en 4 niet t *DVP Server*.

Deze tabel bevat alleen die uitzonderingssituaties ten aanzien waarvan het MedMij afsprakenstelsel ei
de implementatie. In de specificatie van OAuth 2.0 staan daarnaast nog generiekere uitzonderingssitu
waarin de redirect URI ongeldig blijkt. Ook deze uitzonderingssituaties moeten geïmplementeerd word

Token interface

Op deze pagina staan alleen de verantwoordelijkheden inzake het token interface die nog niet genoemd staan in de OAuth 2-specificatie.

1. De parameters in de access token request worden als volgt gevuld: core.tknint.200

parameter	vulling	toelichting
`grant_type`	conform verantwoordelijkheid core.autorisatie.205, core.autorisatie.206, core.autorisatie.207 en core.autorisatie.208	Dit is het gevolg van verantwoordelijkheid core.autorisatie.201.
`code`	conform verantwoordelijkheid core.autorisatie.205, core.autorisatie.206, core.autorisatie.207 en core.autorisatie.208	Zie de toelichting bij verantwoordelijkheid core.autorisatie.205, core.autorisatie.206, core.autorisatie.207 en core.autorisatie.208.
`client_id`	de hostname van de *Node* van de *OAuth Client* die de authorization request deed die de nu aangeboden authorization code opleverde	Het gebruik van client_id is verplicht. Conform de verantwoordelijkheden als beschreven in het hoofdstuk TLS en certificaten moet al het netwerk-verkeer beveiligd worden met TLS. In hoofdstuk 2 van RFC8705 staat beschreven aan welke eisen voldaan moet worden bij een combinatie van OAuth2 en mutual TLS.
`redirect_uri`	dezelfde waarde als in de voorafgaande authorization request. De redirect_uri moet urlencoded zijn (conform RFC 3986).	NB: De redirect_uri MOET NIET dubbel encoded worden(!)

Conform de OAuth 2- specificatie moeten overige parameters die meegestuurd worden in het request genegeerd worden.

2. De parameters in de access token response worden als volgt gevuld: core.tknint.201

parameter	vulling	toelichting
`access_token`	Het hiermee uitgegeven access token.	
`token_type`	letterlijke waarde `"Bearer"`	
`expires_in`	900	Conform verantwoordelijkheid core.autorisatie.204

	`refresh_token`	**niet gebruikt**	Conform verantwoordelijkheid core.autorisatie.204	
	`scope`	Conform sectie 5.1 van de OAuth 2.0-specificatie . In toevoeging daarop: verplicht indien het authorization request verzocht om *Verzamelen* van meerdere *Gegevensdiensten* en hiervan niet alle *Gegevensdiensten* beschikbaar bleken voor *Persoon*. In dat geval is de `scope`-parameter gelijk aan die in de betreffende authorization request, met daaruit weggelaten de niet-beschikbare aanbieder-gegevensdienst-combinaties.		
3.	De *OAuth Client* biedt een, via de in de *authorization request* opgenomen `redirect_uri` ontvangen authorization code, slechts aan de *Authorization Server* aan indien: • de waarde van de, in de authorization response ontvangen, state overeenkomt met de door de *OAuth Client* zelf gegenereerde state, die werd verzonden in het authorization request.			core.tknint.202
4.	De *OAuth Client* biedt een zekere authorization code maximaal eenmaal aan aan de *Authorization Server*.			core.tknint.203
5.	De *Authorization Server* voert een authorization code af, wanneer het eenmaal door een *OAuth Client* is aangeboden. Dit is een maatregel tegen beveiligingsrisico 4.1.1 uit RFC 6819 (zie toelichting bij verantwoordelijkheden core.beveiliging.202, core.beveiliging.203, core.beveiliging.204). Het afvoeren van een authorization code houdt in dat de *Authorization Server* van een eenmaal uitgegeven authorization code bijhoudt of die al eens gebruikt is voor het verkrijgen van een access token. Mocht een authorization code voor een tweede of volgende keer worden aangeboden ter verkrijging van een access token, dan zal de *Authorization Server* dat weigeren en de flow afbreken. Als de *Client* aan wie die geweigerd wordt te kwader trouw was, is hiermee een gevaar afgewend. Was hij wel te goeder trouw en handelde hij conform het MedMij Afsprakenstelsel, dan was hij niet degene die al eerder dezelfde authorization code aanbood en blijkt er dus sprake geweest te zijn van een security breach.			core.tknint.204
6.	De *OAuth Authorization Server* draagt geen access token over als in de token request geen `redirect_uri` is opgenomen, en evenmin als er in de token request wel een `redirect_uri` is opgenomen, maar deze niet identiek is aan de `redirect_uri` die de *OAuth Authorization Server*, bij uitreiking, verbonden heeft aan de authorization code die in de token request wordt aangeboden. Dit is een maatregel tegen beveiligingsrisico's 4.4.1.3, 4.4.1.5 en 4.4.1.7 uit RFC 6819 (zie verantwoordelijkheid core.beveiliging.205). Met het oog op de parameters client_id en redirect_uri in de authorization request en de access token request geldt dat:			core.tknint.205

- de client_id in de authorization request overeen moet komen met de hostname van de redirect_uri in diezelfde authorization request (verantwoordelijkheid 1 bij Authorization interface);
- de redirect_uri in de access token request overeen moet komen met de redirect_uri in de authorization request (deze verantwoordelijkheid).

In de access token request speelt de redirect_uri dan niet de rol van adressering van de response, zoals in de authorization request wel, maar enkel als terugverwijzing naar de redirect_uri van het Authorization interface. Bij de afhandeling van het Token interface wordt helemaal niet geredirect; die speelt zich geheel op het backchannel af.

7.	Na ontvangst van een access token request, in de functies *Verzamelen* of *Delen*, zal de *OAuth Authorization Server*, indien in antwoord daarop een access token dient te worden uitgegeven, na maximaal tien (10) seconden dit acces token ter beschikking stellen aan de *OAuth Client*. Dit gedrag van de *OAuth Authorization Server* is gedurende minimaal 99,5% van de tijd beschikbaar.	core.tknint.206
8.	*OAuth Authorization Server* en *OAuth Client* behandelen uitzonderingssituaties inzake het token interface volgens onderstaande tabel.	core.tknint.207

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Vervolg
Token interface 1	Verzamelen 6 Delen 6	*Authorization Server* moet vanwege één van de in de OAuth 2.0-specificatie, par. 5.2, genoemde redenen de token request weigeren.	*Authorization Server* informeert *DVP Server* over deze uitzondering. *DVP Server* informeert daarop *Persoon* hierover.	met de conform OAuth 2.0-specificatie, par. 5.2, toepasselijke error code	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

De uitzonderingssituaties kunnen gezien worden als de implementatie-tegenhangers van de uitzonderingen van de functies Verzamelen en de Delen. Op de Applicatielaag zijn deze echter per interface geordend. Alle uitzonderingen worden door de *Authorization Server* ontdekt. In deze versie van het MedMij Afsprakenstelsel is bepaald dat zij altijd leiden tot het zo snel mogelijk afbreken van de flow door alle betrokken rollen. Daartoe moeten echter eerst nog de andere rollen geïnformeerd worden.

Deze tabel bevat alleen die uitzonderingssituaties ten aanzien waarvan het MedMij afsprakenstelsel eigen eisen stelt aan de implementatie. In de specificatie van OAuth 2.0 staan daarnaast nog generiekere uitzonderingssituaties, zoals de situatie waarin de redirect URI ongeldig blijkt. Ook deze uitzonderingssituaties moeten geïmplementeerd worden.

Resource interface

Het resource interface hoort bij de hoofdfunctie *Uitwisseling*.

Op deze pagina staan alleen de verantwoordelijkheden inzake het resource interface die nog niet genoemd staan in:

- de OAuth 2-specificatie;
- de informatiestandaard van de *Gegevensdienst* die op het resource interface wordt aangesproken.

1. De *OAuth Client* gebruikt voor het sturen van het acces token, in de resource request, de methode `Autho` `Request Header Field`, zoals beschreven in sectie 2.1 van RFC6750.

   De methode `Authorization Request Header Field` biedt de beste beveiliging.

2. De *OAuth Client* voegt bij het versturen van een resource request een `HTTP Header Field` toe met de `Request-ID`. Het `MedMij-Request-ID` moet een willekeurige waarde bevatten en dient uniek te zijn bi netwerk. Het kan een integer waarde zijn, of een UUID, maar kan ook volgens een ander geldig identificat gevuld.

3. Na ontvangst van een resource request, in de functies *Verzamelen* of *Delen*, zal de *Resource Server*, indi daarop een resource response dient te worden gedaan, na maximaal zestig (60) seconden dit resource re beschikking stellen aan de *DVP Server*. Dit gedrag van de *Resource Server* is gedurende minimaal 98,5% beschikbaar.

4. Voor zover er in het verkeer tussen *DVP Server* en *Resource Server* in de implementaties van de functies *Delen* sprake is, in de stuurgegevens, van een gegevenselement dat tot de identiteit van de *Persoon* herle gebruiken zij daarvoor niets anders dan de OAuth-gegevens die zij in hun respectievelijke *OAuth Client* en *Server* moeten uitwisselen. *DVP Server*, *Authorization Server* en *Resource Server* treffen goed beveiligde waarmee zij hieruit waar nodig zelf de identiteit van de *Persoon* kunnen vaststellen.

   Met het oog op het borgen van de privacy en het zo eenvoudig mogelijk houden van de architectuur va Afsprakenstelsel, wordt ervoor gekozen de identifier voor de *Persoon* onderweg zo betekenisloos mog Alle betekenis wordt er ter weerszijden aan verbonden door raadpleging van interne registraties. Omda *Authorization Server* en *Resource Server* samen een OAuth-flow afhandelen, beschikken zij (na authe *Persoon*) over tokens die de identiteit van de *Persoon* vertegenwoordigen, namelijk (eerst) de authoriz (later) het access token. Buiten deze hoeft en zal er geen identificerende gegevenselementen in het ve opgenomen. Het FHIR-gegevenselement *PatientID* wordt *niet* gebruikt.

5. *OAuth Resource Server* en *OAuth Client* handelen uitzonderingssituaties inzake het resource interface af onderstaande tabel. De *Resource Server* dient de status code uit de tabel te retourneren in combinatie me melding zoals gespecificeerd in de gebruikte informatiestandaard (indien van toepassing).

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding
Resource interface 1	Verzamelen 6 Delen 6	Het resource request bevat geen access_token.	*Resource Server* informeert *DVP Server* over deze uitzondering.	Een Status-Code 401 conform HTTP specificatie. In deze situatie retourneert de *Resource Server* uitdrukkelijk géén nadere informatie over de opgetreden uitzondering.

Resource interface 2	De *Resource Server* detecteert dat het meegezonden access_token is verlopen of om een andere reden niet geldig is.	Een Status-Code 401 conform HTTP specificatie en een `WWW-Authenticate` HTTP response header met als auth-scheme "`Bearer`" en een `error` attribuut met waarde "`invalid_token`". conform RFC 6750.
Resource interface 3	De *Resource Server* detecteert dat de scope die is verbonden aan het meegezonden access_token niet toereikend voor de uitvoering van het resource request.	Een Status-Code 403 conform HTTP specificatie en een `WWW-Authenticate` HTTP response header met als auth-scheme "`Bearer`" en een `error` attribuut met waarde "`insufficient_scope`". conform RFC 6750.
Resource interface 4	Het resource request mist een vereiste (header) parameter, bevat een niet-ondersteunde (header) parameter of parameterwaarde, gebruikt meer dan één methode voor het doorgeven van een access_token, of is op een andere wijze misvormd.	Een `Status-Code` 400 conform HTTP specificatie en een `WWW-Authenticate` HTTP response header met als auth-scheme "`Bearer`" en een `error` attribuut met waarde "`invalid_request`". conform RFC 6750.
Resource interface 5	De *Resource Server* detecteert dat niet kan worden voldaan aan de beschikbaarheidsvoorwaarde. Zie ook de toelichting op Beschikbaarheids- en ontvankelijkheidsvoorwaarde.	Een Status-Code 403 conform HTTP specificatie en een `WWW-Authenticate` HTTP response header met als auth-scheme "`Bearer`" en een `error` attribuut met waarde "`access_denied`". conform RFC 6750. Het vereiste error attribuut is bewust in lijn gebracht met het gedrag van de *Authorization Server* bij deze uitzonderingssituatie.

Resource interface 6		*Resource Server* kan in de request niet, niet geheel of niet tijdig voorzien, om redenen anders dan in bovengenoemde uitzonderingen.		Een toepasselijke Status-Code conform HTTP specificatie.

MedMij Extensies

1. Inleiding

Alle in de MedMij Core beschreven onderwerpen vormen de essentie van het MedMij afsprakenstelsel. Deze onderwerpen zijn noodzakelijk om de *Persoon* in de regie te stellen over de eigen gezondheidsgegevens. Extensies vormen een uitbreiding van functionaliteiten, waarmee de regie van de gebruiker uitgebouwd.

2. Gegevensuitwisseling

In de MedMij Core staan de functies *Verzamelen* en *Delen* beschreven. Hiernaast kent het afsprakenstelsel nog twee functies, die nauw aan elkaar gelinkt zijn. Het gaat om *Abonneren* en *Notificeren*. Daar waar *Verzamelen* en *Delen* tot de essentie behoren van het in de regie plaatsen van de *Persoon*, vormen *Abonneren* en *Notificeren* een uitbreiding op deze functionaliteiten.

3. Vertegenwoordiging

Een vertegenwoordiging houdt in dat de ene persoon (de *Vertegenwoordigde*) zich laat vertegenwoordigen door een andere persoon (de *Vertegenwoordiger*). Met de juiste machtigingen mag een Vertegenwoordiger rechtshandelingen uitvoeren namens de Vertegenwoordigde. Zonder machtiging kan vertegenwoordiging niet plaatsvinden. Binnen het huidige afsprakenstelsel van MedMij betekent dit dat machtigingen gegeven kunnen worden voor het uitvoeren van de functie *Verzamelen*.

Iemand kan op basis van een wettelijke grondslag zijn gemachtigd, zoals gezaghebbende ouder(s) of voogd voor kinderen onder de 12 jaar of op basis van een vrijwillig afgegeven machtiging. Het gebruik van vrijwillig afgegeven machtigingen is bijvoorbeeld noodzakelijk om mantelzorgers hun taak goed uit te kunnen laten voeren in de langdurige zorg.

In deze versie van het afsprakenstelsel richt *Vertegenwoordiging* zich alleen op de functie Verzamelen en alleen voor vrijwillige vertegenwoordiging. De *Vertegenwoordigde* machtigt de *Vertegenwoordiger* voor het verzamelen van alle gezondheidsgegevens die op *Vertegenwoordigde* van toepassing zijn.

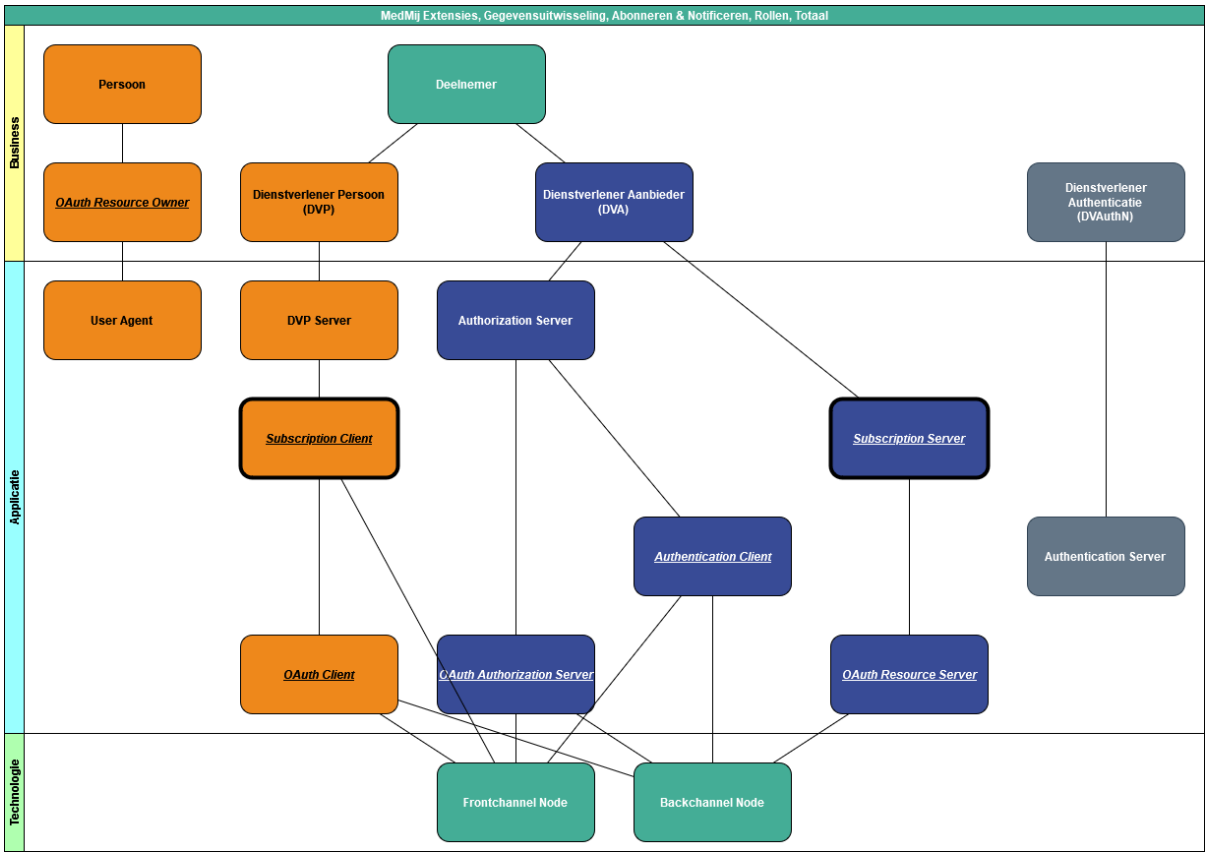
Extensie Abonneren

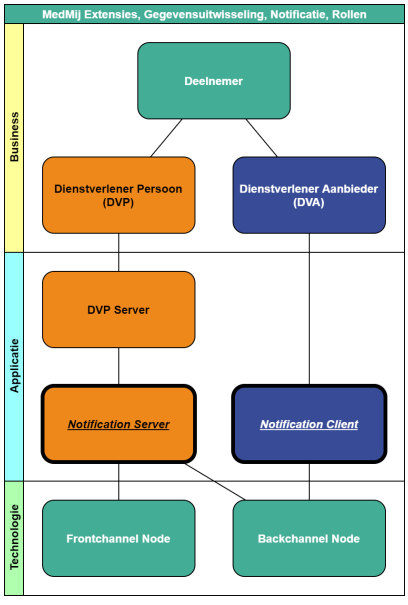
1. Inleiding

In de MedMij Core staan de functies *Verzamelen* en *Delen* beschreven. Hiernaast kent het afsprakenstelsel nog twee functies, die nauw aan elkaar gelinkt zijn. Het gaat om *Abonneren* en *Notificeren*. Daar waar *Verzamelen* en *Delen* tot de essentie behoren van het in de regie plaatsen van de *Persoon*, vormen *Abonneren* en *Notificeren* een uitbreiding op deze functionaliteiten.

2. Rollen

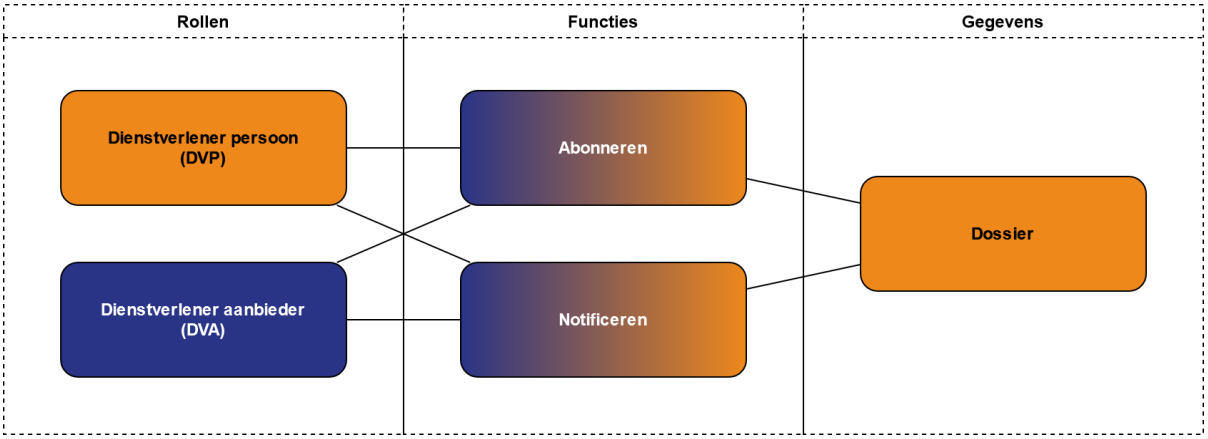
De MedMij Core beschrijft rol *Resource Server*. Nauw gerelateerd aan deze rol beschrijft deze extensie de rollen *Subscription Server*, *Subscription Client*, *Notification Server* en *Notification Client*.





3. Functies en gegevens

Onderstaand diagram toont de functies die vanuit deze extensie worden aangeboden, welke rollen verantwoordelijk zijn voor het leveren van deze functies en welke gegevens door de functie geleverd worden.



Dit diagram toont alleen de verantwoordelijke rol, behorende bij een aangeboden functie. De rollen die de functie gebruiken worden benoemd in de uitwerking van de functie, bijvoorbeeld in een stroomdiagram.

Dienstverlener aanbieder biedt aan *Dienstverlener persoon* twee functies, namelijk

- *Abonneren*
- *Notificeren*

4. Verantwoordelijkheden

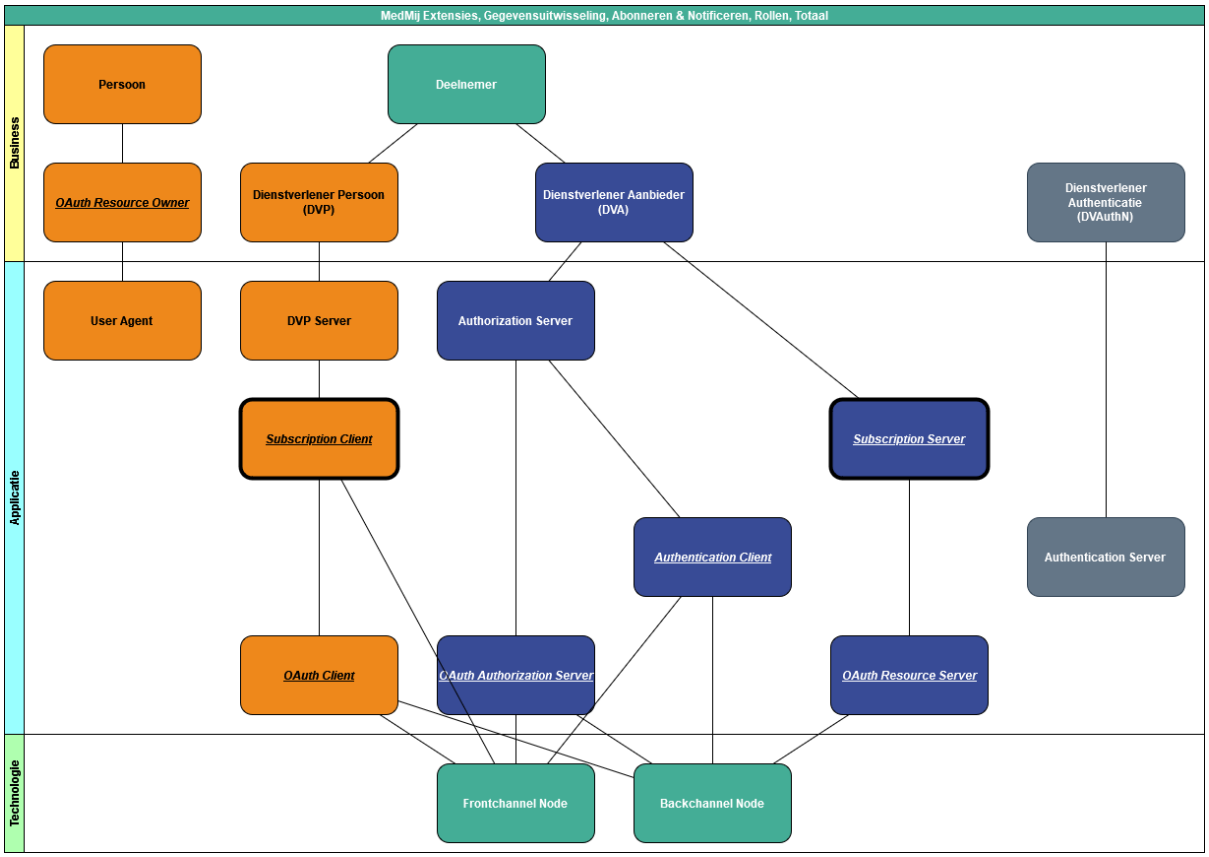
De verantwoordelijkheden die in de MedMij Core staan beschreven, zijn ook van toepassing op deze extensie. Daarnaast gelden de hieronder (vervangende) verantwoordelijkheden. Net als in de MedMij Core zijn de volgende kleuren voor de verantwoordelijkheden op de verschillende lagen gebruikt:

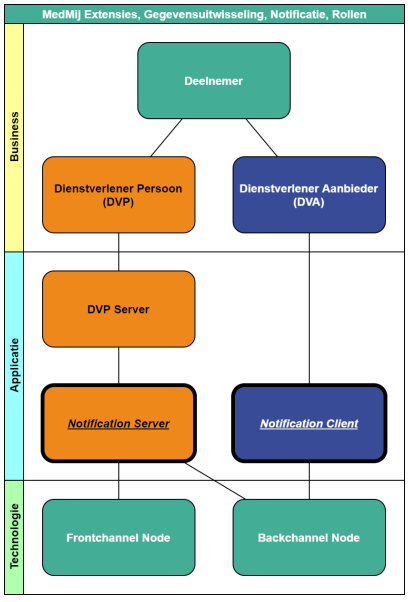
- Geel voor de businesslaag;
- Blauw voor de applicatielaag;
- Groen voor de technologielaag.

Rollen, Abonneren

1. Inleiding

De MedMij Core beschrijft rol *Resource Server*. Nauw gerelateerd aan deze rol beschrijft deze extensie de rollen *Subscription Server*, *Subscription Client*, *Notification Server* en *Notification Client*.





2. Roldefinities

Toelichting

De basis voor het rollenmodel van deze extensie wordt gevormd door het rollenmodel van de MedMij Core. Alleen de bij deze extensie behorende rollen staan op deze pagina uitgewerkt.

2.1. Applicatie

- **Subscription Server**
  Als *Dienstverlener aanbieder* de functie Abonneren aanbiedt dan biedt deze een geautomatiseerde rol voor het namens *Aanbieders* aangaan van Abonnementen, bestaande uit *Authorization Server* en *Subscription Server*.

- **Subscription Client**
  Als Dienstverlener persoon de functie Abonneren aanbiedt dan biedt deze een geautomatiseerde rol voor het namens *Personen* aangaan van Abonnementen, genaamd *Subscription Client*.

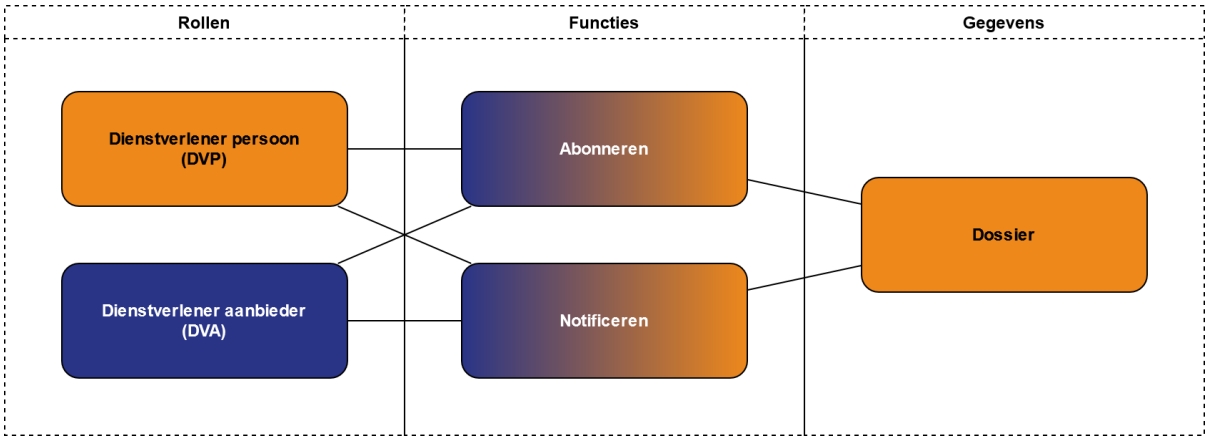
- **Notification Server**
  De *Dienstverlener persoon* stelt, indien deze functie Notificeren aanbiedt, aan *Aanbieder* een geautomatiseerde rol *Notification Server* ter beschikking, waarop de *Aanbieder* Notificaties kan aanbieden.

- **Notification Client**
  Dienstverlener aanbieder biedt, indien deze functie Notificeren aanbiedt, een geautomatiseerde rol voor het namens *Aanbieders* plaatsen van Notificaties, genaamd *Notification Client*.

Functies en gegevens, Abonneren

1. Inleiding

Onderstaand diagram toont de functies die vanuit deze extensie worden aangeboden, welke rollen verantwoordelijk zijn voor het leveren van deze functies en welke gegevens door de functie geleverd worden.



Dit diagram toont alleen de verantwoordelijke rol, behorende bij een aangeboden functie. De rollen die de functie gebruiken worden benoemd in de uitwerking van de functie, bijvoorbeeld in een stroomdiagram.

Dienstverlener aanbieder biedt aan *Dienstverlener persoon* twee functies, namelijk

- *Abonneren*
- *Notificeren*

Abonneren

1. Inleiding

In de platen hieronder staat het stroomdiagram van de functie *Abonneren*:

- De happy flow van de usecase Abonneren;
- De implementatie van de usecase Abonneren;
- De implementatie van het front- en backchannelverkeer.

De functie *Abonneren* hoort geheel bij de hoofdfunctie *Regie*. Zij omvat het aangaan, het veranderen van de duur en het beëindigen van *Abonnementen*.

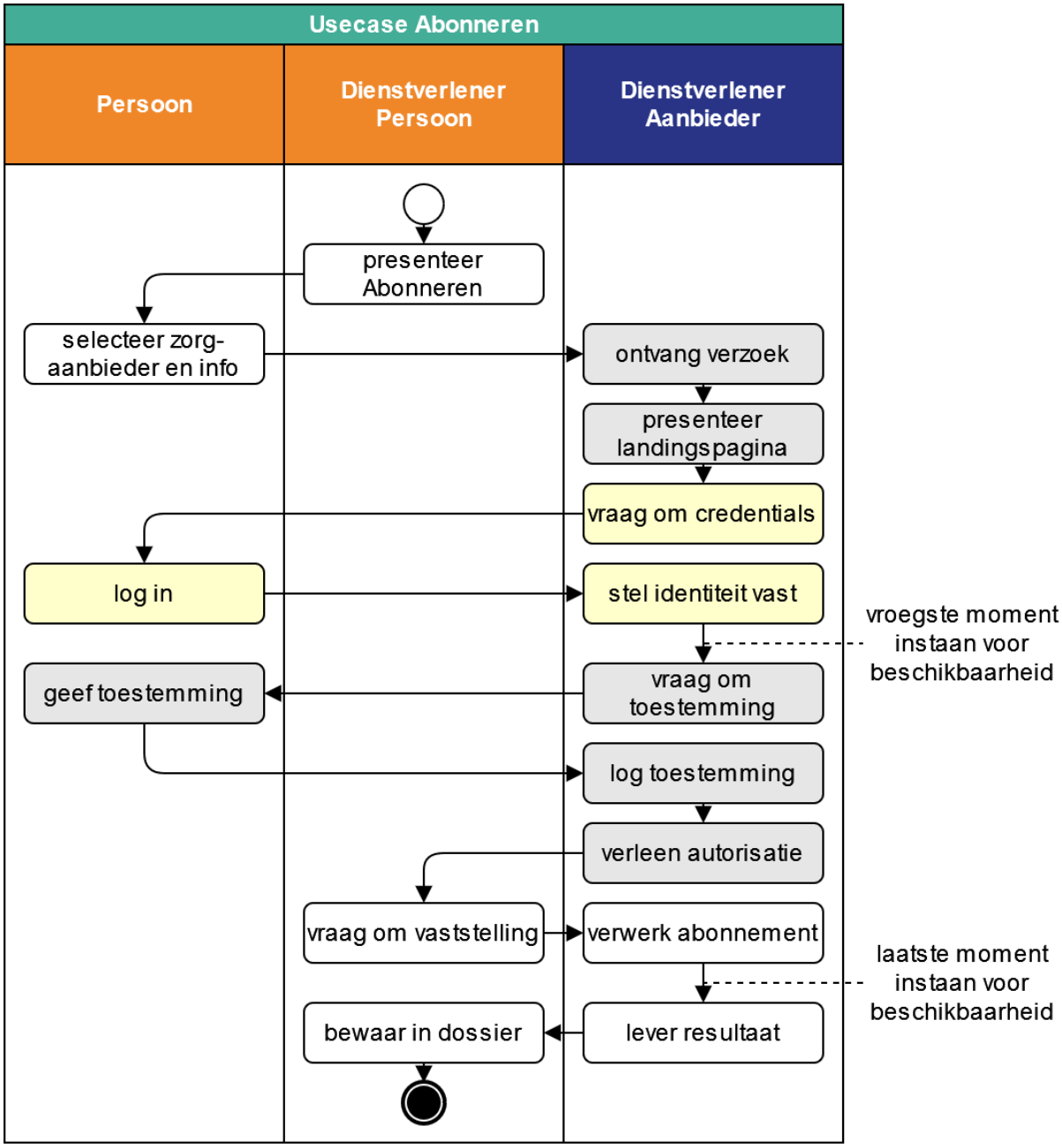
De stroomdiagrammen tonen allereerst de situatie waarin alle acties slagen tot en met het uiteindelijke afsluiten van een *Abonnement* (de zogenaamde happy flow). De oranje banen horen bij het Persoonsdomein, de blauwe bij het Aanbiedersdomein.

2. Usecase Abonneren

Menige actie in het stroomdiagram is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow; de zachtgeel gekleurde acties vormen samen de authenticatieflow.

Omdat het stroomdiagram alleen de happy flow bevat, worden zijn daarna de uitzonderingen beschreven.

2.1. Stroomdiagram



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De totale procesgang van de *usecase Abonneren* kent de volgende stappen:

- De *Dienstverlener persoon* presenteert aan de *Persoon* de mogelijkheid om *Abonnementen* aan te gaan, aan te passen of te beëindigen.
- De *Persoon* selecteert voor het aangaan van een *Abonnement* expliciet de *Aanbieder* en de specifieke *Gegevensdienst*, en voor het aanpassen of beëindigen het betreffende *Abonnement*. Daarvoor kunnen desgewenst de *Gegevensdienstnamen* worden gebruikt uit de *Gegevensdienstnamenlijst*. Het verzoek gaat naar de passende *Dienstverlener aanbieder*.
- De *Dienstverlener aanbieder* ontvangt de *Persoon*.
- De *Dienstverlener aanbieder* authentiseert de *Persoon*.

- Wanneer de *Persoon* de authenticatie heeft afgebroken geeft de *Dienstverlener aanbieder* de mogelijkheid alsnog te authenticeren of de flow af te breken.
- Indien het gaat om het aangaan of aanpassen van een *Abonnement*, breekt dan het moment aan waarop de *Dienstverlener aanbieder* op zijn vroegst ervoor instaat dat de *Aanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft, of anders de happy flow afbreekt. Het MedMij Afsprakenstelsel adviseert de beschikbaarheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. In deze release staat het MedMij Afsprakenstelsel het toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment. Het beëindigen van een *Abonnement* mag de *Aanbieder* niet weigeren.
- De *Dienstverlener aanbieder* vraagt aan de *Persoon* of hij toestemming geeft tot het verstrekken van de gevraagde informatie aan de *Dienstverlener persoon*. Deze vraag staat op de pagina Toestemmingsverklaring Abonneren. Indien het om de beëindiging van een abonnement gaat, staat de juiste informatie op de pagina Beëindigingsverklaring Abonnement.
- De *Dienstverlener aanbieder* logt die toestemming en laat de *Dienstverlener persoon* weten dat de toestemming gegeven is.
- Nu kan de *Dienstverlener persoon* de *Dienstverlener aanbieder* vragen om diens vaststelling van het aangaan, aanpassen of beëindigen van het *Abonnement*.
- Indien het gaat om het aangaan of aanpassen van een Abonnement, zal uiterlijk na de ontvangst van het verzoek de *Dienstverlener aanbieder* ervoor instaan dat de *Aanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft, of anders de happy flow afbreken.
- Bij ontvangst van het resultaat verwerkt de *Dienstverlener persoon* het nieuwe, aangepaste of beëindigde *Abonnement* in het persoonlijke *Dossier*.
- Bij de informatie wordt ook de meta-informatie opgeslagen die wordt bedoeld in verantwoordelijkheden core.logging.100, core.logging.101 en core.logging.102

De beschikbaarheidsvoorwaarde hoort bij *Regie*, niet bij *Uitwisseling*. De voorwaarde geeft de *Aanbieder* ruimte om deel te nemen in aan de *Persoon* gegeven *Regie*. Omdat echter bestaande implementatie-architecturen veelal uitwisseling centraal zetten, en niet *Regie*, hebben zij moeite de beschikbaarheidsvoorwaarde in de regiefase te implementeren. Daarom biedt het MedMij Afsprakenstelsel vooralsnog de gelegenheid om deze in de uitwisselingsfase te implementeren.

2.2. Uitzonderingen op de Happy flow van de usecase

In onderstaande tabel staan de uitzonderingssituaties beschreven. Alle worden door de *Dienstverlener aanbieder* ontdekt. Om te voorkomen dat de *Dienstverlener persoon* informatie over het bestaan van behandelrelaties verkrijgt zonder dat daarvoor (al) toestemming is gegeven, moet het onderscheid tussen de uitzonderingen 2, 3 en 4 niet te maken zijn door de *Dienstverlener persoon*.

Of de *Aanbieder* de gevraagde gezondheidsinformatie beschikbaar stelt aan de *Persoon*, is om te beginnen een zaak tussen de *Aanbieder* en *Persoon*, die daarvoor een behandelrelatie moeten hebben. Gegeven zo'n behandelrelatie is er wetgeving van toepassing op deze terbeschikkingstelling. Daarbinnen is eigen beslisruimte voor de *Aanbieder*. Omdat *Aanbieder* en *Persoon* evenwel geen *Deelnemers* in het MedMij Afsprakenstelsel zijn, specificeert het MedMij Afsprakenstelsel niet de exacte logica van de beslissing om de gezondheidsinformatie al dan niet ter beschikking te stellen. Om privacy-redenen vereist het MedMij Afsprakenstelsel echter wel dat er een behandelrelatie moet (hebben) bestaan waarbij de betreffende gezondheidsinformatie hoort én dat de *Persoon* minstens zestien jaar oud is (zie uitzondering Abonneren 3).

Voor het verstrekken van gegevens aan een minder dan zestienjarige moet toestemming of een machtiging tot toestemming worden verleend door degene die de ouderlijke verantwoordelijkheid of de wettelijke verantwoordelijkheid voor de minder dan zestienjarige draagt. Omdat in dergelijke toestemmingen of machtigingen nog niet is voorzien in deze versie van het MedMij afsprakenstelsel, kan deze controle vooralsnog als onderdeel van de beschikbaarheidsvoorwaarde worden opgevat. Wanneer een toekomstige release van het MedMij afsprakenstelsel wel zulke toestemmingen of machtigingen omvat, zal de leeftijdsvoorwaarde gescheiden moeten worden van de beschikbaarheidsvoorwaarde.

nr.	uitzondering	actie	vervolg
Abonneren 1	*Dienstverlener aanbieder* vindt het ontvangen verzoek ongeldig.	*Dienstverlener aanbieder* informeert *Dienstverlener persoon* over deze uitzondering. *Dienstverlener persoon* informeert daarop *Persoon* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
Abonneren 2	*Dienstverlener aanbieder* kan de identiteit van de *Persoon* niet vaststellen.	*Dienstverlener aanbieder* informeert *Dienstverlener persoon* dat verzoek niet wordt ingewilligd.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
Abonneren 3	*Dienstverlener aanbieder* stelt op enig moment namens *Aanbieder* vast dat niet wordt voldaan aan de beschikbaarheidsvoorwaarde. Hiervan is in elk geval sprake indien hetzij: • er geen behandelrelatie is aan te wijzen als grondslag voor het verzamelen; • *Persoon* nog geen zestien jaar oud is. Zie de toelichting op Beschikbaarheids- en ontvankelijkheidsvoorwaarde.		
Abonneren 4	*Persoon* geeft geen Toestemmingsverklaring Abonneren of Beëindigingsverklaring Abonnement af.		
Abonneren 5	*Dienstverlener aanbieder* kan het antwoord op de toestemmingsvraag niet vaststellen.	*Dienstverlener aanbieder* informeert *Dienstverlener persoon* over deze uitzondering. *Dienstverlener persoon* informeert daarop *Persoon* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
Abonneren 6	*Dienstverlener aanbieder* kan, zelfs na toestemming, de gezondheids- of *Abonnements*-informatie alsnog niet ter beschikking stellen aan de *Dienstverlener persoon*.	*Dienstverlener aanbieder* informeert *Dienstverlener persoon* over deze uitzondering. *Dienstverlener persoon* informeert daarop *Persoon* hierover, met opgave van oorzaak.	Mocht de gezondheidsinformatie deels wel (geautoriseerd) ter beschikking staan, dan kan de flow dat nog verzorgen.

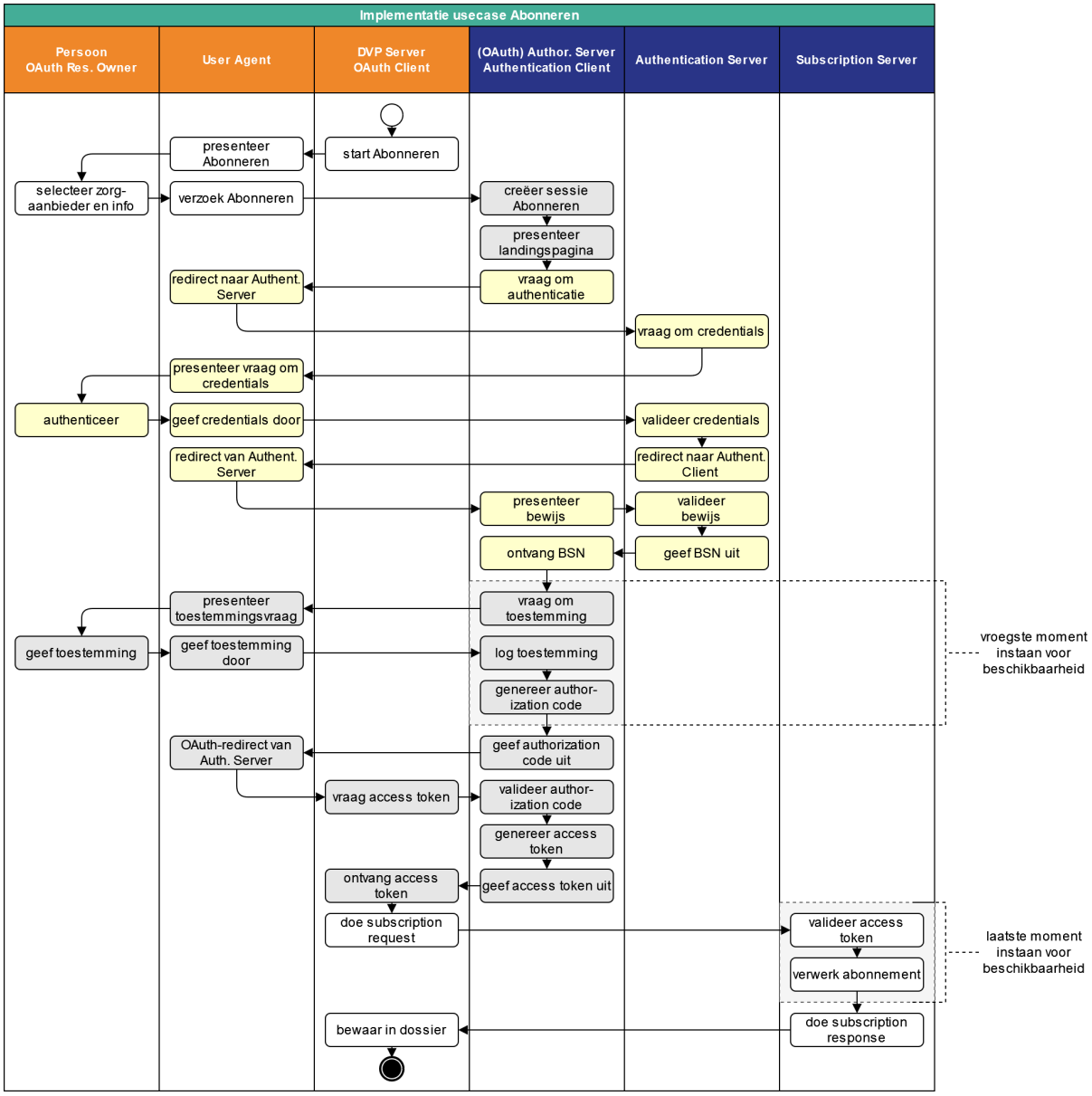
Abonneren 7	*Persoon* annuleert het inloggen.	*Dienstverlener aanbieder* presenteert een annuleringspagina en biedt *Persoon* de optie om toch in te loggen.	Indien *Persoon* kiest niet in te willen loggen, kan het scherm gesloten worden. *Persoon* kan er ook voor kiezen toch in te loggen. In dat geval vraagt *Dienstverlener aanbieder* weer om credentials.

3. Implementatie van de usecase Abonneren

Menige actie in het stroomdiagram is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow volgens OAuth; de zachtgeel gekleurde acties vormen samen de authenticatieflow. Deze kleuren verwijzen dus alleen maar naar de gebruikte standaarden en zeggen niets over welke component de stap zou moeten uitvoeren. Authenticatie is dus ingebed in autorisatie.

Verantwoordelijkheden inzake uitzonderingen op de happy flow zijn opgenomen bij de respectievelijke interface, waar de uitzonderingen bij de usecases zijn genoemd.

3.1. Stroomdiagram



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De flow kent de volgende stappen:

1. De *DVP Server* start de flow door in de *User Agent* van de *Persoon* de mogelijkheid te presenteren om zich bij een zekere *Aanbieder* te *Abonneren* op *Notificaties* voor een bepaalde *Gegevensdienst*. Het gaat altijd om precies één *Gegevensdienst*. Uit de *Aanbiederslijst* weet de *DVP Server* op welke *Gegevensdiensten* een *Aanbieder Abonnementen* aanbiedt worden. Desgewenst worden de *Gegevensdienstnamen* uit de *Gegevensdienstnamenlijst* gebruikt.
2. De *Persoon* maakt expliciet zijn selectie en laat de *User Agent* een abonneer-verzoek sturen naar de *Authorization Server*. Het adres van het authorization endpoint komt uit de *Aanbiederslijst*. De `redirect_uri` geeft aan waarnaartoe de *Authorization Server* de *User Agent* verderop moet redirecten (met de authorization code).

3. Daarop begint de *Authorization Server* de OAuth-flow (in zijn rol als *OAuth Authorization Server*) door een sessie te creëren.
4. De *Authorization Server* vraagt de *Persoon* via zijn *User Agent* in te loggen.
5. Dan start de *Authorization Server* (nu in de rol van *Authentication Client*) de authenticatieflow door de browser naar de *Authentication Server* te redirecten, onder meegeven van een `redirect_uri`, die aangeeft waarnaartoe de *Authentication Server* straks de *User Agent* moet terugsturen, na het inloggen van de *Persoon*.
6. De *Authentication Server* vraagt van de *Persoon* via zijn *User Agent* om inloggegevens.
7. Wanneer deze juist zijn, redirect de *Authentication Server* de *User Agent* terug naar de *Authorization Server*, onder meegeven van een ophaalbewijs. Wanneer het inloggen is afgebroken geeft de *Authorization Server* de *Persoon* alsnog de mogelijkheid via zijn *User Agent* in te loggen.
8. Met dit ophaalbewijs haalt de *Authorization Server* rechtstreeks bij de *Authentication Server* het BSN op.
9. Dan breekt het vroegste moment aan waarop de *Authorization Server* ervoor instaat dat de *Aanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft, of anders de happy flow afbreekt. Daarvan maakt deel uit dat de *Persoon* daarvoor minstens 16 jaar oud moet zijn.
10. Zo ja, dan presenteert de *Authorization Server* via de *User Agent* aan *Persoon* de vraag of laatstgenoemde hem toestaat de gevraagde persoonlijke gezondheidsinformatie (*Notificaties*) aan de *DVP Server* (als *OAuth Client*) te sturen. Onder het flow-diagram staat gespecificeerd welke informatie, waarvandaan, de *OAuth Authorization Server* verwerkt in de aan *Persoon* voor te leggen Toestemmingsverklaring Abonneren of Beëindigingsverklaring Abonnement.
11. Bij akkoord logt de *Authorization Server* dit als toestemming, genereert een authorization code en stuurt dit als ophaalbewijs, door middel van een browser redirect met de in stap 1 ontvangen `redirect_uri`, naar de *DVP Server*. De *Authorization Server* stuurt daarbij de local state-informatie mee die hij in de eerste stap van de *DVP Server* heeft gekregen. Laatstgenoemde herkent daaraan het verzoek waarmee hij de authorization code moet associëren.
12. De *DVP Server* vat niet alleen deze authorization code op als ophaalbewijs, maar leidt er ook uit af dat de toestemming is gegeven en logt het verkrijgen van het ophaalbewijs.
13. Met dit ophaalbewijs wendt de *DVP Server* zich weer tot de *Authorization Server*, maar nu zonder tussenkomst van de *User Agent*, voor een access token.
14. Daarop genereert de *Authorization Server* een access token en stuurt deze naar de *DVP Server*.
15. Nu is de *DVP Server* gereed om het verzoek tot vaststelling van het *Abonnement* naar de *Subscription Server* te sturen. Het adres van het subscription endpoint haalt hij uit de *Aanbiederslijst*. Hij plaatst het access token in het bericht en zorgt ervoor dat in het bericht geen BSN is opgenomen.
16. De *Subscription Server* controleert of het ontvangen token recht geeft op het gevraagde *Abonnement*. Dan breekt het uiterste moment aan waarop de *Subscription Server* ervoor moet instaan dat voor de betreffende *Gegevensdienst* de *Aanbieder* de gezondheidsgegevens beschikbaar heeft. Is dat zo, dan verstuurt de *Subscription Server* deze ze in de subscription response naar de *DVP Server*. Is dat niet zo, dan breekt de *Subscription Server* de happy flow af.
17. De *Subscription Server* legt het *Abonnement* vast zodanig dat bij een optredende wijziging in de *Gegevensdienst* voor deze *Persoon* een *Notificatie* verstuurd kan worden (zie functie Notificeren).
18. De *DVP Server* legt het *Abonnement* vast het *Dossier* van de *Persoon*.

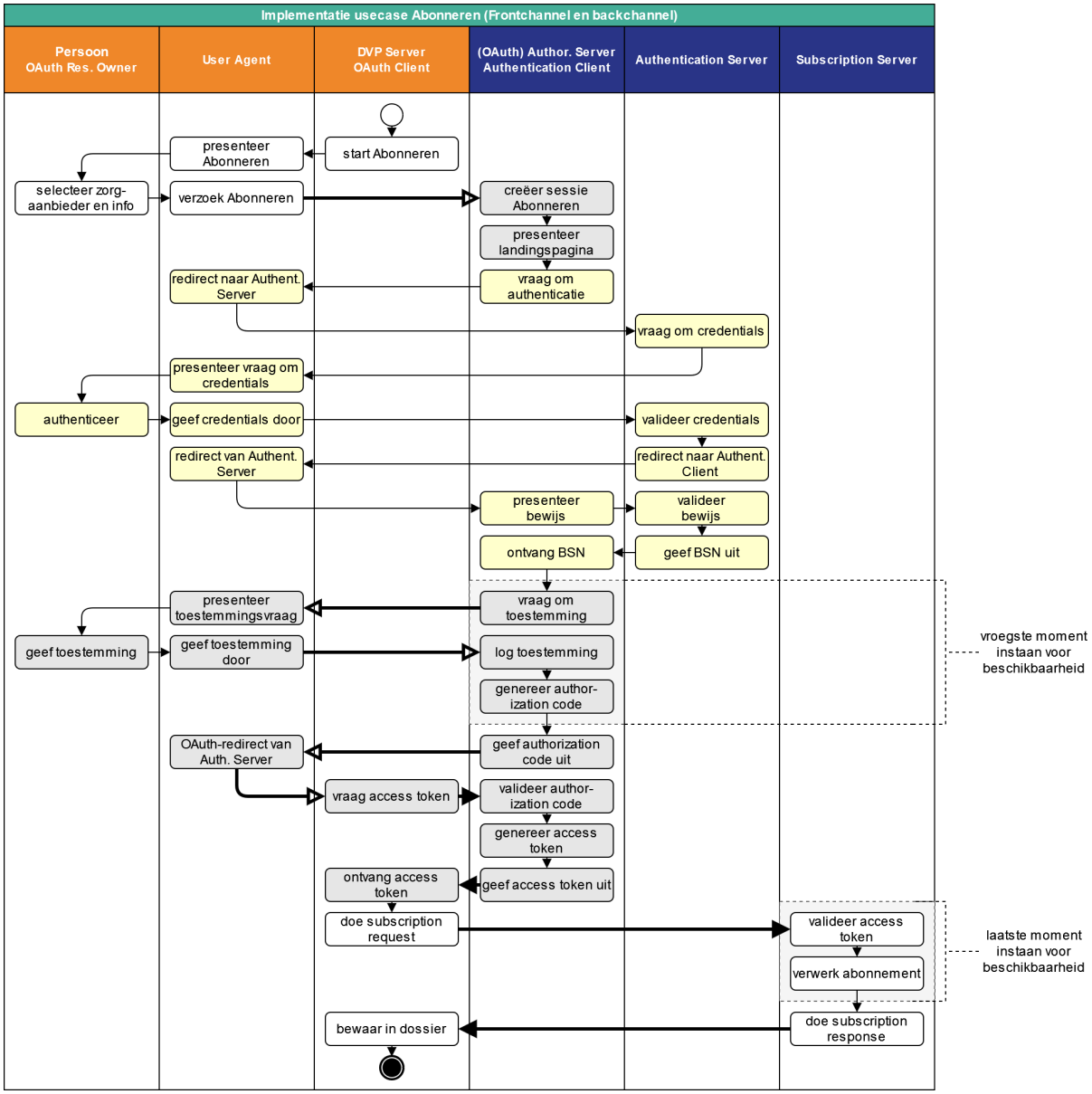
In de regel worden bij een eenmalig gebruik van de functie *Abonneren* het authorization interface, het token interface en het subscription interface allemaal aangesproken, in die volgorde. Mocht de *DVP Server* echter nog beschikken over een nog niet verlopen access token voor de betreffende *Aanbieder-Gegevensdienst-Interfaceversie*-combinatie, dan kan het onmiddellijk het subscription interface aanspreken.

Het MedMij Afsprakenstelsel adviseert de beschikbaarheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. Vooralsnog staat het MedMij Afsprakenstelsel toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment.

Bij de implementatie van de voorwaarde op beschikbaarheid bij de *Aanbieder* voor de te verzamelen gezondheidsgegevens is het zaak rekening te houden met privacy-vereisten. Wanneer de *Dienstverlener*

aanbieder ten behoeve van de beschikbaarheidsvoorwaarde nieuwe gegevensverzamelingen zou aanleggen, vindt een verwerking altijd onder de verantwoordelijkheid van één *Aanbieder* plaats. Het combineren van verwerkingen of het onvoldoende segregeren moet worden vermeden. Afwijking hiervan is alleen mogelijk onder expliciete instructie van de *Aanbieder(s)* en vereist een zorgvuldige voorafgaande afweging, vanwege de daaraan verbonden privacyrisico's.

3.2. Front- en backchannel



In ovenstaand stroomschema geven de dikke pijlen het *MedMij-verkeer* weer en zijn daarbinnen de vijf gevallen van frontchannel-verkeer (open pijlpunt) en vier gevallen van backchannel-verkeer (gesloten pijlpunt) aangegeven.

Notificeren

1. Inleiding

In de platen hieronder staat het stroomdiagram van de functie *Notificeren*:

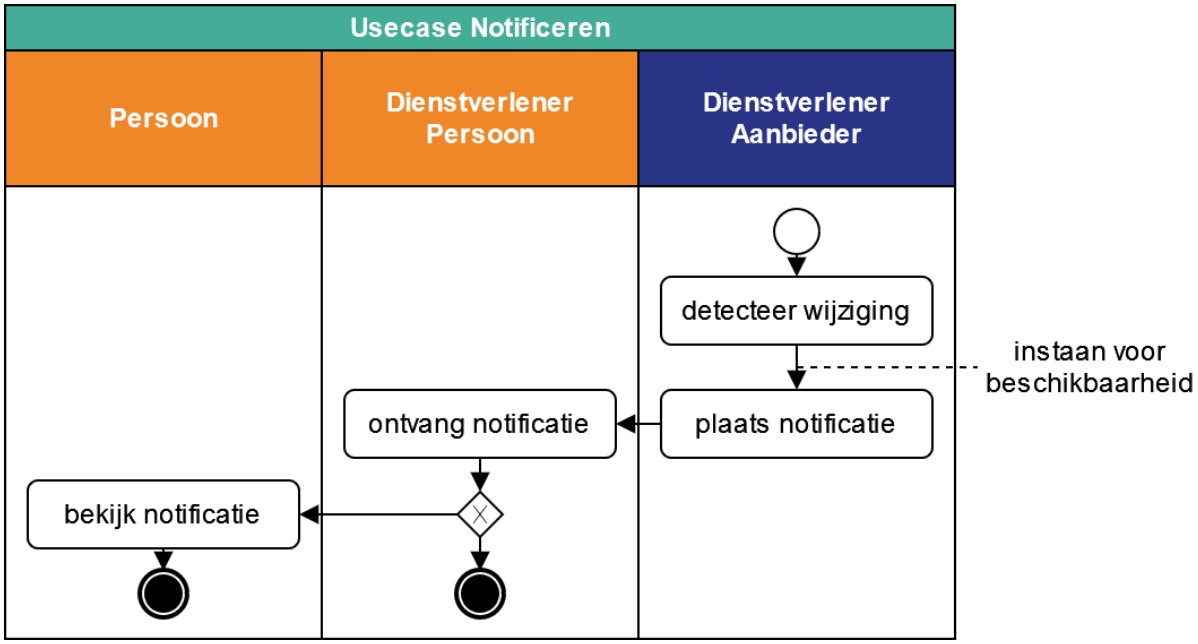
- De happy flow van de usecase Notificeren;
- De implementatie van de usecase Notificeren;
- De implementatie van het front- en backchannelverkeer.

De stroomdiagrammen tonen alleen de situatie waarin alle acties slagen tot en met het uiteindelijke verzamelen van de gezondheidsinformatie (de zogenaamde happy flow). De oranje banen horen, conform de MedMij-huisstijl tot het Persoonsdomein, de blauwe tot het Aanbiedersdomein.

2. Usecase Notificeren

Omdat het stroomdiagram alleen de happy flow bevat, worden zijn daarna de uitzonderingen beschreven.

2.1. Stroomdiagram



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De totale procesgang van de usecase Notificeren kent de volgende stappen:

- Hetzij de *Dienstverlener aanbieder* detecteert een wijziging in (gezondheids)informatie waarop *Persoon* een *Abonnement* heeft genomen (een inhoudelijke wijziging) of de *Dienstverlener aanbieder* beëindigt, op eigen initiatief, een specifiek *Abonnement* (een abonnementswijziging).
- Indien het een inhoudelijke wijziging betreft, wordt vastgesteld dat de *Persoon* instaat voor de beschikbaarheid van de betreffende gezondheidsinformatie. De notie van beschikbaarheid is dezelfde als die in de functie *Verzamelen*.
- De *Dienstverlener aanbieder* plaatst een *Notificatie* bij de *Dienstverlener persoon* en slaat de meta-informatie op die wordt bedoeld in verantwoordelijkheid core.logging.100.

- Bij ontvangst van een *Notificatie* slaat de *Dienstverlener persoon* de meta-informatie op die wordt bedoeld in verantwoordelijkheid ext.abo.logging.100.
- Mogelijk stelt de *Dienstverlener persoon* de *Persoon* op de hoogte van de *Notificatie*. Indien dat door middel van een tekstbericht gebeurt, worden hiervoor de teksten gebruikt die zijn opgenomen op de pagina Notificatie van Persoon.

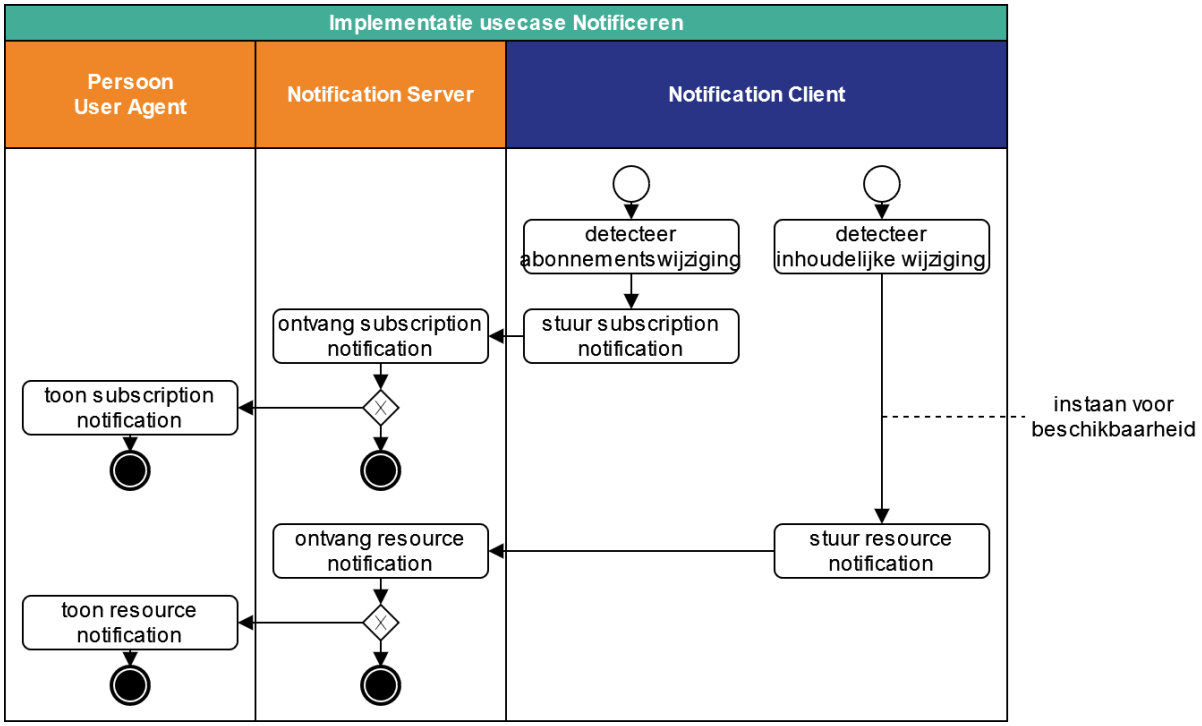
2.2. Uitzonderingen op de Happy flow van de usecase

Notificeren 1	*Dienstverlener persoon* vindt de ontvangen *Notificatie* ongeldig.	*Dienstverlener persoon* informeert *Dienstverlener aanbieder* over deze uitzondering.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
Notificeren 2	*Dienstverlener persoon* kan de *Notificatie* niet, niet geheel of niet tijdig verwerken.	*Dienstverlener persoon* informeert *Dienstverlener aanbieder* over deze uitzondering.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

3. Implementatie van de usecase Notificerene

Verantwoordelijkheden inzake uitzonderingen op de happy flow zijn opgenomen bij de respectievelijke interface, waar de uitzonderingen bij de usecases zijn genoemd.

3.1. Stroomdiagram

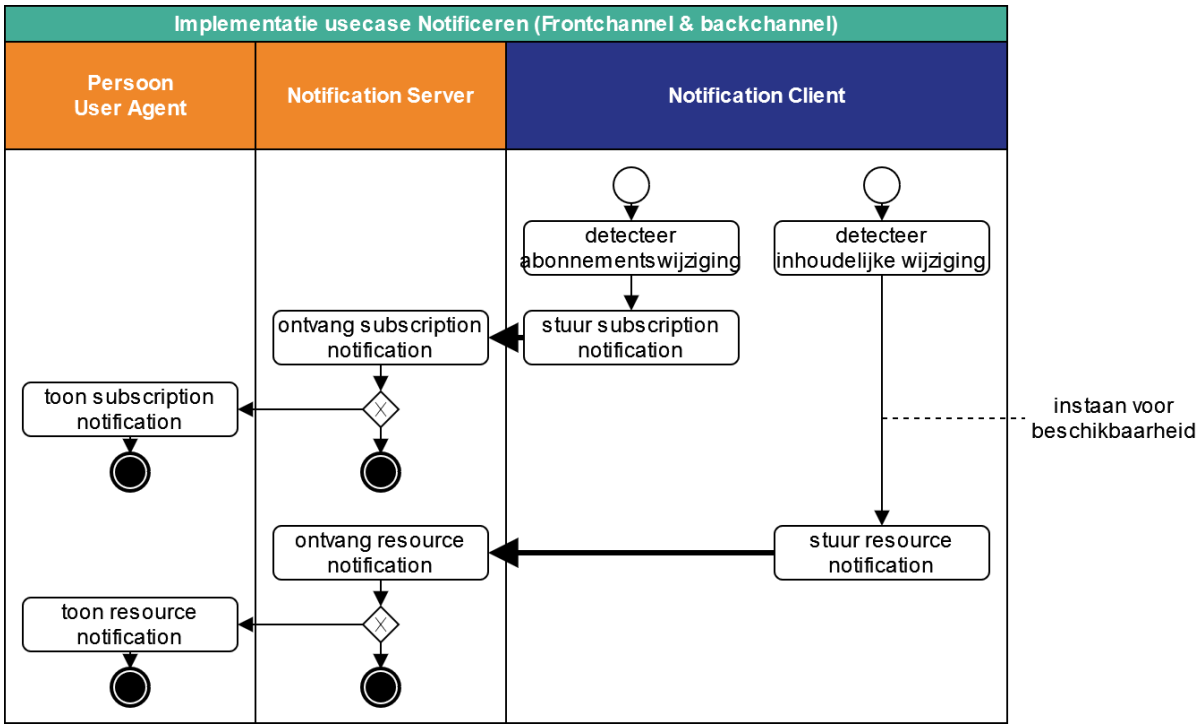


In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De flow kent de volgende stappen:

1. De *Notification Client* detecteert een inhoudelijke wijziging in de gezondheidsinformatie waarop *Persoon* een geldig *Abonnement* is aangegaan, respectievelijk de *Notification Client* detecteert dat de *Aanbieder* een zeker abonnement beëindigt.
2. In beide gevallen bepaalt de *Notification Client*, o.b.v. de `client_id` die werd gebruikt bij het aangaan van het *Abonnement*, in de *OAuth Client List* het juiste *Resource Notification Endpoint* , respectievelijk *Subscription Notification Endpoint*.
3. De *Notification Client* stuurt subscription notification, respectievelijk resource notification naar de *Notification Server*.
4. De *Notification Server* controleert de *Notificatie* , laat deze eventueel aan de *Persoon* tonen, en verstuurt een antwoord naar de *Notification Client*.

3.2. Front- en backchannel



Beide soorten *Notificaties* betreffen backchannel-verkeer.

Verantwoordelijkheden, Abonneren

1. Inleiding

De verantwoordelijkheden die in de MedMij Core staan beschreven, zijn ook van toepassing op deze extensie. Daarnaast gelden de hieronder (vervangende) verantwoordelijkheden. Net als in de MedMij Core zijn de volgende kleuren voor de verantwoordelijkheden op de verschillende lagen gebruikt:

- Geel voor de businesslaag;
- Blauw voor de applicatielaag;
- Groen voor de technologielaag.

2. Rollen

1	*Dienstverlener persoon stelt, indien deze de functie Notificeren aanbiedt, aan Aanbieder* een geautomatiseerde rol *Notification Server* ter beschikking, waarop de Aanbieder Notificaties kan aanbieden. Eén zulke Dienstverlener persoon biedt één of meerdere *Notification Servers* en elke *Notification Server* wordt door één Dienstverlener persoon geboden.	ext. abo. rollen. 200
2.	*Dienstverlener aanbieder* biedt een geautomatiseerde rol *Authorization Server*, voor het namens *Aanbieders* uitwisselen van gezondheidsinformatie met *DVP Server*. Deze rol wordt altijd in combinatie met een *Resource Server* en/of *Subscription Server*. Dit geldt als uitbreiding op de verantwoordelijkheid zoals beschreven in core.rollen. 201	ext. abo. rollen. 201
3.	*Dienstverlener aanbieder* biedt, indien deze de functie *Abonneren* aanbiedt, een geautomatiseerde rol *Subscription Server* voor het namens *Aanbieders* aangaan van *Abonnementen*. Elke zulke *Dienstverlener aanbieder* biedt één of meer combinaties van één *Authorization Server* en één *Subscription Server* en elke combinatie van één *Authorization Server* en één *Subscription Server* wordt door één *Dienstverlener aanbieder* geboden.	ext. abo. rollen. 202
4.	*Dienstverlener aanbieder* biedt, indien deze de functie *Notificeren* aanbiedt, een geautomatiseerde rol *Notification Client* voor het namens *Aanbieders* plaatsen van Notificaties, genaamd *Notification Client*. Elke zulke *Dienstverlener aanbieder* biedt één of meer *Notification Clients* en elke *Notification Client* wordt door één *Dienstverlener aanbieder* geboden.	ext. abo. rollen. 203
5.	Ten behoeve van het autoriseren van *DVP Server* voor toegang tot Subscription Server, in het kader van de functie *Abonneren*, zullen de betrokken *User Agent*, *DVP Server, Authorization Server* en *Subscription Server* gebruik maken van OAuth 2.0, waarbij als grant type gebruik wordt gemaakt van Authorization Code en waarbij: a. de rol van *OAuth Resource Owner* wordt verzorgd door de *Persoon*; b. de rol van *OAuth Client* wordt verzorgd door de *DVP Server*; c. de rol van *OAuth Resource Server* wordt verzorgd door de *Subscription Server*; d. de rol van *OAuth Authorization Server* wordt verzorgd door de *Authorization Server.* Dit geldt als uitbreiding op de verantwoordelijkheid zoals beschreven in core.rollen. 206.	ext. abo. rollen. 204

6.	De keuze, in OAuth, voor de grant type Authorization Code past bij de typische software-architectuur die in MedMij in het Persoonsdomein wordt aangetroffen: toegang tot een PGO-dienst via componenten die niet onder controle van de *OAuth Client* vallen en als betrekkelijk onveilig moeten worden gezien. Als *MedMij-verkeer* is gedefinieerd: al het gegevensverkeer in het kader van enige usecase-implementatie, onmiddellijk tussen twee verschillende van de vier volgende soorten rollen, namelijk: • ten eerste *DVP Server* of *Notification Server*, • ten tweede *User Agent*, • ten derde *Authorization Server*, *Resource Server*, *Subscription Server* of *Notification Client* , en • ten vierde *MedMij Registratie*, met dien verstande dat: • in deze rollen telkens begrepen zijn de door hen eventueel verzorgde respectievelijke Autorisatie-rollen, • van deze rollen telkens uitgesloten zijn de door hen eventueel verzorgde Authenticatie-rollen, en • in deze rollen, met betrekking tot de usecase-implementaties, telkens inbegrepen zijn de Nodes waarop zij functioneren. Dit geldt als uitbreiding op de verantwoordelijkheid zoals beschreven in core.rollen.207.	ext.abo.rollen.205
7.	Op één: • *Node* functioneert hetzij één *DVP Server*, hetzij één *Notification Server*, hetzij de combinatie van één *DVP Server* en één *Notification Server*. • *Node* functioneert hetzij één *Authorization Server*, hetzij één *Resource Server*, hetzij één *Subscription Server*, hetzij één *Notification Client,* hetzij een combinatie van voorgaande rollen. Dit geldt als uitbreiding op de verantwoordelijkheid zoals beschreven in core.rollen.301	ext.abo.rollen.300

3. Functies & gegevens

3.1. Abonneren

1.	Desgewenst biedt *Dienstverlener persoon* aan *Persoon* de functie *Abonneren.* Daarmee kan *Persoon* een *Abonnement op Notificaties* aangaan, verlengen, verkorten of beëindigen bij een *Aanbieder*, via *Dienstverlener aanbieder. Deze Notificaties* hebben betrekking op een *Gegevensdienst*. Bij deze functie betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.	ext.abo.abonneren.100
2.	Bij elke combinatie van *Persoon*, *Dienstverlener persoon*, *Aanbieder* en *Gegevensdienst* mag op elk moment maximaal één *Abonnement* actief zijn. De *Aanbieder* bepaalt de	

	duur van het *Abonnement*.	ext.abo. abonneren. 101
3.	Een *Dienstverlener persoon* of *Dienstverlener aanbieder* die de functie *Abonneren* aanbiedt, biedt ook de functie *Notificeren* aan.	ext.abo. abonneren. 102
4.	Een *Dienstverlener aanbieder* die de functie *Abonneren* ondersteunt, beëindigt een *Abonnement* wanneer: 1. het daartoe een verzoek van de *Dienstverlener persoon* ontvangt; 2. de *Dienstverlener aanbieder* na het sturen van een *Notificatie* ontdekt dat *Dienstverlener persoon* het betreffende *Abonnement* niet kent. 3. de looptijd van het *Abonnement* is verlopen; 4. de *Aanbieder* de betreffende *Gegevensdienst* niet langer aanbiedt, of wanneer de *Dienstverlener aanbieder* de betreffende *Gegevensdienst* niet langer ontsluit. In deze situatie beëindigt de *Dienstverlener aanbieder* onverwijld alle betreffende *Abonnementen*. Er worden geen eisen gesteld omtrent het beëindigen van een *Abonnement* ingeval (gezondheids)informatie van een *Persoon* niet langer beschikbaar is bij een *Aanbieder*, bijvoorbeeld na een dossieroverdracht, of na vernietiging van het dossier. Wanneer deze situatie zich voordoet, zullen simpelweg tot de einddatum van het *Abonnement* geen inhoudelijke *Notificaties* meer worden gegenereerd. Het zou kunnen gebeuren dat een *Notification Client* een *Notificatie* wenst te sturen, in het kader van een lopend *Abonnement*, maar de *OAuth Client List* aangeeft dat de betreffende *Notification Server* hetzij geen *Notificaties* meer kan ontvangen of de betreffende *Gegevensdienst* niet (meer) ondersteunt. In die gevallen wordt de *Notificatie* niet verzonden, maar blijft het *Abonnement* in beginsel wel intact. Omdat er geen *Notificaties* worden verstuurd, bestaan er geen risico's om het *Abonnement* aan te houden. Mocht de *OAuth Client List* een administratieve fout bevatten, is dat nog geen reden voor ontbinding van het *Abonnement* tussen *Persoon* en *Aanbieder*; als zo'n fout hersteld zou worden, kunnen er daarna weer *Notificaties* onder hetzelfde *Abonnement* verstuurd gaan worden. Mocht een *Notification Client* een dergelijke situatie aantreffen, is er wel aanleiding voor de betreffende *Dienstverlener aanbieder* om contact op te nemen met de betreffende *Dienstverlener persoon* en, waar dan nog nodig, met de MedMij-beheerorganisatie. Zie ook verantwoordelijkheid 3e. Het vierde punt gaat ervan uit dat de *Dienstverlener aanbieder* een eigen administratie bijhoudt van welke *Gegevensdiensten* hij voor welke *Aanbieders* ontsluit, en daarvoor niet leunt op de *Zorgaanbiederslijst* of andere lijsten. Zijn verwerkersrelaties met *Personen* zijn immers de bron van die lijsten, niet andersom. Het kan zijn dat de *Dienstverlener aanbieder* een fout in die eigen administratie maakt en dan, vanwege het vierde punt, de betreffende *Abonnementen* beëindigd. Het MedMij Afsprakenstelsel voorkomt dat niet, omdat die fout moet worden gezien als een fout van de *Dienstverlener aanbieder* als verwerker voor de *Aanbieder,* met andere woorden, in het kader van de *Dienstverleningsovereenkomst* tussen die twee, en niet op het MedMij-koppelvlak.	ext.abo. abonneren. 103
5.	Een *Dienstverlener persoon* die voornemens is het voeren van een zekere *Gegevensdienst* te beëindigen, of het voeren van *Abonnementen* te beëindigen, informeert daarover zijn gebruikers en laat, voor zover mogelijk, alle hierdoor getroffen	ext.abo. abonneren. 104

	lopende *Abonnementen* beëindigen.	
6.	Een *Abonnement* heeft een duur, gerekend in hele dagen vanaf het moment van aangaan, verlengen of verkorten. • De *Catalogus* geeft bij elke *Gegevensdienst* de maximale duur aan van een *Abonnement* op die *Gegevensdienst*; is die maximale duur `0`, dan kunnen er op die *Gegevensdienst* geen *Abonnementen* worden aangegaan. • De *Aanbieder* heeft, binnen de door de *Catalogus* aangegeven grenzen, ruimte voor eigen beleid aangaande de (maximale) duur van een *Abonnement*, gegeven de *Gegevensdienst* in kwestie. Dit wordt aangegeven in de *Zorgaanbiederslijst.* • De *Aanbieder* heeft, binnen de in de *Aanbiederslijst* aangegeven grenzen, ruimte voor eigen beleid aangaande de (maximale) duur van een *Abonnement*, gegeven de *Persoon* in kwestie. Dit beleid maakt deel uit van de beschikbaarheidsvoorwaarde. • De door een *Persoon* via zijn *Dienstverlener persoon* gevraagde duur van een *Abonnement* wordt gemaximeerd op de in de vorige drie punten bedoelde maximale duren. Bij het aangaan, verlengen, verkorten en beëindigen van Abonnementen wordt bij de betrokken interfaces gebruik gemaakt van twee verschillende parameters voor het aanduiden van de duur van het Abonnement: duration en end_date. • Abonnementsduur wordt toegepast in de *Authorization Interface* en de *Token Interface* en geeft de duur aan in het gewenste aantal dagen. Hierdoor is de controle door de *Authorization Interface* op een geldige waarde voor deze parameter eenduidig en ongecompliceerd. • `End_date` wordt toegepast in de *Subscription Interface*. In de transactie die daar plaats vindt, wordt de definitieve en precieze waarde van de datum tot waar een *Abonnement* loopt vastgesteld. Het door de *Aanbieder* gevoerde beleid omtrent de maximale duur van een *Abonnement,* de gewenste duur zoals ingebracht door de *Persoon* en een zekere vrijheidsgraad rond het hanteren van datumgrenzen en systeemtijden maken het noodzakelijk dat een eenduidige einddatum wordt vastgesteld.	ext.abo. abonneren. 105

3.2. Notificeren

1.	Een *Dienstverlener persoon* of *Dienstverlener aanbieder* mag de functie *Notificeren* aanbieden, als deze ook de functie *Abonneren* aanbiedt. Bij deze functie betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.	ext.abo. notificeren. 100
2.	Een *Notificatie* hoort altijd bij slechts één *Abonnement*.	ext.abo. notificeren. 101
3.	Er zijn twee soorten *Notificaties:* • inhoudelijke *Notificaties* brengen *Dienstverlener persoon* (en mogelijk *Persoon*) op de hoogte van de beschikbaarheid van nieuwe (gezondheids)informatie van *Aanbieder* bij *Dienstverlener aanbieder*, betreffende een *Gegevensdienst* waarop *Persoon* bij die *Aanbieder* geabonneerd is; • abonnements-*Notificaties* brengen *Dienstverlener persoon* (en mogelijk *Persoon*) op de hoogte van het door de *Aanbieder*, via *Dienstverlener aanbieder*, beëindigen van een *Abonnement* (zie verantwoordelijkheid 4 bij Abonneren).	ext.abo. notificeren. 102

4.	Indien een *Dienstverlener aanbieder* bij een *Aanbieder* een wijziging detecteert in gezondheidsinformatie die hoort bij een *Gegevensdienst* waarop een *Persoon* bij die *Aanbieder* een op dat moment geldig *Abonnement* heeft, via een *Dienstverlener persoon* , voorziet die *Dienstverlener aanbieder* die *Dienstverlener persoon* van een zogenoemde inhoudelijke *Notificatie*, door middel van de functie *Notificeren*.	ext.abo. notificeren. 103
5.	Indien een *Dienstverlener aanbieder* bij een *Aanbieder* een wijziging detecteert in een op dat moment geldig *Abonnement* dat een *Persoon, via een Dienstverlener persoon*, bij die *Aanbieder* is aangegaan, voorziet die *Dienstverlener aanbieder* die *Dienstverlener persoon* van een zogenoemde abonnements-*Notificatie*, door middel van de functie *Notificeren*.	ext.abo. notificeren. 104
6.	De in verantwoordelijkheid 4 bij Abonneren bedoelde beëindiging leidt: • niet tot een abonnements-notificatie in het eerste en tweede geval; • wel tot een abonnements-notificatie in het derde en vierde geval.	ext.abo. notificeren. 105

3.3. Opvragen Aanbiederslijst

1.	*MedMij Beheer* beheert en publiceert een *Aanbiederslijst*, namens de deelnemende *Dienstverlener aanbieder*. De gepubliceerde *Aanbiederslijst* bevat steeds en slechts alle actuele entries, en beschrijft van elke *Aanbieder*: • welke *Gegevensdiensten* deze momenteel aanbiedt, en welke technische adressen daarvoor moeten worden aangesproken bij de *Dienstverlener aanbieder*, gegeven een zekere *Interfaceversie*; • voor welke *Gegevensdiensten* het mogelijk is om *Abonnementen* aan te gaan en via welke technische adressen dit kan worden gedaan, gegeven een zekere *Interfaceversie*. In deze release van het MedMij Afsprakenstelsel staat de *Catalogus* alleen *Abonnementen* toe op *Gegevensdiensten* die zijn gebaseerd op de functie *Verzamelen*. Dit geldt als uitbreiding op de verantwoordelijkheid zoals beschreven in core.alst.100.	ext. abo. alst. 100

3.4. Opvragen Whitelist

1.	De *Node* die • de TLS-server is, voert de in verantwoordelijkheid core.whl.306 bedoelde controle tegen de *Whitelist* geheel uit voordat enige volgende stap wordt gezet door de *OAuth Authori-zation Server* of *OAuth Resource Server*, volgens de specifi-ca-ties van de functies *Abonneren* en *Notificeren*. Deze vereiste wordt volgordelijkheid genoemd. Indien de contro-le tegen de *Whitelist* niet kan worden uit-gevoerd, of een negatief resultaat ople-vert, wordt de proces-gang onmiddellijk af-gebroken en komt het niet tot een start van de uit-voering van die eerstvolgende stap. De con-trole tegen de*Whitelist* slaagt in dit geval dan en slechts dan als op de *Whitelist* tenmin-ste een van de vol-gende namen uit het de door de TLS-client aange-boden certificaat voorkomen: de `Com-mon Name` of een van de eventuele `Subject Alterna-tive Names`	ext. abo. whl. 300

	Dit geldt als uitbreiding op de verantwoordelijkheid zoals beschreven in core.whl.307.	

3.5. Opvragen OAuth Client List

1.	*MedMij Beheer* beheert en publiceert een actuele *OAuth Client List*, namens de deelnemende *Dienstverleners persoon*. De gepubliceerde *OAuth Client List* bevat steeds en slechts alle actuele entries, en beschrijft van elke *OAuth Client*: • wat de gebruikersvriendelijke namen zijn die voor de *Dienstverleners persoon* worden gebruikt in de Toestemmingsverklaring , de Bevestigingsverklaring en de Notificatie van Persoon; • op welke *Gegevensdiensten* de *Dienstverlener persoon* het ontvangen van *Notificaties*, in het kader van een *Abonnement*, ondersteunt en op welke technische adressen deze *Notificaties* moeten worden afgeleverd, gegeven een zekere Interfaceversie. In deze release van het MedMij Afsprakenstelsel kunnen slechts *Abonnementen* worden aangegaan op *Gegevensdiensten* die zijn gebaseerd op de functie *Verzamelen*. *De OAuth Client List bevat dus geen namen voor Dienstverleners aanbieder.* Dat is niet nodig, omdat deze niet voorkomen in de *Toestemmingsverklaring.* Dit geldt als uitbreiding op de verantwoordelijkheid zoals beschreven in core.ocl.100	ext. abo. ocl. 100
2.	*Notification Client* implementeert de functie *Opvragen OAuth Client List*, door middel van het bepaalde inzake het interface voor OAuth Client List op Interfaces lijsten.. Hiervoor wordt het betreffende stroomdiagram gebruikt.	ext. abo. ocl. 200
2.	*Notification Client* betrekt minstens elke vijftien minuten (900 seconden) de meest recente OAuth Client List (OCL) van *MedMij Registratie*.	ext. abo. ocl. 201
2.	*Notification Client* valideert elke nieuwe verkregen OAuth Client List (OCL) tegen het XML-schema van de *OAuth Client List*. Dit XML-schema is een technische implementatie van het MedMij-metamodel.	ext. abo. ocl. 202

4. Autorisatie

1.	*Dienstverlener aanbieder* vergewist zich ervan, elke keer opnieuw voordat hij *Persoon* een *Abonnement* met *Aanbieder* laat aangaan, dat deze *Persoon* uitdrukkelijk *Toestemming* heeft gegeven aan *Aanbieder* om *Notificaties,* betreffende de in de *Gegevensdienst* betrokken (gezondheids)informatie, aan *Dienstverlener persoon* ter beschikking te laten stellen. De vraag om *Toestemming* heeft een vaste formulering, die is opgenomen in de functie *Abonneren*. *Dienstverlener aanbieder* handelt dus ook bij het beschikbaar kunnen stellen van *Notificaties* conform een *Toestemming* van de *Persoon*. Deze *Toestemming* wordt gegeven bij het aangaan van het *Abonnement* en blijft geldig voor de duur van het *Abonnement*.	ext.abo. autorisatie. 100

2.	In de implementatie van de functie *Abonneren* handelen *DVP Server* enerzijds en *Authorization Server* en *Subscription Server* anderzijds, hun onderlinge verkeer af conform de standaard OAuth 2.0. Conform wettelijke verplichting geeft *Persoon*, in de functie *Abonneren*, actief toestemming aan de *Aanbieder.* De *User Agent* presenteert een venster waarin de *Persoon* deze toestemming, respectievelijk bevestiging, kan geven. Aangezien in het persoonsdomein niet met BSN gewerkt mag worden, moet er een vervangende identificatie van de *Persoon* gebruikt worden.	ext.abo.autorisatie.200

5. Authenticatie

1.	*Dienstverlener aanbieder* draagt ervoor zorg dat de onder core.gegevensdiensten.103, core.gegevensdiensten.104, core.autorisatie.100, core.autorisatie.101 en ext.geguit.autorisatie.100 bedoelde vraag om *Toestemming*, respectievelijk bevestiging, slechts plaatsvinden wanneer hij de identiteit van de *Persoon* met passende zekerheid heeft vastgesteld. Dit geldt als uitbreiding op de verantwoordelijkheid zoals beschreven in core.authenticatie.100	ext.abo.authenticatie.100

6. Adressering

1.	De *OAuth Client* stelt conform RFC 3986 de URI samen waarmee hij zichzelf, de *Authorization Server* en de *Subscription Server* adresseert. De *Notification Client* stelt conform RFC 3986 de URI samen waarmee hij de *Notification Server* adresseert. Dit geldt als uitbreiding op de verantwoordelijkheid zoals beschreven in core.adressering.200	ext.abo.adressering.200
2.	In alle adressering op de Subscription interface, de Subscription notification interface en de resource notification interface is het gebruik van het voor `https` bedoelde poortnummer, zoals opgenomen in de Service Name and Transport Protocol Port Number Registry van IANA, verplicht.	ext.abo.adressering.201
3.	Voor het samenstellen van alle adressen van het subscription request, betrekt de *OAuth Client* de eerste onderdelen van de URI, namelijk `host` en `path`, uit de *Aanbiederslijst*, op basis van de van toepassing zijnde *Aanbieder*, *Interfaceversie* en *Gegevensdienst.* Andere elementen van de algemene URI-syntax, zoals `user`, `password`, `query` en `fragment`, zijn afwezig in de adressen.	ext.abo.adressering.202
4.	De adressen voor de subscription notification en de resource notification betrekt de *Notification Client* uit de *OAuth Client List*, op basis van de van toepassing zijnde *OAuth Client* en *Gegevensdienst*.	ext.abo.adressering.203

De *Aanbiederslijst* wordt dus gebruikt door de *OAuth Client* om, gegeven een zekere *Interfaceversie*, het endpoint te kennen dat past bij de van toepassing zijnde *Aanbieder, Gegevensdienst* en, voor het resource endpoint, *Systeemrol*. Net zo gebruikt de *Notification Client* de *OAuth Client List* om, gegeven een zekere *Interfaceversie*, het endpoint te kennen dat past bij de van toepassing zijnde *OAuth Client* en *Gegevensdienst*. Daarom moet er uit één zo'n setje één endpoint-adres volgen. Andersom echter is dat

geen eis. Het is mogelijk om, in elke door de *Dienstverlener aanbieder* gewenste combinatie, endpointadressen te hergebruiken voor meerdere van zulke setjes in de *Aanbiederslijst*, respectievelijk door de *Dienstverlener persoon* in de *OAuth Client List*.

7. Logging

1.	*Dienstverlener persoon* zal het *Dossier* zo inrichten dat deze ook dienst kan doen als logbestand van ontvangen *Notificaties* en aangegane *Abonnementen*.	ext.abo. logging. 100
2.	*Dienstverlener aanbieder* zal een logbestand bijhouden van verzonden *Notificaties* en aangegane *Abonnementen*.	ext.abo. logging. 101

8. Beveiliging

1.	In het gegevensverkeer voor de functies Abonneren en Notificeren, maken betrokken rollen gebruik van de functies *Versleuteling*, *Server Authentication* en *Server Authorization*.	ext.abo. beveiliging. 200

Interfaces, Abonneren

1. Inleiding

Op deze pagina's staan de verantwoordelijkheden die horen bij de interfaces binnen deze Extensie. In elke functie wordt gebruik gemaakt van één of meer van deze interfaces. Onderstaande tabel laat zien welke functies welke interface gebruiken.

hoofdfunctie	*Regie*					*Uitwisseling*	
interface	**user interface**	**authorization interface**	**token interface**	**subscription interface**	**subscription notification interface**	**resource notification interface**	**resourc interfac**
geboden door rol		***Authorization Server***		***Subscription Server***	***Notification Server***		***Resour Serve***
Abonneren	X	X	X	X			
Notificeren					X	X	

Verantwoordelijkheden over de adressering van deze interfaces komen hieronder aan de orde. Verantwoordelijkheden voor de specifieke interfaces zijn opgenomen in specifieke subpagina's, die klikbaar zijn in bovenstaande tabel.

2. Adressen en interfaces

Op de zes interfaces in de flows van Abonneren en Notificeren adresseren Applicatie-rollen elkaar op basis van een URI. Onderstaande tabel geeft een overzicht.

hoofdfunctie	**interface**	**geadresseerde**	**bericht**	**kanaal**
Regie	subscription interface	*Subscription Endpoint* van de *Subscription Server*	subscription request	backchannel
	subscription notification interface	*Subscription Notification Endpoint* van de *Notification Server*	subscription notification	
Uitwisseling	resource notification interface	*Resource Notification Endpoint* van de *Notification Server*	resource notification	

In de nu verantwoordelijkheden wordt bepaald hoe de URI's zijn opgebouwd waarmee de adresbepaler de adresgebruiker de geadresseerde laat adresseren, en hoe de parameters worden gevuld. De opbouw van het adres is steeds dezelfde, ook voor frontchannel en backchannel. Desondanks maken we in het logische informatiemodel, in de *Aanbiederslijst*, wel onderscheid tussen *Frontchanneluri* en *Backchanneluri*. Dat houdt dat model wendbaarder, mocht er ooit wel adresseringsverschillen tussen frontchannel en backchannel ontstaan.

User interface (Autorisatieserver), Abonneren

De user interface hoort bij de hoofdfunctie *Regie*.

`NaamAanbieder`, `NaamGegevensdienst` en `NaamLeverancierPGO` zijn placeholders, zoals opgenomen in de Toestemmingsverklaring en de Bevestigingsverklaring.

`Duur` is een placeholder, zoals opgenomen in de Toestemmingsverklaring Abonneren.

1.	Het welkomstscherm dat aan de *Persoon* wordt gepresenteerd bij ontvangst op de Autorisatieserver in de functie *Abonneren* staat gespecificeerd op de pagina Landingspagina. Daarbij geldt dat: • de gebruikersvriendelijke weergave van de identiteit van de *Aanbieder* (`NaamAanbieder`) wordt bepaald door de betreffende *Dienstverlener aanbieder*, in haar dienstverleningsrelatie met de betreffende *Aanbieder*;	ext. abo. usrint. 100
2.	Het Annuleringsscherm, dat aan de *Persoon* wordt gepresenteerd na afbreken van de authenticatie in de functie Abonneren staat gespecificeerd op de pagina Annuleringspagina. Daarbij geldt dat: • de gebruikersvriendelijke weergave van de identiteit van de *Aanbieder* (`NaamAanbieder`) wordt bepaald door de betreffende *Dienstverlener aanbieder*, in haar dienstverleningsrelatie met de betreffende *Aanbieder*;	ext. abo. usrint. 101
3.	De vraag die aan de *Persoon* gesteld moet worden in de stap "autoriseer" in *Abonneren* staat gespecificeerd op de pagina Toestemmingsverklaring Abonneren. Daarbij geldt dat: • de gebruikersvriendelijke weergave van de identiteit van de *Aanbieder* (`NaamAanbieder`) wordt bepaald door de betreffende *Dienstverlener aanbieder*, in haar dienstverleningsrelatie met de betreffende *Aanbieder*; • de aangeboden looptijd van het Abonnement (`Duur`) door de beleid van de *Aanbieder* wordt bepaald, op basis van de door de *Persoon* gevraagde looptijd, en nooit langer dan de maximale looptijd die in de *Catalogus* bij de betreffende *Gegevensdienst* staat genoemd; • de gebruikersvriendelijke weergave van de *Gegevensdienst* (`NaamGegevensdienst`) wordt betrokken uit de scope die de *Authorization Server* in de allereerste stap van de flow heeft gekregen, die overeenkomt met de *Weergavenaam* die bij de betreffende *Gegevensdienst* in de *Gegevensdienstnamenlijst* is opgenomen; • de gebruikersvriendelijke weergave van de identiteit van de *Dienstverlener persoon* (`NaamLeverancierPGO`) wordt betrokken uit de *OAuth Client List*, op basis van de `redirect_uri` (van OAuth) die in stap 1 is verkregen.	ext. abo. usrint. 102

Authorization interface, Abonneren

De authorization interface hoort bij de hoofdfunctie *Regie*.

Op deze pagina staan alleen de verantwoordelijkheden inzake de authorization interface die nog niet genoemd staan in de OAuth 2-specificatie. Deze verantwoordelijkheden vormen een uitbreiding op de al geldende verantwoordelijkheden voor de Authorization interface vanuit de MedMij Core.

1. De parameters in de authorization request worden als volgt gevuld:

parameter	vulling	toelichting
`scope`	Voor "abonneren": • de letterlijke waarde `subscribe` • gevolgd door een tilde ~ • gevolgd door een niet-negatief geheel getal, aangevende de gevraagde maximale duur van het *Abonnement* • gevolgd door een forward slash / • gevolgd door één aanbieder-gegevensdienst-combinatie. Een aanbieder-gegevensdienst-combinatie bestaat uit: • één *Aanbiedernaam*, ontdaan van de suffix `@medmij` • gevolgd door een tilde (~) • gevolgd door één *GegevensdienstId* van een *Gegevensdienst* uit de *Gegevensdienstnamenlijst.*	Er worden geen andere scopes of onderdelen van scopes de genoemde. Voorbeelden van syntactisch juiste scopes zijn: • `"subscribe~180/eenofanderezorgaanbieder~` aangaan van een *Abonnement* op *Gegevensdienst* 42 `eenofanderezorgaanbieder@medmij` van maxima het aanpassen van het *Abonnement* op *Gegevensdier* `eenofanderezorgaanbieder@medmij` naar maxim vanaf vandaag; • `"subscribe~0/eenofanderezorgaanbieder~42` beëindigen van het *Abonnement* op *Gegevensdienst* 4 `eenofanderezorgaanbieder@medmij`.

> Bovenstaande tabel is een uitbreiding op de tabel die is weergegeven in core.authint.200

2. Vervolgens verifieert de *OAuth Authorization Server* dat:
   - de gevraagde *GegevensdienstId* voorkomt op de *OAuth Client List,* bij de betreffende `client_id` en gehanteerde *Interfaceversie*;

- zij namens deze *Aanbieder*, voor de gehanteerde *Interfaceversie*, deze *Gegevensdienst* ontsluit, in ov de gepubliceerde *Aanbiederslijst*;
- indien in de scope ook `subscribe` voorkomt (in geval van de functie Abonneren is dit verplicht):
  - de scope slechts één *GegevensdienstId* bevat;
  - bij de betreffende `client_id` en *Gegevensdienst* op de *OAuth Client List* ook een subscription n en een resource notification endpoint voorkomen;
  - zij namens deze *Aanbieder* ook *Abonnementen* op deze *Gegevensdienst* ontsluit;
  - de waarde van de duur parameter in het request de waarde heeft van `0` of een waarde groter dan is aan de maximale duur van het *Abonnement* zoals de betreffende *Aanbieder* deze aanbiedt.

Als een van deze verificaties niet slaagt dan behandelt de *Authorization Server* dit als uitzondering 1b volg verantwoordelijkheid core.authint.207.

Zo voorkomt de *Authorization Server* dat gevolg wordt gegeven aan een verzoek dat blijkens de *OAut Aanbiederslijst* niet is toegestaan.

> Dit geldt als uitbreiding op de verantwoordelijkheid zoals beschreven in core.authint.203.

3. Onmiddellijk na authenticatie van de *Persoon*, zoals bedoeld in verantwoordelijkheid core.authint.204, en slaagt, vraagt de *OAuth Authorization Server* de *Persoon* om een *Toestemmingsverklaring* (in het geval v *Abonneren*) of een *Bevestigingsverklaring* (in het geval van *Delen*), volgens het daaromtrent bepaalde op interface (Autorisatieserver), volgens de standaard OAuth 2.0, op de wijze waarop deze in het MedMij Afs toegepast.

   > Dit geldt als uitbreiding op de verantwoordelijkheid zoals beschreven in core.authint.205.

4. *Authorization Server* en *DVP Server* behandelen uitzonderingssituaties inzake het authorization interface onderstaande tabel.

Nummer	Implementeert uitzonderingen	Uitzondering	Actie	Melding
Authorization interface 1a	Abonneren 1	*Authorization Server* ontvangt een authorization request zonder (geldige) `redirect_uri` en/of zonder een (geldige) `client_id`.	*Authorization Server* informeert *User Agent* over deze uitzondering. *Authorization Server* voert geen redirect naar de *Client* uit, ook niet met een foutmelding.	conform OAut 2.0-specificati par. 4.1.2.1
Authorization interface 1b		*Authorization Server* ontvangt een ongeldige authorization request, anders dan uitzondering 1.	*Authorization Server* informeert *DVP Server*	conform OAut 2.0-specificati par. 4.1.2.1, m de daar

			over deze uitzondering. *DVP Server* informeert *Persoon* daarover.	genoemde, zo specifiek mogelijke, toepasselijke error code
Authorization interface 2	Abonneren 2	*Authorization Server* kan de identiteit van de *Persoon* niet vaststellen.	*Authorization Server* informeert *DVP Server* over deze uitzondering. *DVP Server* informeert *Persoon* dat diens verzoek geen voortgang kan vinden, maar laat de oorzaak daarvan helemaal in het midden.	conform OAutl 2.0-specificatie par. 4.1.2.1, er code `access denied`, met i de error description " `Access denied.`"
Authorization interface 3	Abonneren 3	*Authorization Server* stelt tijdens de afhandeling van de authorization request vast dat: • in geval van de functie *Verzamelen*: van *Persoon* bij *Aanbieder* geen gezondheidsinformatie voor die *Gegevensdienst* beschikbaar is; • in geval van de functie *Delen*: *Aanbieder* niet ontvankelijk is voor die *Gegevensdienst* van *Persoon;* • in geval van de functie *Abonneren*: *Persoon* geen *Notificaties* beschikbaar maakt voor *Persoon* op die *Gegevensdienst*. Zie de toelichting op Beschikbaarheids- en ontvankelijkheidsvoorwaarde .		
Authorization interface 4	Abonneren 4	De autorisatievraag wordt ontkennend beantwoord.		
Authorization interface 5	Abonneren 5	*Authorization Server* kan de autorisatie niet vaststellen.	*Authorization Server* informeert *DVP Server* over deze uitzondering. *DVP Server* informeert daarop *Persoon* hierover.	conform OAutl 2.0-specificatie par. 4.1.2.1, er code `access denied`, met i de error description " `Authorizati failed.`"

De uitzonderingssituaties kunnen gezien worden als de implementatie-tegenhangers van de uitzonde
functies Verzamelen en de Delen. Op de Applicatielaag zijn deze echter per interface geordend. Alle u
worden door de *Authorization Server* ontdekt. In deze versie van het MedMij Afsprakenstelsel is bepaa
tot het zo snel mogelijk afbreken van de flow door alle betrokken rollen. Daartoe moeten echter eerst r
geïnformeerd worden. Om te voorkomen dat de *DVP Server* informatie over het bestaan van behande
zonder dat daarvoor (al) toestemming is gegeven, moet het onderscheid tussen de uitzonderingen 2, 3
zijn door de *DVP Server*.

Deze tabel bevat alleen die uitzonderingssituaties ten aanzien waarvan het MedMij afsprakenstelsel ei
de implementatie. In de specificatie van OAuth 2.0 staan daarnaast nog generiekere uitzonderingssitu
situatie waarin de redirect URI ongeldig blijkt. Ook deze uitzonderingssituaties moeten geïmplementee

Token interface, Abonneren

Op deze pagina staan alleen de verantwoordelijkheden inzake het token interface die nog niet genoemd staan in de OAuth 2-specificatie.

<table>
<tr>
<td>1.</td>
<td>De parameters in de access-token response worden als volgt gevuld:
<table>
<tr><th>parameter</th><th>vulling</th><th>toelichting</th></tr>
<tr><td><code>scope</code></td><td>Conform sectie 5.1 van de OAuth 2.0-specificatie.

In toevoeging daarop: verplicht indien het authorization request verzocht om een Abonnement. In dat geval is de <code>scope</code>-parameter gelijk aan die in de betreffende authorization request, maar met de Abonnements-einddatum gesteld op de door de Authorization Server toegekende, en dus mogelijk beperkte, waarde. De toegekende duur van het Abonnement is:

• niet hoger dan de in de authorization request gevraagde duur van het Abonnement;
• niet hoger dan de maximale abonnementsduur die de Aanbieder in de Aanbiederslijst had opgenomen bij die Gegevensdienst en die Interfaceversie;
• bij een gevraagde beëindiging gelijk aan <code>0</code>.

In toevoeging daarop:

1. Verplicht indien het authorization request verzocht om Verzamelen van meerdere Gegevensdiensten en hiervan niet alle Gegevensdiensten beschikbaar bleken voor Persoon. In dat geval is de <code>scope</code>-parameter gelijk aan die in de betreffende authorization request, met daaruit weggelaten de niet-beschikbare zorgaanbieder-gegevensdienst-combinaties.
2. Verplicht indien het authorization request verzocht om een Abonnement. In dat geval is de <code>scope</code>-parameter gelijk aan die in de betreffende authorization request, maar met de Abonnements-einddatum gesteld op de door de Authorization Server toegekende, en dus mogelijk beperkte, waarde. De toegekende duur van het Abonnement is:

• niet hoger dan de in de authorization request gevraagde duur van het Abonnement;
• niet hoger dan de maximale abonnementsduur die de Aanbieder in de Aanbiederslijst had opgenomen bij die Gegevensdienst en die Interfaceversie;
• bij een gevraagde beëindiging gelijk aan <code>0</code>.</td><td></td></tr>
</table>
Bovenstaande tabel is een uitbreiding op de tabel die is weergegeven in core.tknint.201</td>
<td>ext. abo. tknint. 200</td>
</tr>
<tr>
<td>2.</td>
<td>Na ontvangst van een access token request, in de functies Verzamelen, Delen of Abonneren, zal de OAuth Authorization Server, indien in antwoord daarop een access token dient te</td>
<td>ext. abo.</td>
</tr>
</table>

worden uitgegeven, na maximaal tien (10) seconden dit acces token ter beschikking stellen aan de *OAuth Client*. Dit gedrag van de *OAuth Authorization Server* is gedurende minimaal 99,5% van de tijd beschikbaar.

tknint.201

> Bovenstaande tabel is een uitbreiding op de tabel die is weergegeven in core.tknint.206

3. *OAuth Authorization Server* en *OAuth Client* behandelen uitzonderingssituaties inzake het token interface volgens onderstaande tabel.

ext.abo.tknint.202

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Vervolg
Token interface 1	Abonneren 6	*Authorization Server* moet vanwege één van de in de OAuth 2.0-specificatie, par. 5.2, genoemde redenen de token request weigeren.	*Authorization Server* informeert *DVP Server* over deze uitzondering. *DVP Server* informeert daarop *Persoon* hierover.	met de conform OAuth 2.0-specificatie, par. 5.2, toepasselijke error code	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

De uitzonderingssituaties kunnen gezien worden als de implementatie-tegenhangers van de uitzonderingen van de functies Verzamelen en de Delen. Op de Applicatielaag zijn deze echter per interface geordend. Alle uitzonderingen worden door de *Authorization Server* ontdekt. In deze versie van het MedMij Afsprakenstelsel is bepaald dat zij altijd leiden tot het zo snel mogelijk afbreken van de flow door alle betrokken rollen. Daartoe moeten echter eerst nog de andere rollen geïnformeerd worden.

Deze tabel bevat alleen die uitzonderingssituaties ten aanzien waarvan het MedMij afsprakenstelsel eigen eisen stelt aan de implementatie. In de specificatie van OAuth 2.0 staan daarnaast nog generiekere uitzonderingssituaties, zoals de situatie waarin de redirect URI ongeldig blijkt. Ook deze uitzonderingssituaties moeten geïmplementeerd worden.

Subscription interface

Het subscription interface hoort bij de hoofdfunctie Regie.

Er zijn drie typen subscription request:

- de subscription creation request voor het aanmaken van een nieuw *Abonnement;*
- de subscription modification request voor het wijzigen van de duur van een bestaand *Abonnement;*
- de subscription termination request voor het beëindigen van een bestaand *Abonnement.*

Met de subscription creation request biedt de *DVP Server* aan de *Subscription Server* een nieuwe *Subscription*-resource aan, die het *Abonnement* representeert, met daaraan verbonden het vooralsnog eenzijdige akkoord van de *Persoon*. Hij verzoekt daarmee bovendien om een subscription response, waarmee ook het akkoord van de *Aanbieder* is verbonden. Zo ontstaat de overeenkomst.

Ook het aanpassen van de duur, via de einddatum parameter, van het *Abonnement,* door het versturen van een subscription modification request, ontvangt zo het akkoord van beide partijen; al mag de *Aanbieder* een verkorting van het *Abonnement* niet weigeren; een verlenging kan wel geweigerd worden door de *Aanbieder*.

Een beëindiging van een *Abonnement*, door het versturen van een subscription termination request, is een eenzijdige opzegging van de overeenkomst. De *Aanbieder* mag deze niet weigeren en er is in die zin geen sprake van een akkoord van beide partijen.

1.	De *OAuth Client* en de *Subscription Server* maken op de subscription interface gebruik van HTTP 1.1.
2.	De *OAuth Client* en de *Subscription Server* maken voor het uitwisselen van subscription requests en de responses gebruik van het formaat JSON. Dit wordt in de HTTP header aangegeven middels: • Content-Type: application/json • Accept: application/json
3.	De *OAuth Client* gebruikt voor het sturen van het access token, voor alle typen subscription request, de `Authorization Request Header Field`, zoals beschreven in sectie 2.1 van RFC6750. De methode `Authorization Request Header Field` biedt de beste beveiliging. Het access token moet een scope hebben die precies overeenkomt met de parameters van het betre request en bij wijzen of beëindigen van een *Abonnement* ook met de zorgaanbieder en gegevensdie *Abonnement* dat wordt aangeduid met het `subscription_id`.
4.	De subscription creation request: • is een HTTP POST-request met structuur: `<base url>/Subscription` en verder zonder paramet • bevat in de HTTP body een complete representatie van de *Subscription* Resource met de volgende

parameter	vulling	toelichting
`aanbieder`	verplicht, dezelfde waarde als voor de *Aanbieder* in de scope van het gebruikte access token	-

`gegevensdienst`	verplicht, dezelfde waarde als voor de *Gegevensdienst* in de scope van het gebruikte access token	-
`client_id`	verplicht, dezelfde waarde als de `client_id` die gebruikt is in het gebruikte access token	-
`end_date`	verplicht, de waarde voor de gewenste dag waarop het *Abonnement* stopt.	De `end_date` dient gespecificee `full-date`: 'YYYY-MM-DD' De *Subscription Server* controlee geldig is, dit is als: • de `end_date` valt binnen de waarde van duur in het gebru Token interface) • de `end_date` heeft een hoge huidige datum

5. Een response op een succesvol verwerkt subscription creation request:

   - bevat een status code met waarde 201
   - bevat een location header bevatten met een link naar de nieuwe resource (inclusief de toegekende s `url>/Subscription/<subscription-id>`
   - bevat in de HTTP body de volgende parameters:

parameter	vulling	toelichting
`subscription_id`	identificatie waarmee de *Subscription Server* het *Abonnement* uniek voor deze *Persoon* en de *Dienstverlener persoon* identificeert	Deze waarde gebruikt de *Subscription* binnenkomende *Subscription modificati* betreffende *Abonnement* te identificere het *Abonnement* in logbestanden. Het `subscription_id` kan een integ UUID, maar kan ook volgens een ande identificatiepatroon worden gevuld.
`zorgaanbieder`	verplicht, dezelfde waarde als voor de *Aanbieder* in het request	-
`gegevensdienst`	verplicht, dezelfde waarde als voor de *Gegevensdienst* in het request	-
`client_id`	verplicht, dezelfde waarde als de `client_id` die gebruikt is in het gebruikte access token	-
`end_date`	datum waarop het *Abonnement* verloopt.	Deze datum geeft de dag aan waarop stopt met het sturen van *Notificaties* vo Conform RFC 3339 `full-date`: 'YYY

6. De subscription modification request:

- is een HTTP PATCH-request met structuur: `<base url>/Subscription/<subscription-id>` parameters in de URL
- bevat in de HTTP body slechts de volgende parameters van de aan te passen *Subscription* Resourc

parameter	vulling	toelichting
`end_date`	verplicht, datum waarop het Abonnement verloopt.	De `end_date` dient gespecificeerd conform RFC 3339 MM-DD' De *Subscription Server* controleert of de `end_date` ge • de end_date valt binnen de huidige datum + de wa gebruikte access token (zie Token interface) • de end_date valt binnen de gestelde maximale duu *Abonnement* • de end_date heeft een hogere waarde dan de huidi

7. In het geval van een subscription modification request verifieert de *Subscription Server* dat voor het mee id een geldig *Abonnement* is geregistreerd, waarvan de waarden van de attributen overeenkomen met d scope van het gebruikte access token. Indien dit niet het geval is, behandelt de *Subscription Server* dat Subscription interface 4.3c.

8. Een response op een succesvol verwerkt modification creation request:

   - bevat een status code met waarde 200
   - bevat in de HTTP body de volgende parameters:

parameter	vulling	toelichting
`end_date`	datum waarop het *Abonnement* verloopt.	Deze datum geeft de dag aan waarop de *Subscription Server* sto *Notificaties* voor dit Abonnement. Conform RFC 3339 `full-dat`

9. De subscription termination request:

   - is een HTTP DELETE-request met structuur: `<base url>/Subscription/<subscription-id>` parameters in de URL
   - bevat in de HTTP body geen parameters

10. In het geval van een subscription termination request verifieert de *Subscription Server* dat voor het mee een geldig *Abonnement* is geregistreerd, waarvan de waarden van de attributen overeenkomen met de van het gebruikte access token. Indien dit niet het geval is, behandelt de *Subscription Server* dat als uitz interface 4.

11. Een response op een succesvol verwerkt termination creation request:

    - bevat een status code met waarde 204
    - bevat in de HTTP body geen parameters

12. In het geval van een subscription creation request of een subscription modification request stelt de *Subs* einddatum (`end_date`) van het *Abonnement* in onder voorbehoud van het beleid van de *Aanbieder* en c maximale duur van de desbetreffende *Gegevensdienst* in de *Catalogus*. Op grond hiervan mag de *Subs* subscription request toetsen aan het beleid dat de *Aanbieder* voert voor *Abonnementen* op de *Gegeven*

op grond hiervan een kortere duur toekennen of weigeren. In geval van weigering behandelt de *Subscrip* uitzondering Subscription interface 5.

Een *Aanbieder* heeft zowel verantwoordelijkheden als vrijheidsgraden rond het aanbieden en aangaa In het Afsprakenstelsel wordt dit gefaciliteerd door de *Aanbieder* de mogelijkheid te geven beleid te v Abonnement op Notificaties. Een *Aanbieder* kan voor een bepaalde Gegevensdienst een eigen maxi gesteld in de Catalogus) opgeven. Een *Aanbieder* mag het verlengen van een bestaand Abonnemen

De *Subscription Server* heeft zekere vrijheid om bij het bepalen van de einddatum van een *Abonnem* met tijdzone's en datumgrenzen.

13. Indien bij het verwerken van een subscription request aan alle voorwaarden is voldaan, dan

- laat de *Subscription Server* het *Abonnement* per direct ingaan, danwel
- beëindigd de *Subscription Server* het *Abonnement* per direct.

De *Subscription Server* heeft enige vrijheid bij het hanteren van het precieze moment op de dag waa het versturen van *Notificaties.* Het staat de *Subscription Server* vrij om dit op enig moment van de be

14. Bij het verlopen van het *Abonnement* verstuurt de *Subscription Server* een subscription notification naar *Persoon.*

15. Na ontvangst van een subscription request , in de functie *Abonneren*, zal de *Subscription Server*, indien subscription response dient te worden gedaan, na maximaal zestig (60) seconden dit subscription respo stellen aan de *DVP Server*. Dit gedrag van de *Subscription Server* is gedurende minimaal 98,5% van de

16. Voor zover er in het verkeer tussen *DVP Server* en *Subscription Server* in de functie *Abonneren* sprake van een gegevenselement dat tot de identiteit van de *Persoon* herleid kan worden, gebruiken zij daarvoo OAuth-gegevens die zij in hun respectievelijke *OAuth Client* en *OAuth Resource Server* moeten uitwisse *Authorization Server* en *Subscription Server* treffen goed beveiligde voorzieningen waarmee zij hieruit w identiteit van de *Persoon* kunnen vaststellen.

Met het oog op het borgen van de privacy en het zo eenvoudig mogelijk houden van de architectuur Afsprakenstelsel, wordt ervoor gekozen de identifier voor de *Persoon* onderweg zo betekenisloos mo betekenis wordt er ter weerszijden aan verbonden door raadpleging van interne registraties. Omdat d *Authorization Server* en *Subscription Server* samen een OAuth-flow afhandelen, beschikken zij (na a *Persoon*) over tokens die de identiteit van de Persoon vertegenwoordigen, namelijk (eerst) de author het access token. Buiten deze hoeven en mogen er geen identificerende gegevenselementen in het opgenomen.

17. *OAuth Resource Server* en *OAuth Client* handelen uitzonderingssituaties inzake het subscription interfac onderstaande tabel.

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding
Subscription interface 1	Abonneren 6	Het subscription request bevat geen access_token.	*Subscription Server* informeert *DVP Server* over deze uitzondering.	Een Status-Code 401 conform HTTP specificatie. In deze situatie retourneert de *Subscription Server* uitdrukkelijk géén nadere informatie over

			de opgetreden uitzondering.
Subscription interface 2	De *Subscription Server* detecteert dat het meegezonden access_token is verlopen of om een andere reden niet geldig is.		Een Status-Code 401 conform HTTP specificatie en een `WWW-Authenticate` HTTP response header met als auth-scheme "`Bearer`" en een `error` attribuut met waarde "`invalid_token`". conform RFC 6750.
Subscription interface 3	De *Subscription Server* detecteert dat de scope die is verbonden aan het meegezonden access_token niet toereikend voor de uitvoering van het subscription request.		Een Status-Code 403 conform HTTP specificatie en een `WWW-Authenticate` HTTP response header met als auth-scheme "`Bearer`" en een `error` attribuut met waarde "`insufficient_scop`". conform RFC 6750.
Subscription interface 4	Het subscription request mist een vereiste (header) parameter, bevat een niet-ondersteunde (header) parameter of parameterwaarde, gebruikt meer dan één methode voor het doorgeven van een access_token, of is op een andere wijze misvormd.		Een `Status-Code` 400 conform HTTP specificatie en een `WWW-Authenticate` HTTP response header met als auth-scheme "`Bearer`" en een `error` attribuut met waarde "`invalid_request`". conform RFC 6750.
Subscription interface 5	De *Subscription Server* detecteert dat niet kan worden voldaan aan de beschikbaarheidsvoorwaarde. Zie ook de toelichting op Beschikbaarheids- en ontvankelijkheidsvoorwaarde.		Een Status-Code 403 conform HTTP specificatie en een `WWW-Authenticate` HTTP response header met als auth-scheme "`Bearer`" en een `error` attribuut met waarde "`access_denied`". conform RFC 6750. Het vereiste error attribuut is bewust in lijn gebracht met het gedrag van de

					Authorization Server b deze uitzonderingssituatie.
	Subscription interface 6		*Subscription Server* ontvangt een correct verzoek dat op basis van door de *Aanbieder* ingesteld beleid geweigerd wordt.		Een Status-Code 422 Aanvraag kan niet verwerkt worden" conform HTTP specificatie.
	Subscription interface 7		*Subscription Server* ontvangt een correct verzoek dat echter verwijst naar een niet bestaand Abonnement (subscription-id).		Een Status-Code 404 Niet gevonden" conform HTTP specificatie.
	Subscription interface 8		*Subscription Server* kan in de request niet, niet geheel of niet tijdig voorzien, om redenen anders dan in bovengenoemde uitzonderingen.		Een toepasselijke Status-Code conform HTTP specificatie.

Subscription notification interface

Het subscription notification interface hoort bij de hoofdfunctie *Regie*, terwijl het resource notification interface bij de hoofdfunctie *Uitwisseling* hoort.

1. De *Notification Client* en de *Notification Server* maken op de subscription notification interface gebruik va

2. De *Notification Client* verstuurt de subscription notification middels een HTTP POST van een *Notification List* aangetroffen *Subscription Notification Endpoint*.

3. De subscription notification hanteert de structuur: <base uri>/Notification (zonder andere parameters in

4. Voor *Notificaties* en foutmeldingen op het subscription notification interface gebruiken *Notification Client* e formaat JSON.

5. De drie parameters in de subscription notification worden als volgt gevuld.

parameter	vulling	toelichting
`subscription_id`	De waarde waarmee de *Subscription Server* dit *Abonnement* in de subscription response heeft geïdentificeerd.	Een gebeurteni theoretisch leid *Notificaties*. Ied bij precies één
`notification_type`	De letterlijke waarde `subscription`.	Zo kan de *Notif* subscription no notification ond
`end_date`	De datum waarop het *Abonnement* afloopt en wordt beëindigd door de *Aanbieder*. Als deze waarde gelijk of kleiner is als de huidige (systeem)datum, dan is het *Abonnement* al beëindigd. In alle andere gevallen is deze waarde niet groter dan de huidige datum plus de maximale duur op basis van de *Abonnementen*-administratie van de *Subscription Server*.	*Abonnementen Aanbieder* als d *persoon* worde door *Dienstverl* de subscription door *Aanbieder* Subscription no Met de mogelijk *Aanbieder* in ge beschikbaarhei kunnen uitvoere

6. De enige parameter van de subscription notification response wordt als volgt gevuld.

parameter	vulling	toelichting
`notification_id`	identificatie waarmee de *Notification Server* de *Notificatie* uniek voor dit *Abonnement* identificeert	Dit kan bijvoorbeeld een integer maar kan ook volgens een ande gevuld.

7. Na ontvangst van een subscription notification, zal de *Notification Server*, indien in antwoord daarop een s response dient te worden gedaan, na maximaal tien (10) seconden dit antwoord ter beschikking stellen aa gedrag van de *Notification Server* is gedurende minimaal 98,5% van de tijd beschikbaar.

8. *Notification Server* en *Notification Client* handelen uitzonderingssituaties inzake het subscription notificati onderstaande tabel.

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Ver
Subscription notification interface 1	Notificeren 1	*Notification Server* vindt de ontvangen *Notification* ongeldig.	*Notification Server* informeert *Notification Client* over deze uitzondering.	Conform HTTP specificatie met met status code 400 "Foute aanvraag", en met in de body de van toepassing zijnde error code ("`invalid_subscription_id`", "`invalid_notification_type`" of "`invalid_duration`")	Alle onm te z Wa een inv " on *Abo* beë hier sub stur
Subscription notification interface 2	Notificeren 2	*Notification Server* kan in de request niet, niet geheel of niet tijdig verwerken.	*Notification Server* informeert *Notification Client* over deze uitzondering.	Conform HTTP specificatie met met status code 500 "Interne serverfout"	Alle onm te z

Resource notification interface

Het resource notification interface hoort de hoofdfunctie *Uitwisseling*, terwijl het subscription notification interface bij de hoofdfunctie *Regie* hoort.

1. De *Notification Client* en de *Notification Server* maken op het resource notification interface gebruik van H

2. De *Notification Client* verstuurt de resource notification middels een HTTP POST van een *Notification* op aangetroffen *Subscription Notification Endpoint*.

3. De resource notification hanteert de structuur: <base uri>/Notification (zonder andere parameters in de U

4. Voor *Notificaties* en foutmeldingen op het resource notification interface gebruiken *Notification Client* en d JSON.

5. De twee parameters in de resource notification worden als volgt gevuld.

parameter	vulling	toelichting
`subscription_id`	De waarde waarmee de *Subscription Server* dit *Abonnement* in de subscription response heeft geïdentificeerd.	Een gebeurtenis bij een *Aan* meerdere *Notificaties*. Iedere precies één *Abonnement*.
`notification_type`	De letterlijke waarde `resource`.	Zo kan de *Notification Serve* subscription notification onde

   Hier is niet, zoals in de subscription notification, een `end_date` opgenomen, omdat dat bij de hoofdfu over de Abonnementen-administratie vindt geheel plaats op het subscription notification interface. Het alleen voor inhoudelijke notificaties. Mogelijk zal in toekomstige releases van het MedMij Afsprakenste ook een nadere indicatie worden opgenomen van het onderdeel van de Gegevensdienst waarop er ni

6. De enige parameter van de resource notification response wordt als volgt gevuld.

parameter	vulling	toelichting
`notification_id`	identificatie waarmee de *Notification Server* de *Notificatie* uniek voor dit *Abonnement* identificeert	Het `id` kan bijvoorbeeld een int maar kan ook volgens een and gevuld.

7. Een *Notification Client* plaats binnen één (1) uur na het beschikbaar komen van nieuwe (gezondheids)inf betreffende die *Gegevensdienst*, een resource notification dienaangaande bij de betreffende *Notification*

   Als het tijdstip van beschikbaar komen van nieuwe (gezondheids)informatie wordt het moment gezien namens verwerkingsverantwoordelijke *Aanbieder* (handmatig of automatisch) als "beschikbaar voor *P*

8. Na ontvangst van een resource notification, zal de *Notification Server*, indien in antwoord daarop een res te worden gedaan, na maximaal tien (10) seconden dit antwoord ter beschikking stellen aan de *Notificatic Notification Server* is gedurende minimaal 98,5% van de tijd beschikbaar.

9.

Notification Server en *Notification Client* handelen uitzonderingssituaties inzake het resource notification i onderstaande tabel.

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding
Resource notification interface 1	Notificeren 1	*Notification Server* vindt de ontvangen resource notification ongeldig.	*Notification Server* informeert *Notification Client* over deze uitzondering.	Conform HTTP specificatie met met status code 400 "Foute aanvraag", en met in de body de van toepassing zijnde error code ("`invalid_subscription_id`" of "`invalid_notification_type`")
Resource notification interface 2	Notificeren 2	*Notification Server* kan in de request niet, niet geheel of niet tijdig verwerken.	*Notification Server* informeert *Notification Client* over deze uitzondering.	Conform HTTP specificatie met met status code 500 "Interne serverfout"

Extensie Vertegenwoordiging

1. Inleiding

Een vertegenwoordiging houdt in dat de ene persoon (de *Vertegenwoordigde*) zich laat vertegenwoordigen door een andere persoon (de *Vertegenwoordiger*). Met de juiste machtigingen mag een Vertegenwoordiger rechtshandelingen uitvoeren namens de Vertegenwoordigde. Zonder machtiging kan vertegenwoordiging niet plaatsvinden. Binnen het huidige afsprakenstelsel van MedMij betekent dit dat machtigingen gegeven kunnen worden voor het uitvoeren van de functie *Verzamelen*.

Iemand kan op basis van een wettelijke grondslag zijn gemachtigd, zoals gezaghebbende ouder(s) of voogd voor kinderen onder de 12 jaar of op basis van een vrijwillig afgegeven machtiging. Het gebruik van vrijwillig afgegeven machtigingen is bijvoorbeeld noodzakelijk om mantelzorgers hun taak goed uit te kunnen laten voeren in de langdurige zorg.

In deze versie van het afsprakenstelsel richt *Vertegenwoordiging* zich alleen op de functie Verzamelen en alleen voor vrijwillige vertegenwoordiging. De *Vertegenwoordigde* machtigt de *Vertegenwoordiger* voor het verzamelen van alle gezondheidsgegevens die op *Vertegenwoordigde* van toepassing zijn.

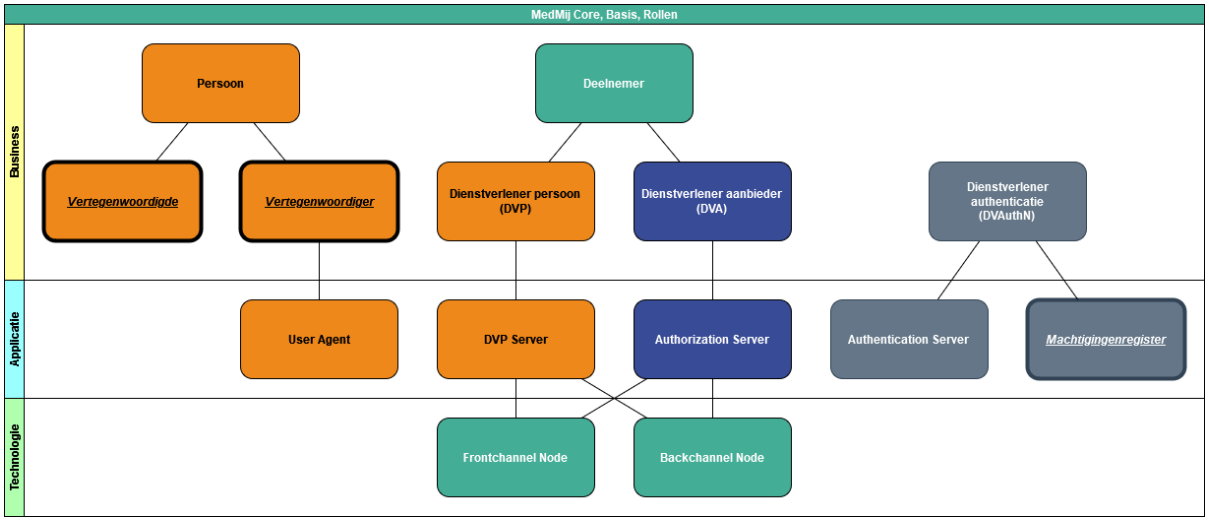
Deze extensie beschrijft nieuwe rollen van de *Persoon* om ruimte maken voor zulke machtigingen. Vrijwillige vertegenwoordiging wordt in het *Persoonsdomein* en het *Aanbiedersdomein*) ondersteund:

- *Dienstverleners persoon* ondersteunen vertegenwoordiging door de mogelijkheid aan te bieden om informatie van een andere Persoon te verzamelen of te delen. Hiervoor wordt gebruikgemaakt van het *Dossier* van de vertegenwoordigde, waarop *Vertegenwoordiger* een account krijgt.
- *Dienstverleners aanbieder* kunnen vertegenwoordiging ondersteunen, door gebruik te maken van uitgegeven machtigingen. Deze machtigingen worden verkregen uit een machtigingenregister.

Hoewel vertegenwoordiging ruimte biedt aan *Deelnemers* voor het gebruiken van machtigingsfunctionaliteit of anderszins ontkoppelen van *Vertegenwoordigers* en *Vertegenwoordigden,* neemt het MedMij Afsprakenstelsel hierover geen expliciete verantwoordelijkheden op, behalve waar deze nieuwe ruimte risico’ s inzake vertrouwen en gegevensintegriteit met zich mee kunnen brengen.

> Deze extensie is beschreven als optionele functionaliteit die geen impact heeft op de interoperabiliteit tussen deelnemers die dit (nog) niet ondersteunen. Het is daarom ook nog geen onderdeel van het acceptatieproces.

2. Rollen



Als er sprake is van vertegenwoordiging dan worden de rollen uit de Core uitgebreid.

Persoon kan bij vertegenwoordiging één van twee rollen hebben:

- Vertegenwoordiger, die informatie uitwisselt via een PGO, of
- Vertegenwoordigde, waarop de informatie betrekking heeft.

Als een *Persoon* informatie ophaalt dat betrekking heeft op de *Persoon* zelf, dan is er geen sprake van vertegenwoordiging. Bij vertegenwoordiging zijn altijd twee *Personen* betrokken, waarbij de ene persoon informatie uitwisselt die betrekking heeft op een andere persoon. Eén *Persoon* kan Vertegenwoordiger zijn voor één of meerdere vertegenwoordigden. Vertegenwoordiging is op basis van een Machtiging die is geregistreerd in het *Machtigingenregister*.

3. Functies en gegevens

In de stroomdiagrammen van de functie *Verzamelen* is vertegenwoordiging toegevoegd:

- De flow van de usecase verzamelen;
- De implementatie van de usecase verzamelen;
- De implementatie van het front- en backchannelverkeer.

De stroomdiagrammen tonen alleen de situatie waarin alle acties slagen tot en met het uiteindelijke verzamelen van de gezondheidsinformatie (de zogenaamde happy flow). De oranje banen horen, conform de MedMij-huisstijl tot het Persoonsdomein, de blauwe tot het Aanbiedersdomein.

4. Verantwoordelijkheden

De verantwoordelijkheden die in de MedMij Core staan beschreven, zijn ook van toepassing op deze extensie. Daarnaast gelden de hieronder (vervangende) verantwoordelijkheden. Net als in de MedMij Core zijn de volgende kleuren voor de verantwoordelijkheden op de verschillende lagen gebruikt:

- Geel voor de businesslaag;
- Blauw voor de applicatielaag;
- Groen voor de technologielaag.

5. Begrippen met betrekking tot vertegenwoordiging

Ten behoeve van machtigen zijn de volgende begrippen toegevoegd:

Term	Definitie	Toelichting	Synoniem
Gemachtigde	Een partij die op grond van een Machtiging de bevoegd verkrijgt om in naam van de Machtigingsverlener (lees: *Vertegenwoordigde*) bepaalde handelingen te verrichten waarvan de rechtsgevolgen worden toegerekend aan de Machtigingsverlener (lees: *Vertegenwoordigde*).		Vertegenwoordiger
Ketenmachtiging	De situatie waarin meer dan één machtigingsrelatie gebruikt moet worden om aan te tonen dat degene die een bepaalde dienst wil afnemen daartoe bevoegd is namens een eerste Machtigingsverlener. De ene zijde van deze keten wordt gevormd door de eerste Machtigingsverlener. De andere zijde van de keten wordt gevormd door de (laatste) Gemachtigde die degene is die de handeling uitvoert.		
Machtiging	De vertegenwoordigingsbevoegdheid die de Machtigingsverlener (lees: *Vertegenwoordigde*) verleent aan een ander (de Gemachtigde) om namens / in naam van de Machtigingsverlener (lees: *Vertegenwoordigde*), bepaalde Rechtshandelingen te verrichten. Met de term Machtiging wordt de juridische vertegenwoordigingsbevoegdheid bedoeld zoals deze tussen partijen wordt afgesproken en niet de registratie daarvan die daarna in een Machtigingsregister wordt vastgelegd.	De term kan zowel betrekking hebben op één machtigingsrelatie als op een geheel dat bestaat uit een keten van machtigingsrelaties waarbij de ene gemachtigde optreedt als machtigingsverlener van de volgende. Dit volgt uit het recht op substitutie (art. 3:64 BW) Substitutie is het recht van een gemachtigde om de aan hem verleende volmacht door te geven aan een ander. Dit recht moet door de machtigingsverlener worden verleend. Vervolgens kan de hoofdgemachtigde. Op grond van dit recht op	Volmacht

		substitutie, de machtiging doorgeven aan de substituut gemachtigde. We hebben het hier dan over Ketenmachtiging.	
Machtigingsregister	Een partij die de verantwoordelijkheid heeft voor het registreren, beheren, controleren van machtigingen en andere bevoegdheden en het afleggen van verklaringen over bevoegdheden (c.q. het op verzoek van de handelende natuurlijk persoon verstrekken van machtigingsverklaringen).	Uitgangpunten volmacht: 1.Volmacht De volmacht zelf is een eenzijdige gerichte rechtshandeling van de machtigingsverlener (3: 60 BW) waarbij aan de gemachtigde de bevoegdheid wordt verleend om binnen de gestelde grenzen namens hem rechtshandelingen te verrichten. Is een volmacht aan twee op meer personen tezamen verleend, dan is ieder van hen bevoegd zelfstandig te handelen, tenzij anders bepaald. (zie ook 3:60, 3:65 en 3: 66 BW). Het rechtsgevolg is gelegen in het verrichten van een rechtshandeling. 2.Vormvereiste De wijze waarop een volmacht wordt verleend is niet aan vormvereisten gebonden. Een volmacht kan uitdrukkelijk of stilzwijgend worden verleend (artikel 3:61 BW). De volmacht kan bijvoorbeeld blijken uit een verklaring van de machtigingsverlener, een geschrift of de onderlinge rechtsverhouding zoals een arbeidsovereenkomst.	

		3.Rechtsgevolg De machtigingsverlening heeft rechtsgevolg op het moment dat zij ter kennis komt van de gemachtigde. De gemachtigde hoeft de machtiging niet te aanvaarden. Wel geldt dat als de gemachtigde de volmacht beëindigt, de volmacht eindigt. Zie ook 3:37 lid 3 en 3:73 BW. 4.Einde De volmacht eindigt tevens door herroeping van de machtigingsverlener, de dood, curatele, faillissement of schuldsanering van de machtigingsverlener of de gemachtigde. Zie voor beëindiging van de volmacht ook artikel 3: 72 BW 5.Kenbaarheid Artikel 3:60 en 3:61 BW bepalen niet hoe de gemachtigde kenbaar moet maken dat hij namens de machtigingsverlener handelt. 6. Handelingsbevoegdheid machtigingsverlener De machtigingsverlener blijft naast de gemachtigde te allen tijde bevoegd om zelf te handelen. 7.Bewijs Artikel 3:71 BW behelst aanwijzingen voor bewijsvoering van een	

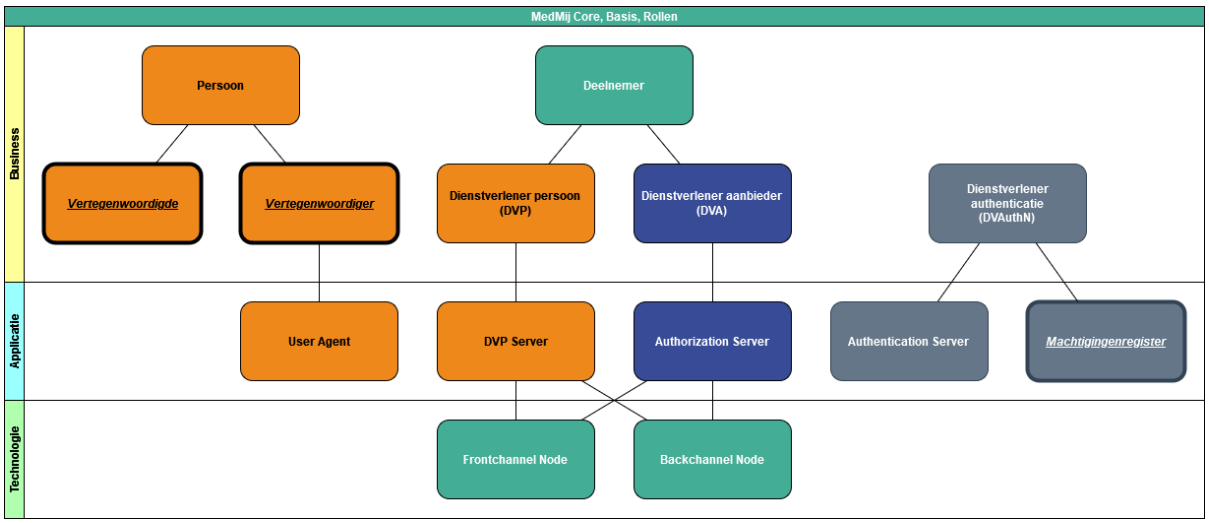
		machtiging. Het betreft de verklaring van de gemachtigde, een geschrift of een bevestiging van de machtigingsverlener. Deze verklaring kan door de wederpartij van de hand worden gewezen als niet bij verzoek om bewijs van de volmacht een geschrift wordt overlegd waaruit de volmacht volgt, dan wel een bevestiging van de machtigingsverlener volgt. 8.Handelingsbevoegd Voor de beantwoording van de vraag of de gemachtigde in de hoedanigheid van gemachtigde namens de machtigingsverlener binnen de grenzen van de bevoegdheid is opgetreden, is bepalend wat partijen over en weer hebben verklaard en redelijkerwijs uit deze verklaring hebben afgeleid en mochten afleiden. 9.Bekrachtiging Wanneer iemand zonder daartoe gemachtigd te zijn namens een ander heeft gehandeld, kan laatstgenoemde de rechtshandeling bekrachtigen waardoor deze toch tot stand komt. Zie ook artikel 3: 69 BW.	
Machtigingsverlener	Een partij (lees: *Persoon*) die een (specifieke) machtiging verleent aan een andere partij (de gemachtigde).		Vertegenwoordigde, Betroffene, Belanghebbende
Opgever	De handelend natuurlijke persoon		

	die opgave doet aan een Machtigingsregister van een verleende machtiging zodat deze gebruikt kan worden en de voor deze registratie vereiste bewijzen aanlevert.		
Substitutie	Het door de Gemachtigde doorgeven van zijn machtiging aan een ander.	Het uitgangspunt van het recht op substitutie is dat dit recht door de machtigingsverlener aan de gemachtigde moet worden verleend. Vervolgens kan de hoofdgemachtigde, op grond van dit recht op substitutie, de machtiging doorgeven aan de substituut gemachtigde. De substituut machtiging kan zowel aan een natuurlijk persoon als aan een onderneming of rechtspersoon worden verleend. Evenals bij een volmacht blijft bij een substitutie, de machtigingsverlener bevoegd de rechtshandelingen te verrichten waarvoor de volmacht is verleend. De bevoegdheid om zelf te handelen blijft ook voor de hoofdgemachtigde bestaan. Dit is slechts anders als tussen partijen is overeengekomen dat de machtigingsverlener voor de duur van die overeenkomst zelf niet meer bevoegd is de betreffende rechtshandelingen te verrichten.	
Vertegenwoordigde	Zie Machtigingsverlener		
Vertegenwoordiger	Zie Gemachtigde		
Vertegenwoordiging	De rechtsfiguur die inhoudt dat van een door een bepaalde partij	De bevoegdheid tot het verrichten van	

	(de vertegenwoordiger of gemachtigde) in naam van een andere partij (vertegenwoordigde of machtigingsverlener) met een derde een verrichte Rechtshandeling aan de vertegenwoordigde wordt toegerekend.	Vertegenwoordiging vloeit voort uit volmacht (privaatrecht Boek 3, Titel 3 Burgerlijk Wetboek (BW) of een Machtiging (bestuursrecht Hoofdstuk 2, afdeling 2.1 Algemene Wet Bestuursrecht). Machtiging kan worden gezien als een synoniem aan volmacht zij het dat de term machtiging voornamelijk in bestuursrechtelijke context wordt gebruikt. Een Rechtshandeling is een op rechtsgevolg gerichte wil die zich door een verklaring heeft geopenbaard (3:33 BW).	
Volmacht	De bevoegdheid die een volmachtgever (lees: *Vertegenwoordigde*) verleent aan een ander, de gevolmachtigde, om namens hem / in zijn naam rechtshandelingen te verrichten.		Machtiging

Rollen, Vertegenwoordiging

1. Rollenmodel



Als er sprake is van vertegenwoordiging dan worden de rollen uit de Core uitgebreid.

Persoon kan bij vertegenwoordiging één van twee rollen hebben:

- Vertegenwoordiger, die informatie uitwisselt via een PGO, of
- Vertegenwoordigde, waarop de informatie betrekking heeft.

Als een *Persoon* informatie ophaalt dat betrekking heeft op de *Persoon* zelf, dan is er geen sprake van vertegenwoordiging. Bij vertegenwoordiging zijn altijd twee *Personen* betrokken, waarbij de ene persoon informatie uitwisselt die betrekking heeft op een andere persoon. Eén *Persoon* kan Vertegenwoordiger zijn voor één of meerdere vertegenwoordigden. Vertegenwoordiging is op basis van een Machtiging die is geregistreerd in het *Machtigingenregister*.

2. Roldefinities

2.1. Business

- Vertegenwoordigde
  - Een *Persoon* die een (specifieke) machtiging verleent aan een andere partij (de gemachtigde).
- Vertegenwoordiger
  - Een *Persoon* die op grond van een *Machtiging* de bevoegdheid verkrijgt om in naam van de *Vertegenwoordigde* bepaalde handelingen te verrichten waarvan de rechtsgevolgen worden toegerekend aan de *Vertegenwoordigde*.
  - Een partij die op grond van een *Machtiging* de bevoegdheid verkrijgt om in naam van de Machtigingsverlener (lees: *Vertegenwoordigde*) bepaalde handelingen te verrichten waarvan de rechtsgevolgen worden toegerekend aan de Machtigingsverlener (lees: Persoon).

2.2. Applicatie

- Machtigingenregister

- Een partij die de verantwoordelijkheid heeft voor het registreren, beheren, controleren van machtigingen en andere bevoegdheden en het afleggen van verklaringen over bevoegdheden (c.q. het op verzoek van de handelende natuurlijk persoon verstrekken van machtigingsverklaringen).

Functies en gegevens, Vertegenwoordiging

1. Inleiding

In de stroomdiagrammen van de functie *Verzamelen* is vertegenwoordiging toegevoegd:

- De flow van de usecase verzamelen;
- De implementatie van de usecase verzamelen;
- De implementatie van het front- en backchannelverkeer.

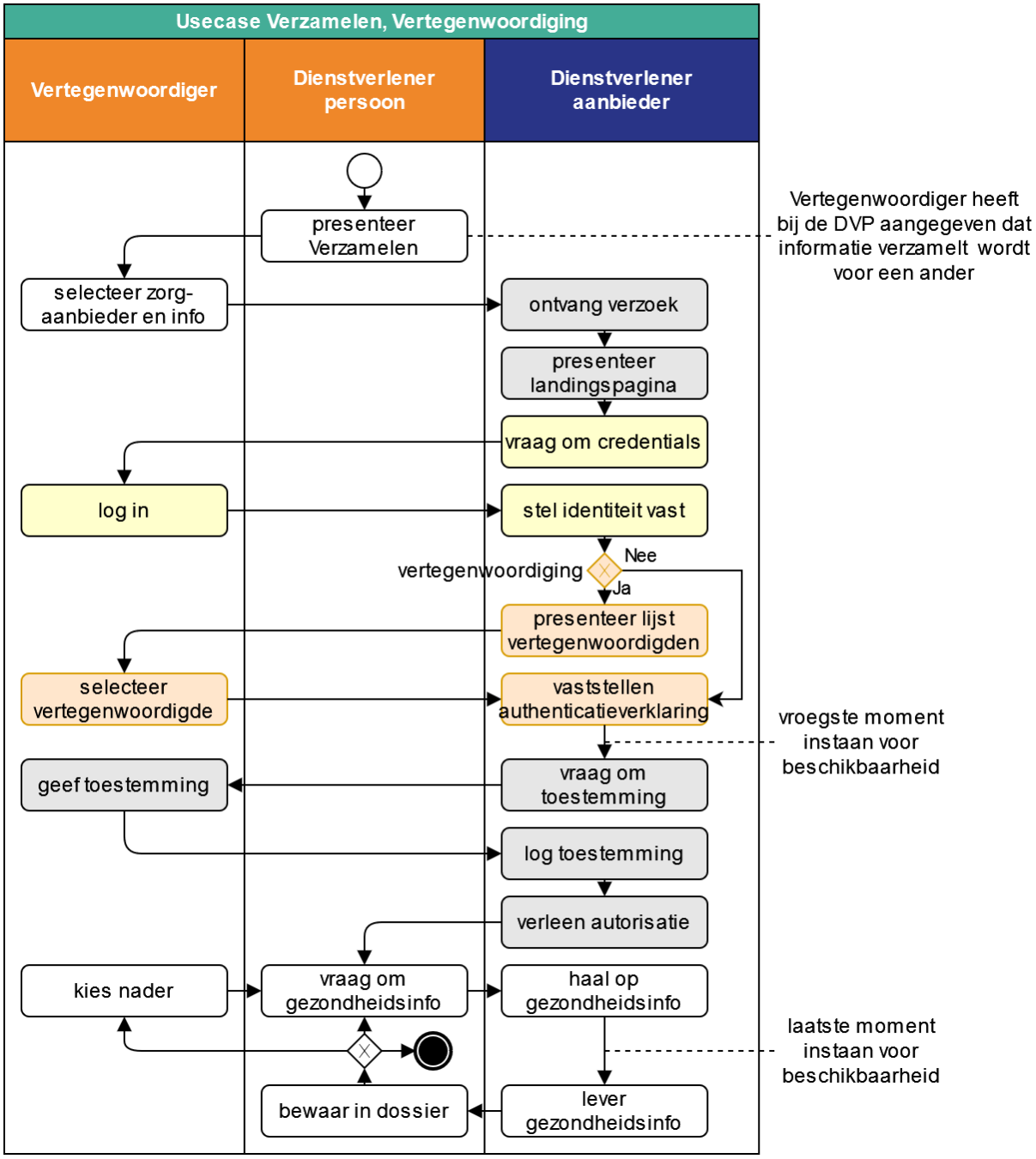
De stroomdiagrammen tonen alleen de situatie waarin alle acties slagen tot en met het uiteindelijke verzamelen van de gezondheidsinformatie (de zogenaamde happy flow). De oranje banen horen, conform de MedMij-huisstijl tot het Persoonsdomein, de blauwe tot het Aanbiedersdomein.

2. Usecase Verzamelen

De acties in het stroomdiagram zijn soms gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow; de zachtgeel gekleurde acties vormen samen de authenticatieflow; de oranje gekleurde acties zijn toegevoegd ten behoeve van vertegenwoordiging.

Omdat het stroomdiagram alleen de happy flow bevat, zijn daarna de uitzonderingen beschreven.

2.1. Stroomdiagram



2.2. Toelichting

De uitbreiding op het stroomdiagram van de functie *Verzamelen*, ten behoeve van vertegenwoordiging, is in oranje aangegeven. De extra stappen zijn:

- De *Persoon* geeft bij starten van de flow aan of hij informatie wil verzamelen van zichzelf of voor een ander. In het laatste geval is er sprake van vertegenwoordiging en is de Persoon dus de *Vertegenwoordiger*
- De *Dienstverlener aanbieder* laat de *Vertegenwoordiger* na authenticatie de *Vertegenwoordigde* selecteren
- De Dienstverlener aanbieder stelt de authenticatieverklaring vast

De rest van de flow is gelijk aan de oorspronkelijke usecase Verzamelen.

2.3. Uitzonderingen

Naast de uitzonderingen die beschreven zijn in de usecase Verzamelen zijn er specifieke uitzonderingen in relatie tot vertegenwoordigen:

Of de *Aanbieder* de gevraagde gezondheidsinformatie beschikbaar stelt aan de *Vertegenwoordiger*, is om te beginnen een zaak tussen de *Aanbieder* en *Vertegenwoordigde*, die daarvoor een behandelrelatie moeten hebben of hebben gehad. Gegeven zo'n behandelrelatie is er wetgeving van toepassing op deze ter beschikkingstelling. Daarbinnen is eigen beslisruimte voor de *Aanbieder*. Omdat *Aanbieder* en *Vertegenwoordigde* evenwel geen *Deelnemers* in het MedMij Afsprakenstelsel zijn, specificeert het MedMij Afsprakenstelsel niet de exacte logica van de beslissing om de gezondheidsinformatie al dan niet ter beschikking te stellen. Om privacy-redenen vereist het MedMij Afsprakenstelsel echter wel dat er een behandelrelatie moet (hebben) bestaan waarbij de betreffende gezondheidsinformatie hoort én dat de *Vertegenwoordigde* minstens zestien jaar oud is (zie uitzondering Verzamelen 3). De *Vertegenwoordiger* vertegenwoordigt *Vertegenwoordigde* op basis van een machtiging. De *Aanbieder* valideert de machtiging.

De machtiging kan gezien worden als onderdeel van de beschikbaarheidsvoorwaarde.

Er zijn verschillende combinaties te maken van ondersteuning van vertegenwoordiging, die impact hebben op het verloop van de flow. Deze staan uitgewerkt in onderstaand diagram

		Dienstverlener aanbieder	
		Geen gebruik vertegenwoordiging	Vertegenwoordiging
Dienstverlener persoon	Geen gebruik vertegenwoordiging	Geen vertegenwoordiging	Dienstverlener aanbieder mag geen vertegenwoordiging aanbieden en breekt de flow af
	Vertegenwoordiging	Dienstverlener persoon biedt geen verantwoordelijkheid aan of stopt de flow af.	Vertegenwoordiging

1. *Dienstverlener persoon* en *Dienstverlener aanbieder* ondersteunen vertegenwoordiging: reguliere flow voor vertegenwoordiging
2. *Dienstverlener aanbieder* ondersteunt geen vertegenwoordiging: Vertegenwoordiging wordt afgebroken door *Dienstverlener persoon*. Om vermenging van gegevens tegen te gaan, mogen geen gegevens verzamelt worden.

3. *Dienstverlener persoon* ondersteunt geen vertegenwoordiging: Vertegenwoordiging wordt niet gestart door *Dienstverlener persoon.* Als, om welke reden dan ook, toch bij de *Authentication Server* gekozen wordt voor Vertegenwoordiging, wordt de flow afgebroken door *Dienstverlener aanbieder*. Om vermenging van gegevens tegen te gaan, mogen geen gegevens verzamelt worden.
4. *Dienstverlener persoon* en *Dienstverlener aanbieder* ondersteunen geen vertegenwoordiging: Vertegenwoordiging wordt niet gestart.

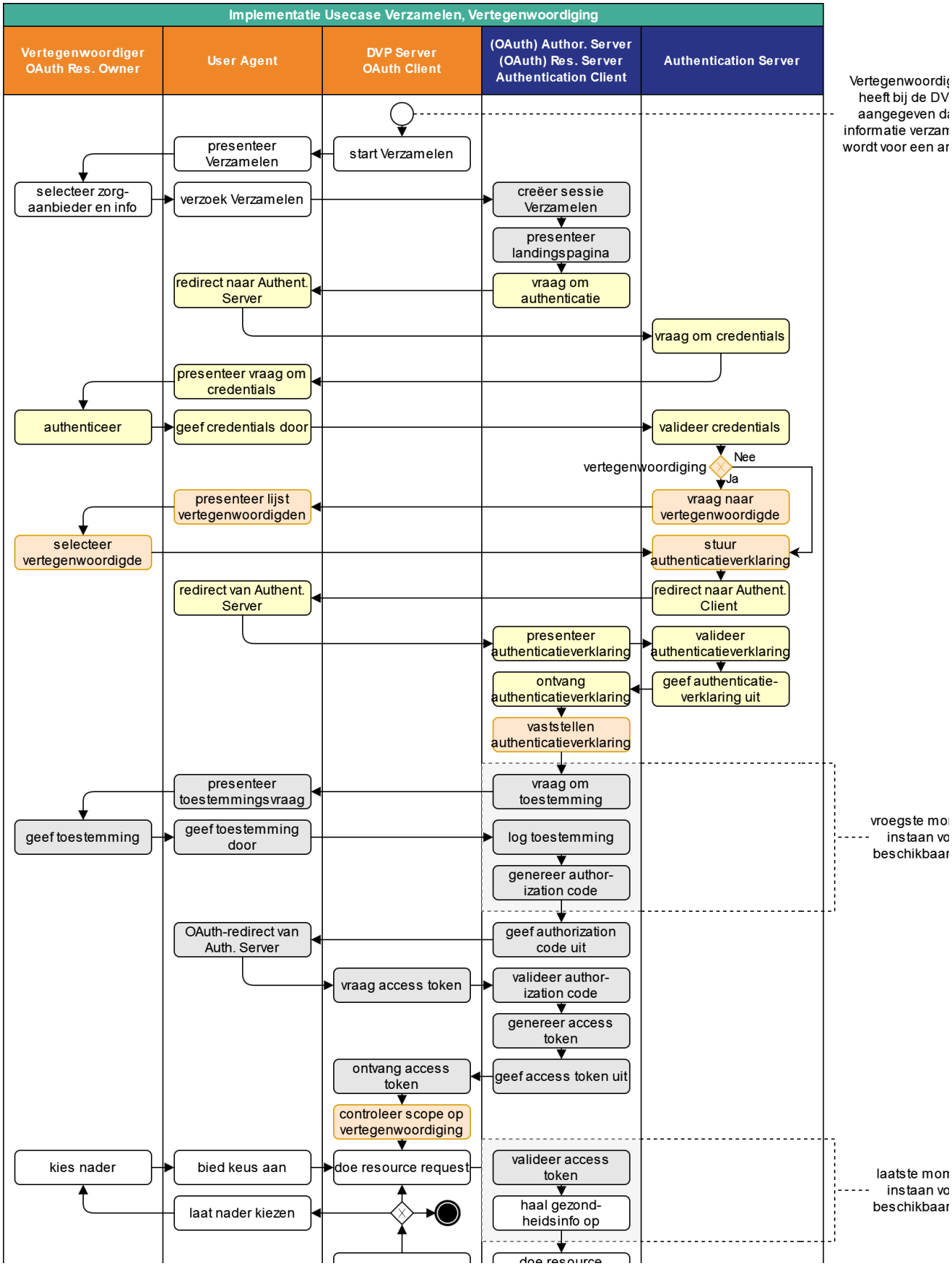
nr.	uitzondering	actie	vervolg
Verzamelen Vert 1	*Dienstverlener aanbieder* kan de identiteit van de *Vertegenwoordigde* niet vaststellen.	*Dienstverlener aanbieder* informeert *Dienstverlener persoon* dat verzoek niet wordt ingewilligd.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
Verzamelen Vert 2	*Dienstverlener aanbieder* kan de machtiging niet vaststellen		
Verzamelen Vert 3	*Dienstverlener aanbieder* ondersteunt geen vertegenwoordiging	*Dienstverlener persoon* biedt geen vertegenwoordiging aan, of breekt de flow af zodra duidelijk is dat in het *Aanbiedersdomein* geen vertegenwoordiging gebruikt is.	
Verzamelen Vert 4	*Aanbieder* - gegevensdienst combinatie ondersteunt geen vertegenwoordiging		*Dienstverlener persoon* stopt de flow.
Verzamelen Vert 5	*Dienstverlener persoon* ondersteunt geen vertegenwoordiging	*Dienstverlener aanbieder* biedt geen vertegenwoordiging aan, of breekt de flow af zodra duidelijk is dat bij de *Authentication Server* vertegenwoordiging gebruikt is.	*Dienstverlener aanbieder* stopt de flow.

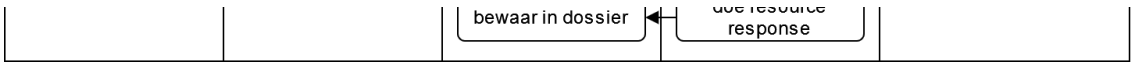
3. Implementatie usecase Verzamelen

Menige actie in het stroomdiagram is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow volgens OAuth 2; de zachtgeel gekleurde acties vormen samen de authenticatieflow. Deze kleuren verwijzen dus alleen maar naar de gebruikte standaarden en zeggen niets over welke component de stap zou moeten uitvoeren. Authenticatie is dus ingebed in autorisatie. Aan het oorspronkelijke diagram zijn in oranje de acties toegevoegd ter ondersteuning van vertegenwoordiging.

Verantwoordelijkheden inzake uitzonderingen op de happy flow zijn opgenomen bij de respectievelijke interface, waar de uitzonderingen bij de usecases zijn genoemd.

3.1. Stroomdiagram


Implementatie Usecase Verzamelen, Vertegenwoordiging
Vertegenwoordiger OAuth Res. Owner
User Agent
DVP Server OAuth Client
(OAuth) Author. Server (OAuth) Res. Server Authentication Client
Authentication Server
start Verzamelen
presenteer Verzamelen
selecteer zorg-aanbieder en info
verzoek Verzamelen
creëer sessie Verzamelen
presenteer landingspagina
vraag om authenticatie
redirect naar Authent. Server
vraag om credentials
presenteer vraag om credentials
authenticeer
geef credentials door
valideer credentials
vertegenwoordiging
Nee
Ja
presenteer lijst vertegenwoordigden
vraag naar vertegenwoordigde
selecteer vertegenwoordigde
stuur authenticatieverklaring
redirect van Authent. Server
redirect naar Authent. Client
presenteer authenticatieverklaring
valideer authenticatieverklaring
ontvang authenticatieverklaring
geef authenticatie-verklaring uit
vaststellen authenticatieverklaring
presenteer toestemmingsvraag
vraag om toestemming
geef toestemming
geef toestemming door
log toestemming
genereer author-ization code
OAuth-redirect van Auth. Server
geef authorization code uit
vraag access token
valideer author-ization code
genereer access token
ontvang access token
geef access token uit
controleer scope op vertegenwoordiging
kies nader
bied keus aan
doe resource request
valideer access token
laat nader kiezen
haal gezond-heidsinfo op
Vertegenwoordig
heeft bij de DV
aangegeven da
informatie verzam
wordt voor een ar
vroegste mo
instaan vo
beschikbaar
laatste mon
instaan vo
beschikbaar



In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De flow kent de volgende stappen:

1. De *DVP Server* start de flow door in de *User Agent* van de *Persoon (*als *Vertegenwoordiger)* de mogelijkheid te presenteren om gezondheidsinformatie van een andere *Persoon* (als *Vertegenwoordigde*) te verzamelen.
2. De *DVP Server* presenteert in de *User Agent* van de *Vertegenwoordiger* de mogelijkheid om één of meerdere *Gegevensdiensten* bij een zekere *Aanbieder* te verzamelen. Uit de *Aanbiederslijst* weet de *DVP Server* welke *Gegevensdiensten* door een *Aanbieder* aangeboden worden. Desgewenst worden de *Gegevensdienstnamen* uit de *Gegevensdienstnamenlijst* gebruikt.
3. De *Vertegenwoordiger* maakt expliciet zijn selectie en laat de *User Agent* een authorization request sturen naar de *Authorization Server*. Het adres van het authorization endpoint komt uit de *Aanbiederslijst*. De `redirect_uri` geeft aan waarnaartoe de *Authorization Server* de *User Agent* verderop moet redirecten (met de authorization code). Het authorization request mag desgewenst, onder voorwaarden, meerdere *Gegevensdiensten* van de *Aanbieder* bevatten. Omdat gekozen is voor vertegenwoordiging moet de authorization request ook de indicatie voor vertegenwoordiging bevatten.

   Toestemming voor meerdere Gegevensdiensten van een Aanbieder

   In een authorization request mogen meerdere *Gegevensdiensten* van eenzelfde *Aanbieder* worden gecombineerd wanneer:

   a. de gegevensdiensten worden aangeboden binnen één zelfde interfaceversie, EN
   b. de FQDN van de in de ZAL, voor deze gegevensdiensten, opgenomen AuthorizationEndpoints met elkaar overeenkomen, EN
   c. de FQDN van de in de ZAL, voor deze gegevensdiensten, opgenomen TokenEndpoints met elkaar overeenkomen.

4. Daarop begint de *Authorization Server* de OAuth-flow (in zijn rol als *OAuth Authorization Server*) door een sessie te creëren met de indicatie dat er sprake is van vertegenwoordiging.
5. De *Authorization Server* vraagt de *Vertegenwoordiger* via zijn *User Agent* in te loggen.
6. Dan start de *Authorization Server* (nu in de rol van *Authentication Client*) de authenticatieflow door de *User Agent* naar de *Authentication Server* te redirecten, onder meegeven van een `redirect_uri`, die aangeeft waarnaartoe de *Authentication Server* straks de *User Agent* moet terugsturen, na het inloggen van de *Vertegenwoordiger*.
7. De *Authentication Server* vraagt de *Vertegenwoordiger* via zijn *User Agent* om inloggegevens.
8. Wanneer deze juist zijn, dan vraagt de *Authentication Server* aan de *Vertegenwoordiger* om de *Vertegenwoordigde te selecteren*
9. Daarna redirect de *Authentication Server* de *User Agent* terug naar de *Authorization Server*, onder meegeven van een ophaalbewijs. Wanneer het inloggen is afgebroken geeft de *Authorization Server* de *Vertegenwoordiger* alsnog de mogelijkheid via zijn *User Agent* in te loggen.
10. Met dit ophaalbewijs haalt de *Authorization Server* rechtstreeks bij de *Authentication Server* de authenticatieverklaring op.
11. Dan breekt het vroegste moment aan waarop de *Authorization Server* ervoor instaat dat de *Aanbieder* voor de betreffende *Gegevensdienst(en)* überhaupt gezondheidsinformatie van die *V ertegenwoordigde* beschikbaar heeft, of anders de happy flow afbreekt. Daarvan maakt deel uit dat de *Vertegenwoordigde* daarvoor minstens 16 jaar oud moet zijn.
12. Indien de *Aanbieder* kan instaan voor de beschikbaarheid van tenminste één *Gegevensdienst*, of wanneer géén gebruik wordt gemaakt van dit vroegste moment, dan presenteert de *Authorization Server* via de *User Agent* aan *Vertegenwoordiger* in een *Toestemmingsverklaring*, de vraag of

Vertegenwoordigde de *Aanbieder* toestaat de gevraagde persoonlijke gezondheidsinformatie aan de *DVP Server* (als *OAuth Client*) te sturen. Indien op dit moment al bekend is dat een bepaalde *Gegevensdienst* niet beschikbaar is voor de *Vertegenwoordiger*, dan mag deze niet worden opgenomen in de *Toestemmingsverklaring*.

13. Bij akkoord logt de *Authorization Server* dit als toestemming, genereert een authorization code en stuurt dit als ophaalbewijs, door middel van een *User Agent* redirect met de in het authorization request ontvangen `redirect_uri`, naar de *DVP Server*. De *Authorization Server* stuurt daarbij de local state-informatie mee die hij in het authorization request van de *DVP Server* heeft gekregen. Laatstgenoemde herkent daaraan het verzoek waarmee hij de authorization code moet associëren.
14. De *DVP Server* vat niet alleen deze authorization code op als ophaalbewijs, maar leidt er ook uit af dat de toestemming is gegeven en logt het verkrijgen van het ophaalbewijs.
15. Met dit ophaalbewijs wendt de *DVP Server* zich weer tot de *Authorization Server*, maar nu zonder tussenkomst van de *User Agent*, voor een access token.
16. Daarop genereert de *Authorization Server* een access token en stuurt deze naar de *DVP Server*.
17. De *DVP Server* controleert de scope van de vertegenwoordiging. Hierbij zijn de volgende situaties mogelijk:
    a. De *DVP Server* stelt vast dat de scope van het access token geen onbehalfof bevat waar dit in de scope van het Authorization Request wel meegegeven was. *DVP Server* stopt de flow onmiddelijk.
    b. De *DVP Server* stelt vast dat de scope van het access token onbehalfof bevat waar dit in de scope van het Authorization Request niet meegegeven was. *DVP Server* stopt de flow onmiddelijk.

    > De *DVP Server* kan deze situaties alleen vaststellen als de *DVP Server* Vertegenwoordiging ondersteunt. Omdat deze extensie optioneel is voor alle deelnemers, kan de situatie zich voordoen dat de uitzondering wel van toepassing is, maar niet opgemerkt wordt door de *DVP Server*. Daarom heeft ook de Authorization Server de verantwoordelijkheid controles uit te voeren. Deze staan beschreven bij de Authorization interface.

18. Nu is de *DVP Server* gereed om één of meerdere verzoeken om de gezondheidsinformatie naar de *Resource Server* te sturen, nadat hij de *Vertegenwoordiger* eventueel nog nadere keuzes heeft laten maken. Het adres van de juiste resource endpoints haalt hij uit de *Aanbiederslijst*. Hij plaatst telkens het access token in het bericht en zorgt ervoor dat in het bericht geen BSN is opgenomen.
19. De *Resource Server* controleert bij ieder verzoek of het ontvangen token recht geeft op de gevraagde resources en haalt deze (al dan niet) bij achterliggende bronnen op. Dan breekt het uiterste moment aan waarop de *Resource Server* ervoor moet instaan dat voor de *Gegevensdienst* waartoe een verzoek behoort de *Aanbieder* de gezondheidsgegevens beschikbaar heeft. Is dat zo, dan verstuurt de *Resource Server* deze ze in een resource response naar de *DVP Server*.
20. De *DVP Server* bewaart de ontvangen gezondheidsinformatie in het persoonlijke dossier. De *DVP Server* bevraagt de *Resource Server* daarna mogelijk opnieuw, eventueel na nieuwe interactie met de *Vertegenwoordiger*. Zolang het access token geldig is, kan dat.

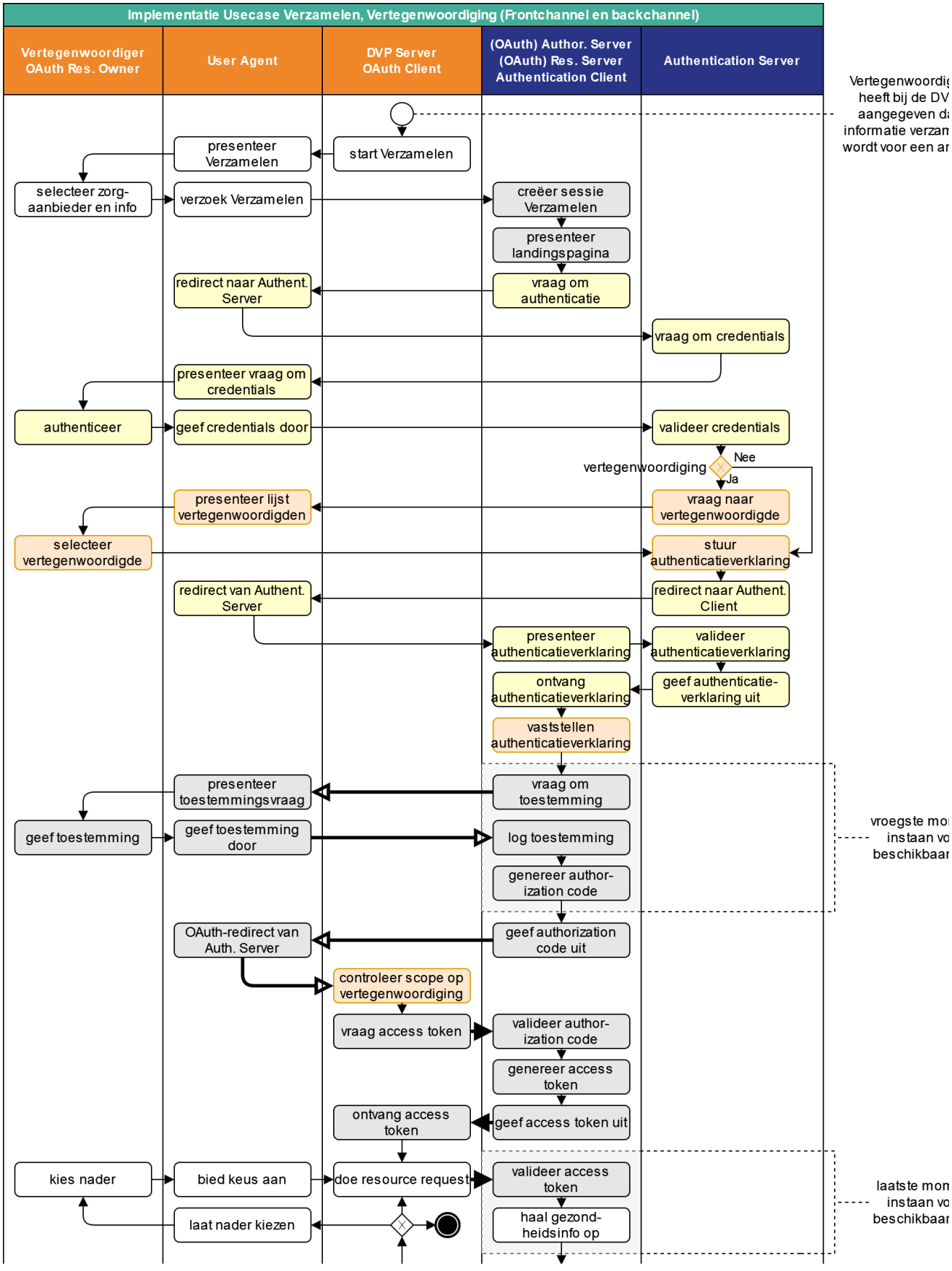
In de regel worden bij een eenmalig gebruik van *Verzamelen* het authorization interface, het token interface en het resource interface allemaal aangesproken, in die volgorde. Mocht de *DVP Server* echter nog beschikken over een nog niet verlopen access token voor de betreffende *Aanbieder-Gegevensdienst*-combinatie, dan kan het onmiddellijk het resource interface aanspreken.

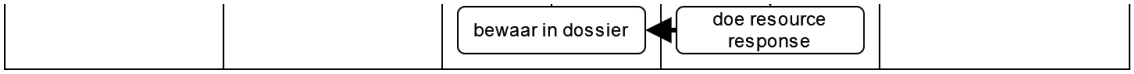
Het MedMij Afsprakenstelsel adviseert de beschikbaarheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. Vooralsnog staat het MedMij Afsprakenstelsel toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment.

Bij de implementatie van de voorwaarde op beschikbaarheid bij de *Aanbieder* voor de te verzamelen gezondheidsgegevens is het zaak rekening te houden met privacy-vereisten. Wanneer de *Dienstverlener aanbieder* ten behoeve van de beschikbaarheidsvoorwaarde nieuwe gegevensverzamelingen zou

aanleggen, vindt een verwerking altijd onder de verantwoordelijkheid van één *Aanbieder* plaats. Het combineren van verwerkingen of het onvoldoende segregeren moet worden vermeden. Afwijking hiervan is alleen mogelijk onder expliciete instructie van de *Aanbieder(s)* en vereist een zorgvuldige voorafgaande afweging, vanwege de daaraan verbonden privacyrisico's.

4. Implementatie van het front- en backchannelverkeer


Implementatie Usecase Verzamelen, Vertegenwoordiging (Frontchannel en backchannel)
Vertegenwoordiger OAuth Res. Owner
User Agent
DVP Server OAuth Client
(OAuth) Author. Server (OAuth) Res. Server Authentication Client
Authentication Server
start Verzamelen
presenteer Verzamelen
selecteer zorg-aanbieder en info
verzoek Verzamelen
creëer sessie Verzamelen
presenteer landingspagina
redirect naar Authent. Server
vraag om authenticatie
vraag om credentials
presenteer vraag om credentials
authenticeer
geef credentials door
valideer credentials
vertegenwoordiging
Nee
Ja
presenteer lijst vertegenwoordigden
vraag naar vertegenwoordigde
selecteer vertegenwoordigde
stuur authenticatieverklaring
redirect van Authent. Server
redirect naar Authent. Client
presenteer authenticatieverklaring
valideer authenticatieverklaring
ontvang authenticatieverklaring
geef authenticatie-verklaring uit
vaststellen authenticatieverklaring
presenteer toestemmingsvraag
vraag om toestemming
geef toestemming
geef toestemming door
log toestemming
genereer author-ization code
OAuth-redirect van Auth. Server
geef authorization code uit
controleer scope op vertegenwoordiging
vraag access token
valideer author-ization code
genereer access token
ontvang access token
geef access token uit
kies nader
bied keus aan
doe resource request
valideer access token
laat nader kiezen
haal gezond-heidsinfo op
Vertegenwoordig
heeft bij de DV
aangegeven da
informatie verzam
wordt voor een ar
vroegste mo
instaan vo
beschikbaar
laatste mon
instaan vo
beschikbaar



In het bovenstaande stroomschema geven de dikke pijlen het *MedMij-verkeer* weer en zijn daarbinnen de gevallen van frontchannel-verkeer (open pijlpunt) en gevallen van backchannel-verkeer (gesloten pijlpunt) aangegeven.

Verantwoordelijkheden, Vertegenwoordiging

1. Inleiding

De verantwoordelijkheden die in de MedMij Core staan beschreven, zijn ook van toepassing op deze extensie. Daarnaast gelden de hieronder (vervangende) verantwoordelijkheden. Net als in de MedMij Core zijn de volgende kleuren voor de verantwoordelijkheden op de verschillende lagen gebruikt:

- Geel voor de businesslaag;
- Blauw voor de applicatielaag;
- Groen voor de technologielaag.

2. Rollen

1.	Een *Persoon* neemt de functionele rol van *Vertegenwoordigde* op zich, waarbij de *Persoon* zich laat vertegenwoordigen door een andere *Persoon* in de rol van *Vertegenwoordiger*.	ext.vert. rollen. 100
2.	Een *Vertegenwoordigde* kan zich door meerdere andere *Personen* laten vertegenwoordigen.	ext.vert. rollen. 101
2.	Een *Persoon* krijgt de functionele rol van *Vertegenwoordiger*, wanneer de *Persoon* gemachtigd is door een andere *Persoon* in de rol van *Vertegenwoordigde*.	ext.vert. rollen. 102
4.	Een *Vertegenwoordiger* kan meerdere *Personen* vertegenwoordigen.	ext.vert. rollen. 103

3. Functies & gegevens

3.1. Algemeen

1.	*Dienstverlener persoon* stelt, indien deze Vertegenwoordiging aanbiedt, aan *Persoon* de rol van *Vertegenwoordiger* ter beschikking met toegang tot het dossier van *Vertegenwoordigde*.	ext.vert. algemeen. 100
2.	*Dienstverlener persoon* stelt in de PGO aan *Vertegenwoordigde* de mogelijkheid om *Vertegenwoordigers* te registreren en dit ook weer ongedaan te maken.	ext.vert. algemeen. 101

3.2. Dossier

1.	*Dienstverlener persoon* neemt maatregelen om te voorkomen dat in een dossier van de Vertegenwoordigde gezondheidsinformatie van een andere Persoon wordt geplaatst.	ext. vert. dossier. 100
2.	*Dienstverlener persoon* biedt Vertegenwoordiger de functie *Verzamelen* om bij *Dienstverlener aanbieder* gezondheidsinformatie te verzamelen van *Aanbieder*, indien deze die informatie beschikbaar stelt, die op de *Vertegenwoordigde* betrekking heeft en laat deze	ext. vert. dossier. 101

	in een persoonlijk gezondheidsdossier (kortweg *Dossier*) van *Vertegenwoordigde* bewaren. Bij deze functie betrokken rollen gebruiken hiertoe het betreffende stroomdiagram. Dit dossier bevat informatie van precies één *Persoon*.	
3.	*Dienstverlener persoon* biedt *Vertegenwoordiger* de functie *Raadplegen dossier* om het persoonlijk gezondheidsdossier van de Vertegenwoordigde te raadplegen.	ext. vert. dossier. 102

3.3. Gegevensdiensten

1.	*Dienstverlener persoon* laat *Persoon of zijn/haar Vertegenwoordiger* met een *Gegevensdienst* uit de *Gegevensdienstnamenlijst* gezondheidsinformatie verzamelen bij een *Dienstverlener aanbieder*.	ext.vert. gegevensdiensten. 100

4. Autorisatie

1.	*Dienstverlener aanbieder* vergewist zich ervan, elke keer opnieuw voordat *Vertegenwoordiger* gezondheidsinformatie van *Aanbieder* laat verzamelen door middel van de functie *Verzamelen*, dat *Vertegenwoordiger* uitdrukkelijk *Toestemming* heeft gegeven aan *Aanbieder* om de in de *Gegevensdienst* betrokken gezondheidsinformatie aan *Dienstverlener persoon* ter beschikking te laten stellen. De vraag om *Toestemming* heeft een vaste formulering, die is opgenomen in de functie *Verzamelen*. Deze *Toestemming* is slechts van kracht binnen deze doorloping van de usecase. Dit geldt als uitbreiding op de verantwoordelijkheid zoals beschreven in core. autorisatie.100	ext.vert. autorisatie. 100
2.	*Dienstverlener aanbieder* draagt ervoor zorg dat de onder core.gegevensdiensten.103, core.gegevensdiensten.104, core.autorisatie.100 en core.autorisatie.101 bedoelde vraag om *Toestemming* slechts plaatsvinden wanneer hij de identiteit van de *Persoon* met passende zekerheid heeft vastgesteld.	ext.vert. autorisatie. 101
3.	Het *Machtigingsregister* heeft de verantwoordelijkheid voor het registreren, beheren, controleren van machtigingen en andere bevoegdheden en het afleggen van verklaringen over bevoegdheden (c.q. het op verzoek verstrekken van machtigingsverklaringen).	ext.vert. autorisatie. 102

5. Authenticatie

1.	*Dienstverlener aanbieder* stelt, indien deze Vertegenwoordiging aanbiedt, aan de *Vertegenwoordiger* de mogelijkheid zich te identificeren en geauthentiseerd te worden passend bij de rol van *Vertegenwoordiger*.	ext.vert. authenticatie. 100
2.	*Dienstverlener aanbieder* draagt ervoor zorg dat de onder core.gegevensdiensten.103 , core.gegevensdiensten.104, core.autorisatie.100 en core.autorisatie.101 bedoelde vraag om *Toestemming*, slechts plaatsvinden wanneer hij de identiteit van de *Vertegenwoordiger* met passende zekerheid heeft vastgesteld.	ext.vert. authenticatie. 101

6. Logging

1.		

	Dienstverlener persoon zal het *Dossier* zo inrichten dat deze ook dienst kan doen als logbestand, zoals bedoeld in de AVG en NEN 7513:2018, van de door enige *Persoon of zijn /haar Vertegenwoordiger* bij enige *Dienstverlener aanbieder* verzamelde persoonsgegevens.	ext. vert. logging. 100

Interfaces, Vertegenwoordiging

1. Inleiding

De interfacebeschrijvingen bevatten binnen deze extensie alleen de uitbreidingen / wijzigingen op de interfaces uit de MedMij Core. Voor een volledig beeld van de verantwoordelijkheden moeten de interfacebeschrijvingen daarom gecombineerd worden met die uit de MedMij Core.

Authorization interface, Vertegenwoordiging

In onderstaande tabel is alleen de uitbreiding aan de scope opgenomen, zoals deze in de MedMij Core staat beschreven, en de verdere toelichtingen daarop.

1.

parameter	vulling	toelichting
`scope`	Optioneel voor "vertegenwoordigen": • de letterlijke waarde `onbehalfof` • met een spatie gescheiden van de andere onderdelen	Voorbeeld van een syntactisch juiste scope is: • `"onbehalfof"`, als indicatie dat hier sprak van vertegenwoordiging

Bovenstaande tabel is een uitbreiding op de tabel die is weergegeven in core.authint.200

2. `Alleen als onbehalfof` in de scope voorkomt, verzoekt de *Authorization Server* de *Authentication S* ook vertegenwoordiging toe te staan. Dit wordt gedaan volgens de voorwaarden van de *Authentication Se*

3. De *OAuth Authorization Server* vergewist zich ervan dat tijdens Authenticatie ook gebruik is gemaakt van Vertegenwoordiging. Indien dit het geval is, geeft de *OAuth Authorization Server* een authorization-code u OAuth Client) voor de identiteit van de Vertegenwoordigde.

4. *OAuth Authorization Server* behandelt uitzonderingssituaties inzake het token interface volgens onderstaa tabel.

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Vervo
Authorization interface Vertegenwoordiging 1		*De OAuth Authorization Server* stelt dat tijdens Authenticatie geen gebruik is gemaakt van Vertegenwoordiging, terwijl dit wel verwacht werd.	*OAuth Authorization Server* informeert daarop *Persoon* hierover.		*OAuth Autho Serve* de flo onmid na geïnfo te zijn de uitzon
Authorization interface Vertegenwoordiging 2		*De OAuth Authorization Server* stelt dat tijdens Authenticatie gebruik is gemaakt van	*OAuth Authorization Server* informeert daarop *Persoon* hierover.		*OAuth Autho Serve* de flo onmid na geïnfo te zijn

		Vertegenwoordiging, terwijl dit niet verwacht werd.			de uitzon

De *OAuth Authorization Server* kan deze uitzonderingen alleen vaststellen als de *OAuth Authorizat Server* Vertegenwoordiging ondersteunt. Omdat deze extensie optioneel is voor alle deelnemers, k situatie zich voordoen dat de uitzondering wel van toepassing is, maar niet opgemerkt wordt door d *OAuth Authorization Server*.

MedMij Domeinen

1. Inleiding

MedMij ondersteunt domeinen als aspecten over de MedMij Core en Extensies heen. Dit betekent dat per domein rollen en verantwoordelijkheden worden beschreven waaraan iedere deelnemer moet voldoen die in een domein werkzaam is.

> Als een deelnemer bijvoorbeeld *Dienstverlener Aanbieder* in het domein *Zorg*, dan geldt voor deze deelnemer een combinatie. In het domein *Zorg* staat de rol *Dienstverlener Zorgaanbieder* beschreven, met de bijbehorende verantwoordelijkheden. Deze moeten gecombineerd worden met de verantwoordelijkheden die beschreven staan in de *MedMij Core*, voor de rol *Dienstverlener Aanbieder*.

2. Zorg

In deze versie van het afsprakenstelsel is Zorg het enige domein. Daarom verwijzen een aantal onderdelen van het afsprakenstelsel, binnen en buiten Architectuur en technische specificaties, naar dit domein. Dit zijn:

- Juridische context
  - Juridisch kader
  - Overeenkomsten en rechtsrelaties
  - Toelichting verwerkingsverantwoordelijkheid
- Informatiemodellen
  - Metamodel
  - Logische modellen
  - XML-schema's
  - XML-bestanden voor lijsten
- Communicatie
  - Toestemmingsverklaring
  - Toestemmingsverklaring Abonneren
  - Bevestigingsverklaring
  - Beëindigingsverklaring Abonnement
- Deelnemersovereenkomsten
  - Deelnemersovereenkomst Dienstverlener persoon
  - Deelnemersovereenkomst Dienstverlener aanbieder
- Toetreding
  - Toetredingsbeleid
  - Intentieverklaringen
    - Intentieverklaring Dienstverlener persoon
    - Intentieverklaring Dienstverlener zorgaanbieder
- Modelverwerkersovereenkomst

Zodra een ander domein aan het afsprakenstelsel wordt toegevoegd, moeten deze onderdelen worden herzien of er moeten nieuwe versies worden toegevoegd.

Zorg

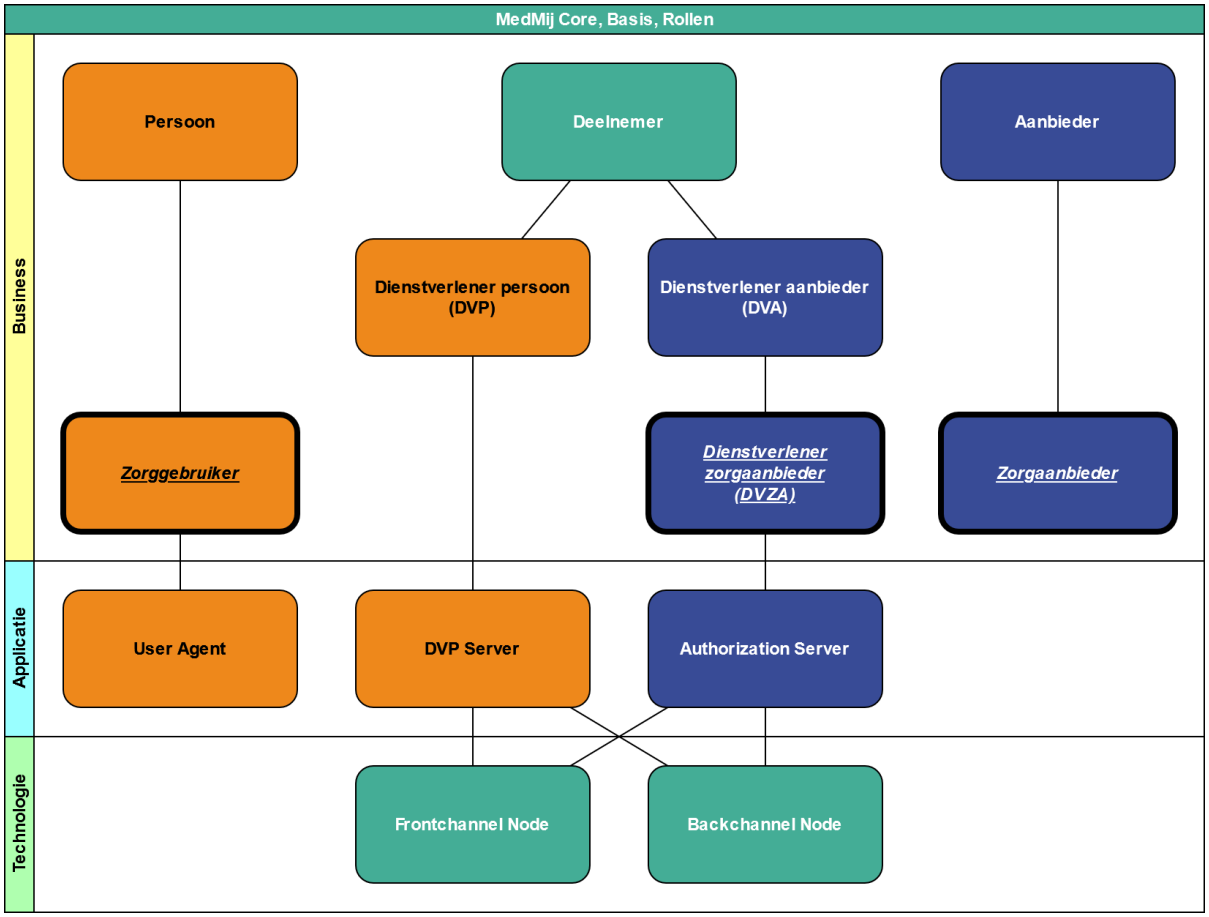
1. Inleiding

In deze versie van het afsprakenstelsel is Zorg het enige domein. Daarom verwijzen een aantal onderdelen van het afsprakenstelsel, binnen en buiten Architectuur en technische specificaties, naar dit domein. Dit zijn:

- Juridische context
  - Juridisch kader
  - Overeenkomsten en rechtsrelaties
  - Toelichting verwerkingsverantwoordelijkheid
- Informatiemodellen
  - Metamodel
  - Logische modellen
  - XML-schema's
  - XML-bestanden voor lijsten
- Communicatie
  - Toestemmingsverklaring
  - Toestemmingsverklaring Abonneren
  - Bevestigingsverklaring
  - Beëindigingsverklaring Abonnement
- Deelnemersovereenkomsten
  - Deelnemersovereenkomst Dienstverlener persoon
  - Deelnemersovereenkomst Dienstverlener aanbieder
- Toetreding
  - Toetredingsbeleid
  - Intentieverklaringen
    - Intentieverklaring Dienstverlener persoon
    - Intentieverklaring Dienstverlener zorgaanbieder
- Modelverwerkersovereenkomst

Zodra een ander domein aan het afsprakenstelsel wordt toegevoegd, moeten deze onderdelen worden herzien of er moeten nieuwe versies worden toegevoegd.

2. Rollen



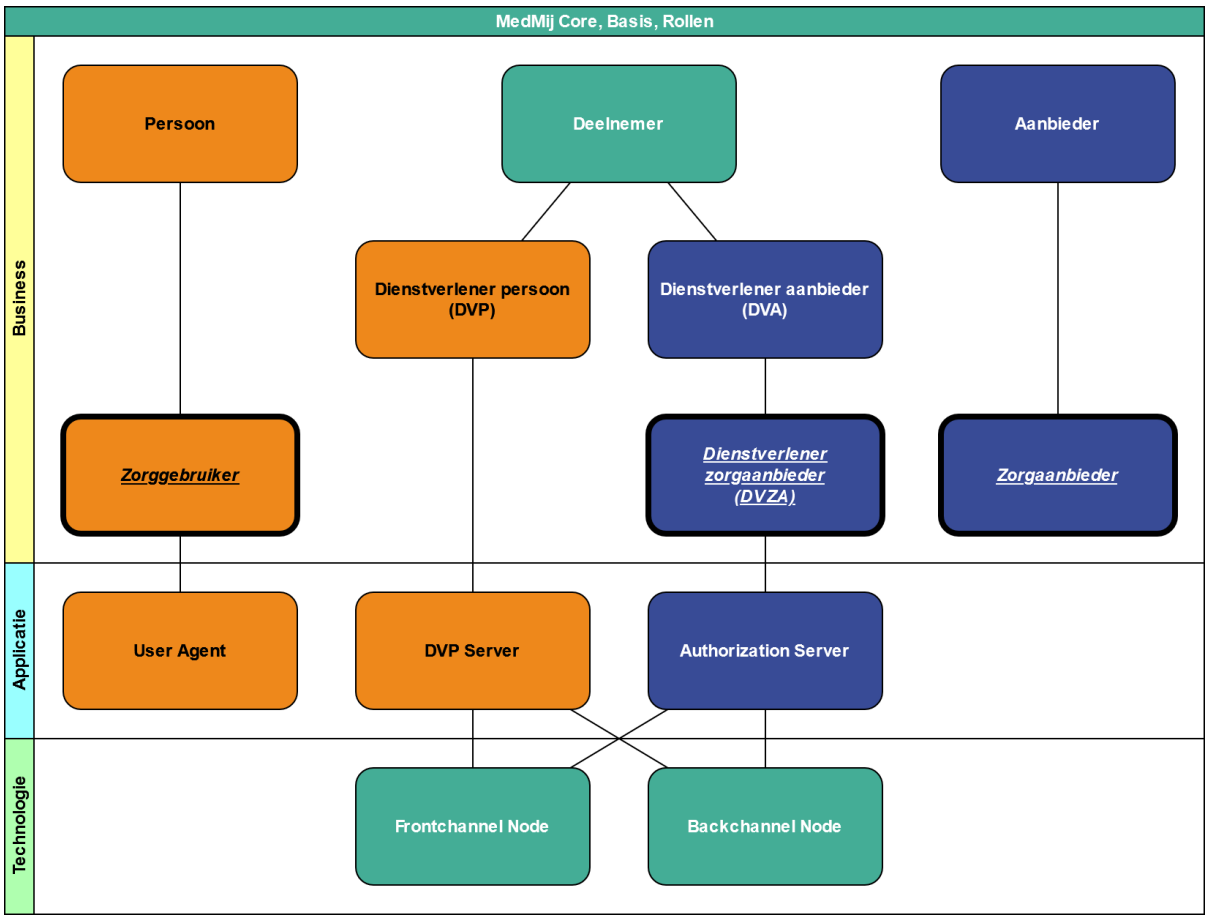
3. Verantwoordelijkheden

De verantwoordelijkheden die in de MedMij Core staan beschreven, zijn ook van toepassing op het domein Zorg. Daarnaast gelden de hieronder (vervangende) verantwoordelijkheden. Net als in de MedMij Core zijn de volgende kleuren voor de verantwoordelijkheden op de verschillende lagen gebruikt:

- Geel voor de businesslaag;
- Blauw voor de applicatielaag;
- Groen voor de technologielaag.

Rollen, Zorg

1. Rollenmodel



2. Roldefinities

2.1. Business

- **Zorggebruiker**
  Een Zorggebruiker is een *Persoon* die gebruikmaakt van een zorgaanbod, ook wel patiënten of cliënten genoemd.

- **Dienstverlener zorgaanbieder**
  Dienstverlener zorgaanbieder levert diensten aan de *Zorgaanbieder* gerelateerd aan de uitwisseling tussen *Persoon* en *Zorgaanbieder* en committeert zich hiervoor aan de naleving van de afspraken van het MedMij Afsprakenstelsel.

- **Zorgaanbieder**
  Een zorgverlener of een verband van zorgverleners die behandelingsovereenkomsten kunnen aangaan met patiënten op grond van art. 7:446 BW en tevens de Gebruiker in het Aanbiedersdomein.

Verantwoordelijkheden, Zorg

De verantwoordelijkheden die in de MedMij Core staan beschreven, zijn ook van toepassing op het domein Zorg. Daarnaast gelden de hieronder (vervangende) verantwoordelijkheden. Net als in de MedMij Core zijn de volgende kleuren voor de verantwoordelijkheden op de verschillende lagen gebruikt:

- Geel voor de businesslaag;
- Blauw voor de applicatielaag;
- Groen voor de technologielaag.

1. Rollen

1.	Een *Persoon* neemt de functionele rol van *Zorggebruiker* op zich. Deze rollen zijn één-op-één gekoppeld aan elkaar.	dmn.zorg.rollen.100

2. Verantwoordelijkheden

2.1. Beschikbaarheids- en ontvankelijkheidsvoorwaarde

Om redenen van dataminimali-satie en gebrui-ksvriendelijkheid zijn de beschikbaarheids- en ontvankelijkheidsvoorwaarden bij voorkeur zo snel mogelijk van kracht, dat wil zeggen, onmid-dellijk na de authenticatie van de *Persoon*, nog voor de autorisatievraag (de vroege variant). De beschikbaarheids- en ontvankelijkheidsvoorwaarde behoren uit hun aard bij de hoofdfunctie *Regie*, niet bij *Uitwisseling*. Daartegenover wordt de implementatie van de voorwaarden voor sommige *Deelnemers* eenvoudiger als zij pas van kracht zouden hoeven te zijn wanneer de procesgang bij de *Resource Server* is aangekomen (de late variant).

1.	De *Zorgaanbieder* voert beleid ten aanzien van het beschikbaar houden van gezondheidsinformatie (en *Abonnementen* op *Notificaties* daarover) voor, en ontvankelijk zijn voor gezondheidsinformatie van, zekere *Zorggebruikers* op zekere *Gegevensdiensten.*	dmn.zorg.besont.100
2.	De *Dienstverlener zorgaanbieder* voert, als verwerker voor elke verwerkingsverantwoordelijke *Zorgaanbieder*, diens in verantwoordelijkheid dmn.zorg.besont.100 bedoelde beleid uit in de functies *Verzamelen, Delen, Abonneren* en *Notificeren*. De *Dienstverlener zorgaanbieder* voert in aanvulling op dat van de *Zorgaanbieders* geen eigen beleid dienaangaande.	dmn.zorg.besont.101
3.	Het in verantwoordelijkheid dmn.zorg.besont.100 bedoelde beleid discrimineert op geen andere aspecten dan de *Zorggebruiker* en de *Gegevensdienst*. In het bijzonder is discriminatie op *Dienstverlener persoon* uitgesloten, tenzij dat door het MedMij Afsprakenstelsel wordt vereist.	dmn.zorg.besont.102
4.	Het instaan voor de beschikbaarheids- en de ontvankelijkheidsvoorwaarde is van kracht: • ergens tussen de gebruikersauthenticatie en de uitwisseling van gezondheidsinformatie, zoals beschreven in de functies *Verzamelen* en *Abonneren*, respectievelijk de functie *Delen*; • onmiddellijk bij het begin van de functie *Notificeren*;	dmn.zorg.besont.103
5.	Het MedMij Afsprakenstelsel verplicht er niet toe om leeftijdsgegevens en behandelrelatiegegevens expliciet te administreren. Waar het bestaan van een behandelrelatie of een toereikende leeftijd, op juridische en/of organisatorische gronden,	

	geïmpliceerd wordt door andere gegevens, mogen laatstgenoemde gegevens ook met die implicatie gebruikt worden. Het MedMij Afsprakenstelsel speci-ficeert daarom geen logica voor de voorwaarden; het bepaalt slechts twee noodzakelijke onderdelen van hun post-conditie: een toereikende leeftijd van de *Persoon* en het (hebben) bestaan van een toepasselijke behandelrelatie.	dmn.zorg.besont.104

Informatiemodellen

Inleiding

Op de pagina's onder deze pagina zijn, op drie abstractieniveaus, modellen opgenomen van de informatie die een rol speelt in de architectuur van het MedMij Afsprakenstelsel, in de hoofdfunctie *Coördinatie*. Het is de precieze "taal" van de hoofdfunctie *Coördinatie*. De drie abstractieniveaus verschillen in scope, stijl en structuur, maar bevatten allemaal dezelfde drie onderdelen:

- een modeldiagram met de structuur van de betrokken soorten informatie;
- een lijst met invarianten die extra eisen opleggen aan de instanties van het model;
- een lijst met zogenoemde basisklassen, dat wil zeggen, klassen waarvan de structuur in het diagram niet uitgewerkt staat, maar waarvan de waarden op zichzelf betekenis geacht worden te hebben.

> De verschillende informatiemodellen die zijn opgesteld voor versie 1.5.0 van het afsprakenstelsel gelden ook voor deze versie (1.5.1). Daarom wordt in de verschillende informatiemodellen nog verwezen naar versie 1.5.0.

Abstractieniveaus

De drie abstractieniveaus zijn:

- het conceptuele niveau met het metamodel;
- het logische niveau met drie logische modellen;
- het technische niveau met vier XML-schema's en een spreadsheet-tabelschema.

De scope van alle drie de niveaus beperkt zich in de deze versie van het MedMij Afsprakenstelsel tot de informatiesoorten die van belang zijn voor de vier door de MedMij-beheerorganisatie te publiceren lijsten en voor de *Catalogus*. Het metamodel bevat de relevante klassen vanuit het oogmerk van aanpasbaarheid en uitbreidbaarheid op de langere termijn. Binnen de grenzen van het object-georiënteerde denken, waarmee een groot deel van het publiek van deze modellen vertrouwd zal zijn, lukt dat het best met de systematische toepassing van associatieklassen. Dit staat nader toegelicht op de metamodel-pagina.

De logische modellen hebben samen dezelfde scope, maar maken een stap naar implementatie van de lijsten en de *Catalogus*. Daarom zijn ze hiërarchisch van opzet, en dus minder aanpasbaar en uitbreidbaar. Bovendien zijn er drie aparte logische modellen:

- één voor de vier lijsten, die gedurende de operatie van het MedMij-netwerk gepubliceerd worden;
- één voor de *Catalogus*, die bij het afsprakenstelsel gepubliceerd wordt op een aparte pagina;
- één voor de *MedMij StelselNode*, die in het afsprakenstelsel zelf gepubliceerd word;
- één voor de twee soorten *rapporten*, waarmee *Deelnemers* moeten rapporteren over hun operatie op het MedMij-netwerk.

De technische modellen bouwen hier voort en zijn ook hiërarchisch, maar maken een verdere keuze voor technologie: XML en spreadsheet. Op dit niveau is er een apart model (XML-schema) voor elke lijst en elk rapport. Voor de *Catalogus* is de implementatietechnologie een tabel in een spreadsheet. Voor de *MedMij StelselNode* is er geen apart technisch model.

Lagere abstractieniveaus erven de relevante informatiesoorten, invarianten en basisklassen van hogere. Daarbij kan echter sprake zijn van structuur- en naamswijzigingen. Op de betreffende pagina's zijn deze abstractiestappen nader toegelicht. Zo wordt het proces van conceptuele specificatie naar technische implementatie zo controleerbaar en beheersbaar mogelijk.

Metamodel

Inleiding

Het metamodel ordent kernbegrippen uit het MedMij Afsprakenstelsel. Het is een conceptueel gegevensmodel, in de vorm van een UML-klassediagram. Het metamodel is gericht op het samenhangend beschrijven van begrippen en relaties die worden gebruikt in de hoofdfunctie *Coördinatie* van MedMij. Het metamodel is allereerst de basis voor de structuur van:

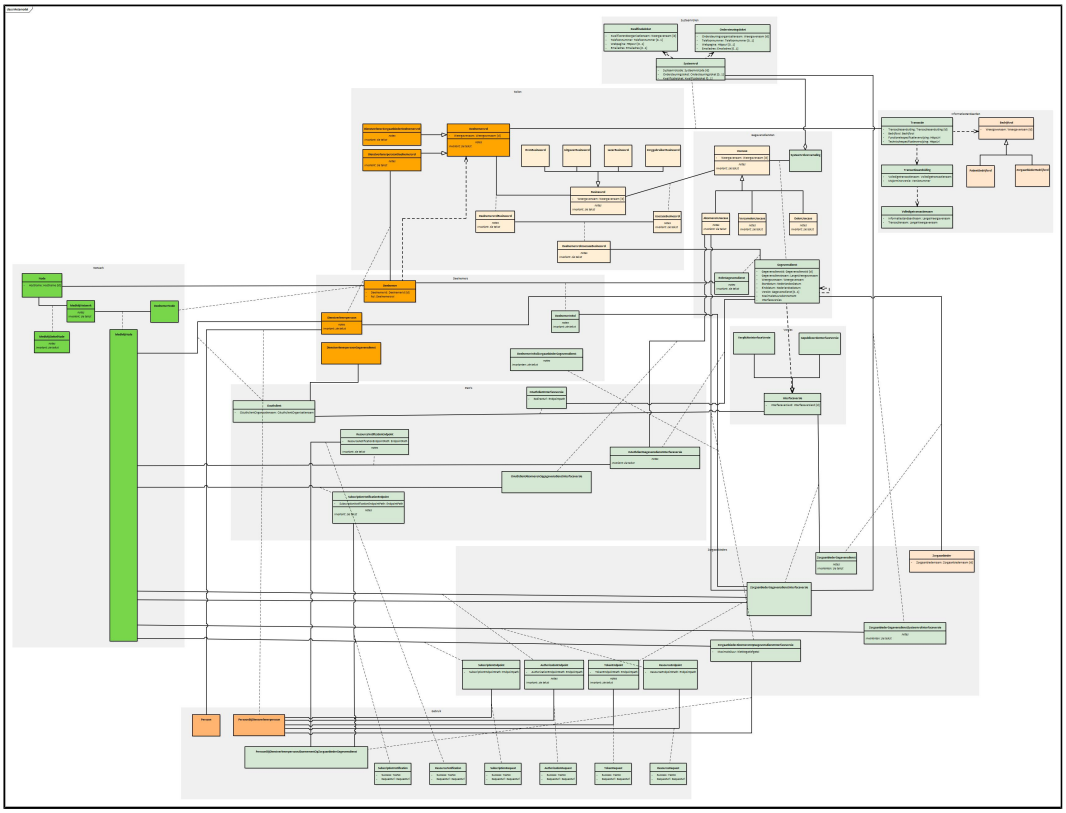
- de *Zorgaanbiederslijst*, waaraan de *OAuth Client* kan zien welke *Zorgaanbieders* momenteel welke *Gegevensdiensten* aanbieden en waarmee hij, gegeven een zekere *Interfaceversie*, de betrokken technische adressen (URI's) vindt van de *OAuth Authorization Server* (twee endpoints: het *Authorization Endpoint* en het *Token Endpoint*) en de *OAuth Resource Server* (het *Resource Endpoint*);
- de *Whitelist*, waarmee de *Nodes* elkaar accepteren als MedMij-nodes;
- de *OAuthclientlist*, waarin de *OAuth Authorization Server:*
  - een gebruikersvriendelijke naam van de *OAuth Client* kan vinden om te gebruiken in de toestemmingsverklaring danwel de bevestigingsverklaring;
  - kan zien voor welke *Gegevensdiensten* de *OAuth Client* gekwalificeerd is;
- de *Gegevensdienstnamenlijst*, waaraan de *OAuth Client* kan zien welke *Weergavenamen* de *Gegevensdiensten* hebben die op enig moment beschikbaar zijn op het MedMij-netwerk.

Een vijfde lijst, de *Catalogus*, wordt door MedMij gepubliceerd als annex van het MedMij Afsprakenstelsel, op deze pagina. Ten slotte is het metamodel de conceptuele basis voor twee rapportages die van Deelnemers worden verwacht:

- het *Beheerrapport*, waarmee elke *Deelnemer* de *Beheerorganisatie* periodiek inlicht over kentallen over het functioneren van het MedMij-netwerk;
- het *Portabiliteitsrapport*, waarmee de *Persoon* door diens *Dienstverlener Persoon* wordt ingelicht over welke gezondheidsinformatie die *Persoon* van *Zorgaanbieders* in zijn PGO heeft verzameld, zodat hij een eventuele andere of nieuwe PGO opnieuw met dezelfde verzamelacties zou kunnen vullen.

Voor alle zeven zijn logische modellen beschikbaar, op een aparte pagina, die implementaties zijn van het metamodel.

Model



Het model

Het metamodel is in een bepaalde stijl opgezet, met vooral associatieklassen. Het voordeel daarvan is dat het metamodel zo aanpasbaar en uitbreidbaar mogelijk blijft. Veel voorkomende constructies, zoals attributen en specialisatie zijn allemaal implementaties van associatieklassen. Implementatie willen we echter aan de logische modellen en de technische modellen (de XML-schema's) overlaten. Een tweede voordeel is dat bestaansafhankelijkheidsrelaties expliciet worden. Bestaansafhankelijkheid wil zeggen dat de ene klasse betekenisloos is zonder de andere en dus dat eerstgenoemde klasse niet kan bestaan zonder laatstgenoemde. Bij een associatieklasse is die associatieklasse altijd bestaansafhankelijk van de twee klassen die het associeert.

Op enkele punten is afgeweken van deze modelleerstijl, om de presentatie van het model niet onnodig te compliceren.

Het metamodel is, voor het overzicht, geordend in negen modelgebieden: *Rollen*, *Deelnemers*, *PGO's*, *Zorgaanbieders*, *Gegevensdiensten*, *Informatiestandaarden*, *Netwerk*, *Changes* en *Gebruik*. Linksboven de plaat van het metamodel staat in een kaartje hoe de verschillende gebieden gebruik maken van concepten uit andere gebieden.

De namen van de klassen en de attributen beginnen allemaal met een hoofdletter. De rest van de namen bestaat uit enkel kleine letters, behalve daar waar de rest van de naam ook als aparte naam in het metamodel voorkomt, of er een eigennaam wordt gebruikt die anderszins eist. Het metamodel noteert dus *OAuthclient*, omdat de naam *OAuth* een eigennaam is waarin de *A* als hoofdletter wordt geschreven, en omdat de naam *Client* niet als aparte naam voorkomt in het metamodel. Het metamodel noteert *ZorgaanbiederGegevensdienst*, met een kapitale eerste *G*, omdat *Gegevensdienst* wel als aparte naam voorkomt.

De MedMij-beheerorganisatie houdt bij welke *Organisaties*, door het aangaan van een *Deelnemersovereenkomst*, *Deelnemer* worden. *Deelnemers* zijn er in twee rollen:

DienstverlenerpersoonDeelnemersrol en *DienstverlenerzorgaanbiederDeelnemersrol*. Deze komen overeen met de respectievelijke rollen *Dienstverlener Persoon* en *Dienstverlener Zorgaanbieder* op de juridische laag.

Organisaties gebruiken *Nodes* waarvan zij de houder zijn. Als een *Organisatie* een *Deelnemer* is, zal zij zo'n *Node* als *DeelnemerNode* bij de MedMij-beheerorganisatie aanmelden. Op het *MedMijnetwerk* verschijnt zo'n *DeelnemerNode* als een *MedMijNode*. De *Hostnames* van deze *MedMijNodes* ontsluit de MedMij-beheerorganisatie over het *MedMijnetwerk*. De *MedMijNodes* gebruiken deze lijst als *Whitelist*, dat wil zeggen, om te bepalen of een *Node* die zich bij hen aandient, geautoriseerd is om op het *MedMijnetwerk* actief te zijn. Deze *Whitelist* verschijnt, als implementatiecomponent, pas in de logische modellen. Dat geldt ook voor de *MedMijStelselNode*, de Node via welke *MedMij Beheer* vier lijsten publiceert. De *MedMijStelselNode* staat niet expliciet op de *Whitelist*, maar is wel geautoriseerd deel te nemen op het *MedMijnetwerk*. Sterker, zonder de *MedMijStelselNode* kan het *MedMijnetwerk* niet werken.

Voor de *MedMijNodes* van *Deelnemers* die *Dienstverlenerpersoon* zijn (beter gezegd: voor de *OAuth Clients* op de applicatielaag gedurende de autorisatiefase van UCI Verzamelen en UCI Delen) bevat de *OAuthclientlist* gebruikersvriendelijke namen (*Organisatienaam*), om gebruikt te worden in de toestemmingsverklaring en de bevestigingsverklaring. Ook de *OAuthclientlist* is een implementatiecomponent en verschijnt pas in de logische modellen. Wanneer een OAuth Client (een PGO) het gebruiken van Abonnementen mogelijk maakt voor de Persoon, moet zij endpoints aanbieden voor de twee soorten notificaties die de *Zorgaanbieder* in dat kader moet kunnen sturen: een *SubscriptionNotificationEndpoint* en een *ResourceNotificationEndpoint*.

In het *Rollen*-modeldomein verschijnen de *Deelnemerrollen*, *Businessrollen* en *Usecases* die in deze release van het MedMij Afsprakenstelsel bestaan, en hun toegestane combinaties. In het *Deelnemers*-modeldomein komen de *Deelnemers* in het MedMij Afsprakenstelsel aan de orde en voor welke *Zorgaanbieders* zij welke *Gegevensdiensten* ontsluiten.

Gegevensdiensten horen bij een *Usecase* en hebben een geldigheidsperiode. Bovendien wordt, door middel van het attribuut *Vereist*, van sommige *Gegevensdiensten* vereist dat, als een *Zorgaanbieder* die *Gegevensdienst* aanbiedt, hij ook zekere andere *Gegevensdiensten* moet aanbieden. Vaak zal die lijst leeg zijn, maar het heeft bijvoorbeeld weinig zin het *Delen* van een afspraakverzoek aan te bieden, zonder ook het *Verzamelen* van het antwoord daarop aan te bieden. De klasse *RolInGegevensdienst* wordt gebruikt om, via de *Deelnemer*, de MedMij-rollen *DienstverlenerpersoonDeelnemersrol* en *DienstverlenerzorgaanbiederDeelnemersrol* te verbinden met de dienovereenkomstige rollen die Nictiz in het Informatiestandaarden-domein heeft geformuleerd, namelijk respectievelijk PatiëntBedrijfsrol en ZorgaanbiederBedrijfsrol. Een *GegevensdienstInterfaceversie* geeft aan dat een *Gegevensdienst* via de *Interfaceversie* mag worden aangeboden.

De klassen in het modeldomein *Informatiestandaarden*, inclusief hun namen, moeten begrepen worden in de zin waarin Nictiz ze gebruikt in het kader van de *Informatiestandaarden*waarvan de onderdelen de basis vormen voor *Gegevensdiensten*. De bouwblokjes van een *Informatiestandaard*noemen we een *Transactie*, die zowel functionele als technische specificaties bevat. Een *Bedrijfsrol*, waarvan er twee zijn (*PatiëntBedrijfsrol* en *ZorgaanbiederBedrijfsrol*), wordt aangenomen door een *Transactie*.

De klassen in het modeldomein *Systeemrollen* leggen de verbinding tussen het domein van de *Informatiestandaarden* en dat van de *Gegevensdiensten*. Een *Systeemrol* is een *Transactie* die voorzien is van een *Systeemrolcode* om hem binnen MedMij uniek te kunnen aanduiden. Merk op dat een *Systeemrol* een concept is met een specifieke betekenis binnen het MedMij Afsprakenstelsel. Het is niet hetzelfde als het concept "Systeemrol" zoals dat wordt gebruikt binnen de Nictiz-informatiestandaarden. Een *Systeemrol* kan een *Ondersteuningsorganisatie* hebben die dienstverlening biedt aan *Deelnemers* bij vragen over de specificaties behorend bij de *Systeemrol*. Vaak zal dit de beheerder van de onderliggende *Informatiestandaard* zijn, maar het is ook denkbaar dat er geen beheerder is of dat een andere partij de rol van beheerder vervult (bijvoorbeeld als de beheerder van de *Informatiestandaard* geen dienstverlening biedt voor MedMij-stakeholders). Een *Systeemrol* kan ook verbonden zijn met een *Kwalificatieloket* waar de ondersteuning van *Systeemrollen* kan worden aangetoond.

Systeemrollen worden gegroepeerd in *Systeemrolverzamelingen* die samen met een *Usecase* een *Gegevensdienst* vormen. Een actueel voorbeeld van een *Systeemrolverzameling* is een verzameling van vier *Systeemrollen* waarvan er twee een overzicht van beschikbare PDF-documenten uitwisselen en twee een PDF-document uit dat overzicht uitwisselen. *Gegevensdiensten* worden als geheel (dat wil zeggen met hun gehele *Systeemrolverzameling*) aan *Zorggebruikers* aangeboden en die gebruikers zullen deze ook ineens autoriseren.

Onder in het model wordt het verband gelegd met de *Zorgaanbieders*. Dit modeldomein is de basis voor het logische model van de *Zorgaanbiederslijst*. Wanneer een *Zorgaanbieder* een zekere *Gegevensdienst* aanbiedt volgens een zekere *Interfaceversie*, hoort daarbij een *ZorgaanbiederGegevensdienstInterfaceversie* . Wanneer een *Zorgaanbieder* bovendien *Abonnementen* op deze *Gegevensdienst* aanbiedt, hoort daarbij een *ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie*. Deze klassen worden gebruikt om *Zorggebruikers* te informeren over wie van de *Zorgaanbieders* (*Abonnementen* op) welke *Gegevensdiensten* aanbieden. Binnen een *Gegevensdienst* zijn bovendien één of meerdere *Systeemrollen* aan de orde. Deze relatie is vervat in de klasse *ZorgaanbiederGegevensdienstSysteemrolInterfaceversie*.

Interfaces zijn geversioneerd: verschillende versies van interfaces kunnen tegelijkertijd op het MedMij-netwerk worden aangeboden. Daarom is er de klasse *Interfaceversie* in het modelgebied *Changes*. Alle endpoints in de *Zorgaanbiederslijst* en *Oauth Client List* (zie onder) horen bij één *Interfaceversie*.

Een *Zorgaanbieder* kan de maximale abonnementsduur die hij aanbiedt voor een *Gegevensduur*, op een *Interfaceversie*, beperken. Daarbij moet hij echter blijven onder de maximale duur die MedMij voor die *Gegevensdienst* in de *Catalogus* heeft aangegeven. De maximale duur geeft de doorlooptijd aan in dagen waarbij de waarde 0 aangeeft dat een abonnement niet wordt ondersteund.

Bij een *ZorgaanbiederGegevensdienst* hoort één *AuthorizationEndpoint*, één *TokenEndpoint* en, indien daarop ook *Abonnementen* worden aangeboden, één *SubscriptionEndpoint*. Bij een *ZorgaanbiederGegevensdienstSysteemrol* hoort één *ResourceEndpoint*. Bij alle soorten endpoints noemt het metamodel het *Endpointpath*, het path in de URI waarmee de endpoints geadresseerd worden, en een *Interfaceversion*, waarmee gelijktijdig operationele versies van dezelfde endpoints kunnen worden onderscheiden. In deze versie van het MedMij Afsprakenstelsel worden op zowel frontchannel als backchannel de standaard IANA-poort voor `https` gebruikt. Er hoeven in de endpointadressen dus geen poortnummers te worden genoemd.

Deze onderdelen worden samen met de *Hostname* van de betreffende *MedMijNode* samengesteld tot een URI die geldt als het adres van het respectievelijke endpoint. Dat gebeurt in het logische model (met invarianten). De eisen aan al deze componenten en de wijzen van samenstellen tot de URI's staat beschreven op de Interface-pagina.

Eenzelfde *Zorgaanbieder* kan voor verschillende *Gegevensdiensten* van diensten van verschillende *Deelnemers* gebruik maken. Maar bij één *ZorgaanbiederGegevensdienst* hoort precies één *DeelnemerInRol*. Voor dit doel is in het metamodel de klasse *DeelnemerInRolZorgaanbiederGegevensdienst* opgenomen, in het *Deelnemers*-modeldomein.

Ten behoeve van het Beheerrapport en het Portabiliteitsrapport moet door Deelnemers informatie kunnen worden overlegd over wat er op het MedMij-netwerk gebeurt. Deze informatie wordt opgespannen door het modelgebied *Gebruik*. Deze informatie is hoofdzakelijk gestoeld op requests die worden gedaan over het MedMij-netwerk. Die zijn er in zes soorten. Van elke request moet bekend zijn wat de *RequestUri* was en of de request al dan niet succesvol was.

Invarianten

Invarianten, dat wil zeggen, beperkingen die te allen tijden aan de orde zijn, staan onderaan in een separate tabel opgenomen. Daarvan bestaan verschillende soorten, genoemd in de rechterkolom:

- Opsommingen stellen dat een zekere klasse een vast aantal expliciet benoemde instanties heeft.

- Getalsverhoudingen vereisen getalsmatige eisen aan het aantal instanties van een klasse, of de verhouding tussen de aantallen in meerdere klassen.
- Lokale afhankelijkheden stellen beperkingen aan de inhoudelijke verhoudingen tussen attributen van eenzelfde klasse.
- Niet-lokale afhankelijkheid stellen beperkingen aan de inhoudelijke verhoudingen tussen instanties van verschillende klassen.
- Rolbindingen beperken de rolcombinaties van verschillende rol-klassen. Zij komen overeen met onder andere de rolbindingen tussen de verschillende lagen.

Lagen in het afsprakenstelsel

De klassen in het metamodel horen bij de verschillende lagen in de architectuur van het afsprakenstelsel. De betreffende laag is aangegeven door de inkleuringen van de klassen.

Adressering

Uit dit metamodel wordt duidelijk hoe in het MedMij Afsprakenstelsel met adressering wordt omgegaan. De adresseringssystematiek bestaat uit drie onderdelen:

- MedMij-zorgaanbiedernamen voor *Zorgaanbieders*, zoals beschreven in verantwoordelijkheid 13 op de Processen-en-Informatielaag;
- *Gegevensdiensten* met *Systeemrollen* zoals opgenomen in de *Catalogus*, respectievelijk het *Register van Informatiestandaarden*;
- Elke *Zorgaanbieder* kent bij elke *ZorgaanbiederGegevensdienstInterfaceversie* (die hij aanbiedt via een *Dienstverlener Zorgaanbieder*) één *AuthorizationEndpoint* en één *TokenEndpoint* en bij elke *ZorgaanbiederGegevensdienstInterfaceversieSysteemrol* daarbinnen één *ResourceEndpoint*. De endpoints hebben elk een URI als technisch adres.

Periodes

Daar waar in het metamodel sprake is van periodes, begrensd door een start en een eind, moeten deze start en eind opgevat als beginmomenten. Als het om een startdatum en einddatum gaat, zoals in de attributen van *Gegevensdienst*, worden dus de beginmomenten van die data bedoeld, om 00h00m00. De start wordt opgevat als het begin van de geldigheid, het eind als het begin van de ongeldigheid. De geldigheid loopt daarom vanaf start tot eind (niet tot en met). Dit betekent ook dat, als het eind ontbreekt, de geldigheid zich voor onbepaalde tijd uitstrekt.

Invarianten

Het diagram hierboven wordt geordend door (bestaans)afhankelijkheden tussen klassen. Binnen deze ordening bestaan er ook nog consistentie-eisen aan de instanties van deze klassen. Dit zijn de invarianten die in onderstaande tabel zijn opgenomen. Wat een invariant uitdrukt is dat een instantie van de betreffende klasse niet bestaat als zij niet aan de invariant voldoet. De tabel doet verder geen uitspraken over hoe de bewaking van deze consistentie wordt geïmplementeerd. In menige implementatie zullen tijdelijke inconsistenties worden toegestaan en pas later geweigerd of verholpen worden. Dat kan op vele manieren, maar het MedMij Afsprakenstelsel wil grote vrijheid laten in hoe de consistentie in registraties wordt geborgd.

De pad-expressies in de invarianten bestaan uit namen gescheiden door punten. Vanuit een zekere klasse wordt altijd een stap gemaakt naar een klasse waarvan eerstgenoemde onmiddellijk bestaansafhankelijk is. De naam van de zijde van de associatie waarover de stap wordt gemaakt wordt geacht de naam te dragen van de klasse aan het betreffende eindpunt van de associatie, de bestemming van de stap dus.

Betreft instanties van klasse ...	Invariant
AbonnerenUsecase	Er is precies één instantie hiervan.

AuthotizationEndpoint	Voor elk *AuthorizationEndpoint a* en voor elke *DeelnemerInRolZorgaanbiederGege* geldt: ALS *d.ZorgaanbiederGegevensdienstInterface* *a.ZorgaanbiederGegevensdienstInterfaceversi* DAN *d.DeelnemerInRol.Deelnemer = a.MedMij* *DeelnemerNode.Deelnemer*
Bedrijfsrol	Elke *Bedrijfsrol* is hetzij *PatiëntBedrijfsrol* of *ZorgaanbiederBedrijfsrol.*
Bedrijfsrol	Voor elke *Bedrijfsrol b* geldt: ALS(*b : PatiëntBedrijfsrol* DAN *b.Weergavenaam* = " *b : ZorgaanbiederBedrijfsrol* DAN *b.Weergaver* "Zorgaanbieder"; ANDERS FOUT)
BronBusinessrol	Er is precies één instantie hiervan.
Businessrol	Voor elke *Businessrol b* geldt: ALS(*b : BronBusinessrol* DAN *b.Weergavenaam* = " *b : LezerBusinessrol* DAN *b.Weergavenaam* = *b : UitgeverBusinessrol* DAN *b.Weergavenaam* ANDERS FOUT)
DeelnemerInRol	Voor elke *DeelnemerInRol d* geldt: *d.Deelnemer.Deelnemersrol* en *d.RolInGegeve* *DeelnemersrolUsecaseBusinessrol.Deelnemer* identiek.
DeelnemerInRolZorgaanbiederGegevensdienst	Voor elke *DeelnemerInRolZorgaanbiederGege* geldt: *d. ZorgaanbiederGegevensdienst.Gegevensdie* *DeelnemerInRol.RolInGegevensdienst.Gegeve*
Dienstverlenerpersoon	Er bestaat hooguit één instantie hiervan bij één en precies één als de *Deelnemersrol* van laatst van het type *DienstverlenerpersoonDeelnemer*
Deelnemersrol	Voor elke *Deelnemersrol d* geldt: ALS(*d : DienstverlenerpersoonDeelnemersrol* DAN *Weergavenaam* = "Dienstverlener persoon"; *d : DienstverlenerzorgaanbiederDeelnemersrol* *Weergavenaam* = "Dienstverlener zorgaanbied ANDERS FOUT)
DeelnemersrolBusinessrol	Er bestaan precies drie instanties hiervan, nam • één zodanig dat *DeelnemersrolBusinessrol* : *DienstverlenerpersoonDeelnemersrol* en *DeelnemersrolBusiness.Businessrol* : *Uitge* ;

	• één zodanig dat *DeelnemersrolBusinessrol* : *DienstverlenerzorgaanbiederDeelnemersr* *DeelnemersrolBusiness.Businessrol* : *Broni* • één zodanig dat *DeelnemersrolBusinessrol* *Deelnemersrol* : *DienstverlenerzorgaanbiederDeelnemersro* *DeelnemersrolBusiness*. *Businessrol* : *Leze*
DeelnemersrolUsecaseBusinessRol	Deze klasse bestaat uit precies één instantie v combinatie van een instantie *d* van *Deelnemers* en een instantie *u* van *UsecaseBusinessrol* wa *BusinessRol = u.BusinessRol.*
DelenUsecase	Er is precies één instantie hiervan.
DienstverlenerpersoonDeelnemersrol	Er is precies één instantie hiervan.
DienstverlenerzorgaanbiederDeelnemersrol	Er is precies één instantie hiervan.
Gegevensdienst	Er zijn nul of meer *Gegevensdiensten*.
Gegevensdienst	Voor elke *Gegevensdienst g* geldt: *g.Startdatum* ligt voor *g.Einddatum*.
Gegevensdienst	Voor elke *Gegevensdienst g1* en *g2* geldt: ALS g*2* voorkomt in g*1.Vereist DAN* (g*2* staat als *Gegevensdienst* in *Catalogus* EN *g1.Startdatum* ligt niet voor g*2.Startdatum* EN *g1.Einddatum* ligt niet na g*2.Einddatum*)
Gegevensdienst	Voor elke twee verschillende *Gegevensdienste* geldt: *g1.Gegevensdienstnaam* /= *g2.Gegevensdiens*
Gegevensdienst	Voor elke *Gegevensdienst* geldt: *g.Usecase* is *VerzamelenUsecase* ofwel *DelenUsecase*.
GepubliceerdeInterfaceversie	Er is precies één instantie hiervan.
Kwalificatieloket	Elk *Kwalificatieloket* heeft ten minste één van d attributen: *Emailadres*, *Telefoonnummer* en *Em*
LezerBusinessrol	Er is precies één instantie hiervan.
MedMijnetwerk	Er is precies één instantie hiervan.
MedMijStelselNode	Er is precies één instantie hiervan.

Node	De hostname van een Node bevat een domein fully-qualified domain name is, conform RFC36
OAuthclient	Voor elke *OAuthclient o* geldt: *o.OAuthclientOrganisatienaam* voldoet aan het namenbeleid.
OAuthclientAbonnerenOpGegevensdienstInterfaceversie	Elke *OAuthclientAbonnerenOpGegevensdienst* heeft precies één *ResourceNotificationEndpoi*
OAuthclientAbonnerenOpGegevensdienstInterfaceversie	Elke *OAuthclientAbonnerenOpGegevensdienst* heeft precies één *SubscriptionNotificationEndp*
OAuthclientGegevensdienstInterfaceversie	Voor elke *OAuthclientGegevensdienstInterface* geldt: ALS er een *OAuthClient AbonnerenOpGegevensdienstInterfaceversie o* • *oagi1.OAuthclientGegevensdienstInterface Gegevensdienst = g* en • *oagi1.OAuthClientGegevensdienstInterface OAuthclientInterfaceversie.Interfaceversie i GepubliceerdeInterfaceversie* DAN is er een *OAuthClient AbonnerenOpGegevensdienstInterfaceversie o* • *oagi2.OAuthclientGegevensdienstInterface Gegevensdienst = g* en • *oagi2OAuthClientGegevensdienstInterface OAuthclientInterfaceversie.Interfaceversie i VerplichteInterfaceversie*
Ondersteuningsloket	Elk *Ondersteuningsloket* heeft ten minste één v volgende attributen: *Emailadres*, *Telefoonnumr Emailadres*.
ResourceEndpoint	Voor elk *ResourceEndpoint r* en voor elke *DeelnemerInRolZorgaanbiederGege* geldt: ALS *d.ZorgaanbiederGegevensdienstInterface r.ZorgaanbiederGegevensdienstSysteemrolInte ZorgaanbiederGegevensdienstInterfaceversie* DAN *d.DeelnemerInRol.Deelnemer = r.MedMij DeelnemerNode.Deelnemer*

ResourceEndpoint	Voor elk *ResourceEndpoint r* geldt: de combinatie van *r.MedMijNode.DeelnemerNo* *Hostname* en *r.ResourceEndpointpath* is gelijk specificaties van *r.* *ZorgaanbiederGegevensdienstSysteemrolInter* *Systeemrol.Transactie* `[base]`heet. Wanneer de specificaties een request identifice geen `[base]` aanduiden, is de combinatie van *DeelnemerNode.Node.Hostname* en *r.* *ResourceEndpointpath* gelijk aan het volledige elke volledige, absolute URI voor resource requ de *Resource Server* mogen en kunnen worden in de context van de *ZorgaanbiederGegevensdienstInterfaceversieS*
ResourceNotificationEndpoint	Voor elk *ResourceNotificationEndpoint s* geldt: *s.MedMijNode.DeelnemerNode.Deelnemer = s* *OAuthClientAbonnerenOpGegevensdienst.* *OAuthclient.MedMijNode.DeelnemerNode.Dee*
RolInGegevensdienst	Deze klasse bestaat uit precies één instantie *r* combinatie van een instantie *d* van *r*. *DeelnemersrolUsecaseBusinessrol* en een inst *Gegevensdienst* waarvoor geldt: *g.Usecase = d* *UsecaseBusinessrol.Usecase*
SubscriptionEndpoint	Voor elk *SubscriptionEndpoint s* en voor elke *DeelnemerInRolZorgaanbiederGegev* geldt: ALS *d.ZorgaanbiederGegevensdienstInterface* *s.* *ZorgaanbiederAbonnerenOpGegevensdienstIn* *ZorgaanbiederGegevensdienstInterfaceversie* DAN *d.DeelnemerInRol.Deelnemer = s.MedMij* *DeelnemerNode.Deelnemer*
SubscriptionEndpoint	Voor elke *ZorgaanbiederGegevensdienst zg*, voor elke *Zorgaanbiedergegevensdienstinterfa* van *zg*, voor elke *ZorgaanbiederAbonnerenOpGegevensdienstIn* *zag* van *zgi*, voor elk *ResourceEndpoint r* van *zagi* en voor elke *DeelnemerinRolZorgaanbiederGegev* van *zg* geldt: *r.MedMijNode.DeelnemerNode.Deelnemer = d.* *DeelnemerInRol.Deelnemer*

SubscriptionNotificationEndpoint	Voor elk *SubscriptionNotificationEndpoint s* gel *s.MedMijNode.DeelnemerNode.Deelnemer = s* *OAuthClientAbonnerenOpGegevensdienst.* *OAuthclient.MedMijNode.DeelnemerNode.Dee*
TokenEndpoint	Voor elk *TokenEndpoint t* en voor elke *DeelnemerInRolZorgaanbiederGege* geldt: ALS *d.ZorgaanbiederGegevensdienstInterface* *t.ZorgaanbiederGegevensdienstInterfaceversie* DAN *d.DeelnemerInRol.Deelnemer = t.MedMijl* *DeelnemerNode.Deelnemer*
UitgeverBusinessrol	Er is precies één instantie hiervan.
Usecase	Voor elke *Usecase u* geldt: ALS(*u : VerzamelenUsecase* DAN *u.Weergavenaan* "Verzamelen"; *u : DelenUsecase DAN u.Weergavenaam* = "D ANDERS FOUT)
Usecase Businessrol	Er zijn precies vier instanties hiervan, namelijk: • één zodanig dat *UseCaseBusinessrol.Busi* *UitgeverBusinessrol* en *UseCaseBusinessr* *VerzamelenUsecase*; • één zodanig dat *UseCaseBusinessrol.Busi* *UitgeverBusinessrol* en *UseCaseBusinessr* *DelenUsecase*; en • één zodanig dat *UseCaseBusinessrol.Busi* *BronBusinessrol* en *UseCaseBusinessrol.U* *VerzamelenUsecase*; en • één zodanig dat *UseCaseBusinessrol.Busi* *LezerBusinessrol* en *UseCaseBusinessrol.* *DelenUsecase.*
VerplichteInterfaceversie	Er is precies één instantie hiervan.
VerzamelenUsecase	Er is precies één instantie hiervan.
ZorgaanbiederBedrijfsrol	Er is precies één instantie hiervan.
Zorgaanbieder	Elke *Zorgaanbieder* heeft minstens één *ZorgaanbiederGegevensdienst*
Zorgaanbieder	Elke *Zorgaanbieder* heeft bij elke *Gegevensdie* hoogste één *ZorgaanbiederGegevensdienst*.
Zorgaanbieder	Voor elke *ZorgaanbiederGegevensdienst zg1* e *Gegevensdienst g* in *zg1.Gegevensdienst.Vere*

	er een *ZorgaanbiederGegevensdienst zg2*, zod *zg1.Zorgaanbieder = zg2.Zorgaanbieder* en *zg1.Gegevensdienst = g*.
ZorgaanbiederAbonnerenOpGegevensdienst	Voor elke *ZorgaanbiederGegevensdienst zg*, Voor elke *ZorgaanbiederAbonnerenOpGegeve* van *zg*, voor elk *SubscriptionEndpoint s* van *zaog* en voor elke *DeelnemerinRolZorgaanbiederGegev* van *zg* geldt: *s.MedMijNode.DeelnemerNode.Deelnemer = d* *DeelnemerInRol.Deelnemer*
ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie	Voor elke *ZorgaanbiederAbonnerenOpGegevensdienstIn* *zgi* geldt: *zgi.ZorgaanbiederGegevensdienstInterfacevers* *ZorgaanbiederGegevensdienst.Gegevensdiens* *VerzamelenUsecase*
ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie	Elke *ZorgaanbiederAbonnerenOpGegevensdienstIn* heeft precies één *SubscriptionEndpoint*.
ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie	Voor elke *ZorgaanbiederAbonnerenOpGegevensdienstIn* *zgi* geldt: *zgi.MaximaleDuur <= zgi.* *ZorgaanbiederGegevensdienstInterfaceversie.* *ZorgaanbiederGegevensdienst.Gegevensdiens* *MaximaleDuur*
ZorgaanbiederGegevensdienst	Voor elke *ZorgaanbiederGegevensdienst zg* ge ALS er een *ZorgaanbiederGegevensdienstInte* *zgi1* is zodat: • *zgi1.ZorgaanbiederGegevensdienst = zg* er • *zgi1.Interfaceversie* is de *GepubliceerdeInt* EN er een *GegevensdienstInterfaceversie gi* is • *gi.Gegevensdienst = zg.Gegevensdienst* er • *gi.Interfaceversie* is de *VerplichteInterfacev* DAN is er een *ZorgaanbiederGegevensdienstI* *zgi2* zodat: • *zgi2.ZorgaanbiederGegevensdienst = zg* er • *zgi2.Interfaceversie* is de *VerplichteInterfac*

ZorgaanbiederGegevensdienst	Voor elke *ZorgaanbiederGegevensdienst zg* ge ALS er een *ZorgaanbiedersAbonnerenOpGegevensdienstI zagi1* is zodat: • *zagi1.ZorgaanbiederGegevensdienstInterfa ZorgaanbiederGegevensdienst = zg* en • *zagi1.ZorgaanbiederGegevensdienstInterfa Interfaceversie* is de *GepubliceerdeInterfac* EN er een *GegevensdienstAbonnerenOpGegevensdienst agi* is zodat: • *agi.Gegevensdienst = zg.Gegevensdienst* e • *agi.Interfaceversie* is de *VerplichteInterface* DAN is er een *ZorgaanbiedersAbonnerenOpGegevensdienstI zagi2* zodat: • *zagi2.ZorgaanbiederGegevensdienstInterfa ZorgaanbiederGegevensdienst = zg* en • *zagi2.ZorgaanbiederGegevensdienstInterfa Interfaceversie* is de *VerplichteInterfacevers*
ZorgaanbiederGegevensdienst	Voor elke *ZorgaanbiederGegevensdienst.Gege Systeemrolverzameling.Systeemrol s* waarvoor geldt dat *s.Transactie.Bedrijfsrol = ZorgaanbiederBedrijfsrol*, geldt dat er een *ZorgaanbiederGegevensdiens* is zodat *z.Systeemrol = s*.
ZorgaanbiederGegevensdienst	Elke *ZorgaanbiederGegevensdienst* heeft preci *DeelnemerInRolZorgaanbiederGegevensdiens* dat *d.DeelnemerInRol.Deelnemer.Rol = DienstverlenerzorgaanbiederDeelnemersrol*.
ZorgaanbiederGegevensdienstInterfaceversie	Elke *ZorgaanbiederGegevensdienstInterfaceve* precies één *AuthorizationEndpoint*.
ZorgaanbiederGegevensdienstInterfaceversie	Elke *ZorgaanbiederGegevensdienst* heeft preci *TokenEndpoint*.
ZorgaanbiederGegevensdienstSysteemrolInterfaceversie	Elke combinatie van een *ZorgaanbiederGegevensdienstInterfaceversie*

	en een *ZorgaanbiederGegevensdienstSysteem* precies één *ZorgaanbiederGegevensdienstSysteemrol*
ZorgaanbiederGegevensdienstSysteemrolInterfaceversie	*ZorgaanbiederGegevensdienstSysteemrolInter* *Systeemrol.Bedrijfsrol = ZorgaanbiederBedrijfs*
ZorgaanbiederGegevensdienstSysteemrolInterfaceversie	Elke *ZorgaanbiederGegevensdienstSysteemro* heeft precies één *ResourceEndpoint*.
ZorggebruikerBusinessrol	Er is precies één instantie hiervan.

Basisklassen

Basisklasse	Definitie
DeelnemerId	String van minimaal één en maximaal 30 tekens.
Emailadres	Semantiek: e-mailadres volgens sectie 3.4.1 van IETF RFC 5322. Syntax: string van een of meer tekens, gevolgd door het teken `@`, gevolgd door een of meer tekens, gevolgd door het teken `.`, gevolgd door twee of meer tekens. Witruimte (spatie, tab, line feed of carriage return) is niet toegestaan.
Endpointpath	Zie adresseringsverantwoordelijkheden op de Interfaces-pagina.
GegevensdienstId	String van minimaal één en maximaal 30 tekens.
Hostname	Zie adresseringsverantwoordelijkheden op de Interfaces-pagina.
HttpsUrl	Semantiek: adres van een resource die via het internet benaderbaar is volgens het HTTPS-protocol. Syntax: string die altijd start met `https://` en daarna ten minste vier karakters bevat, niet zijnde witruimtekarakters (spatie, tab, line feed of carriage return) bevat.
InterfaceversieId	String van minimaal één en maximaal 30 tekens.
LangeWeergavenaam	String van minimaal drie en maximaal 125 tekens.
NederlandseDatum	Semantiek: datum volgens lokale Nederlandse tijd. Syntax: datum volgens het type `xs:date`, zoals gespecificeerd in XML Schema 1.0, zonder tijdzone-indicatie.
Nietnegatiefgetal	Conform het type `xs:nonNegativeInteger`, zoals gespecificeerd in XML Schema 1.0.
OAuthclientOrganisatienaam	Conform toepasselijk Oauthclient-namenbeleid.
RequestUri	String van minimaal twaalf en maximaal 2048 tekens.

Systeemrolcode	String van minimaal één en maximaal 30 tekens.
Telefoonnummer	Semantiek: internationaal telefoonnummer volgens Recommendation ITU-T E.164 (11/2010). Syntax: string die altijd start met + en vervolgens bestaat uit maximaal vijftien cijfers (0 tot en met 9).
Versienummer	String van minimaal één en maximaal 30 tekens.
Weergavenaam	String van minimaal drie en maximaal 50 tekens.
YesNo	Conform het type `xs:boolean`, zoals gespecificeerd in XML Schema 1.0.
Zorgaanbiedernaam	Conform toepasselijk Zorgaanbiedersnamenbeleid.

Logische modellen

Inleiding

Er is één metamodel, maar er zijn meerdere logische modellen. Logische modellen bereiden de implementatie voor van bepaalde onderdelen van het metamodel. Deze versie van het MedMij Afsprakenstelsel kent drie logische modellen. Elk daarvan hoort bij een of enkele specifieke implementatie-component(en) in MedMij Afsprakenstelsel. Het gaat om de volgende componenten:

- de vier door *MedMij Registratie* gepubliceerde lijsten: *Gegevensdienstnamenlijst*, *OAuthclientlist*, *Whitelist* en *Zorgaanbiederslijst*;
- de in het MedMij Afsprakenstelsel te publiceren *Catalogus* van *Gegevensdiensten*;
- de in het MedMij Afsprakenstelsel te publiceren (*Hostname* van de) *MedMijStelselNode*;
- de twee van Deelnemers gevraagde rapportages: Beheerrapport en *Portabiliteitsrapport*.

De vier lijsten staan gecombineerd in één logisch model, onder de klasse *MedMijBeheerlijst*, omdat zij basiskenmerken delen. Iets dergelijks geldt voor de twee rapporten, onder de klasse *MedMijRapport*.

Vertaling van metamodel naar logisch model

Logische modellen gehoorzamen het metamodel, maar verbijzonderen dat. In de stap van metamodel naar logisch model kunnen er (logische) klassen, invarianten en basisklassen bijkomen. Maar de logische modellen bouwen vooral ook voort op het metamodel door klassen en attributen daarvan te gebruiken. In dat geval hebben logische klassen, waarde en basisklassen dus overeenkomstige klassen in het metamodel. De overeenkomsten staan hieronder bij het logische model genoemd in een tabel. Waar de tabel bij een zekere logisch klasse, waarde of basisklasse de overeenkomst met het metamodel niet noemt, is deze nieuw voor het logische niveau.

Logische klassen hebben minder of meer attributen dan de overeenkomstige klassen in het metamodel . Waar het er minder zijn, hoeven de weggelaten attributen dus niet te worden opgenomen in de te implementeren component, bijvoorbeeld van een te publiceren lijst. Waar het er meer zijn, worden deze attributen overgeërfd van een klasse in het metamodel waarvan de overeenkomstige klasse in dat metamodel bestaansafhankelijk was. In het metamodel was laatstgenoemde klasse dus toegankelijk voor de bestaansafhankelijke klasse, maar in het specifieke logische model niet meer aanwezig en dus ook niet meer toegankelijk. Zou de betreffende klasse in het logische model het attribuut dus niet hebben overgenomen, zou deze verloren zijn.

Waar een invariant uit het metamodel past binnen de scope van het specifieke logische model, verschijnt deze ook als invariant bij het logische model, hoewel de formulering zal zijn aangepast aan de ordening en naamgeving in het logische model. Daarenboven kunnen op logisch niveau ook nieuwe invarianten verschijnen. De meeste daarvan zijn vererving: in de stap van het metamodel naar een logisch model raken verbanden verbroken tussen klassen. Als die verbanden toch van belang zijn in het logische model worden er attributen uit het metamodel verorven van een bepaalde klasse in het metamodel naar een lagere klasse, waarvan wel een pendant voorkomt in het logische model. Met "lagere klasse" wordt bedoeld dat deze bestaansafhankelijk is van de andere (hogere) klasse. Zo'n vererving invariant staat opgeschreven met een . Vóór dat pijltje staat het ervende attribuut van de *logische* klasse, erachter staat het pad *in het metamodel* naar de vererende klasse.

Ook de basisklassen uit het metamodel worden, waar van toepassing, overgenomen door het logische model. Op een enkele plek verschijnen in het logische model ook nieuwe basisklassen.

Vuistregels

De logische modellen hebben een meer op implementatie toegespitste structuur dan het metamodel. Dat metamodel is gestoeld op associatieklassen en bestaansafhankelijkheid, de logische modellen zijn meer

hiërarchisch. Hiërarchie is een insnoering van associatieve bestaansafhankelijkheid, maar past beter bij menige gangbare implementatietechnologie, waaronder zeker XML, waarin de vier lijsten geïmplementeerd worden. Die insnoering betekent wel dat de logische modellen minder duurzaam en minder uitbreidbaar zijn dan het metamodel; wat voor het metamodel een eenvoudige uitbreiding is kan voor de logische modellen een stevige ingreep zijn. Dat is de prijs van hiërarchie.

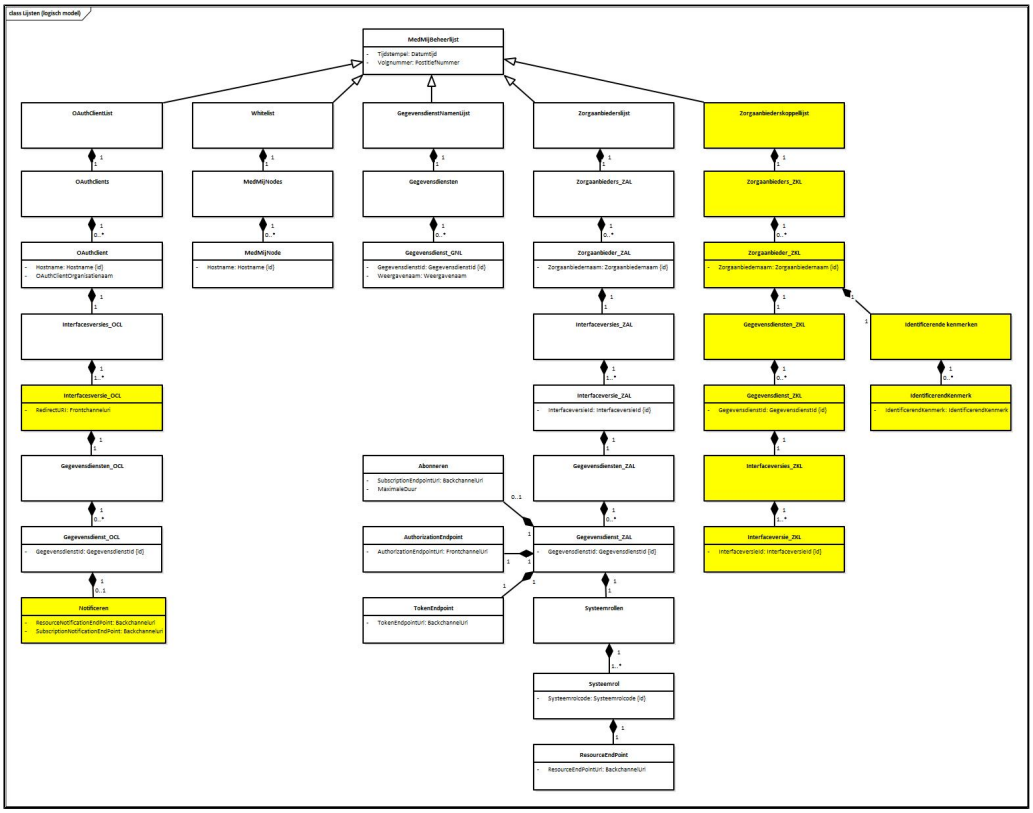
Bij de vertaling van de associativiteit van het metamodel naar de hiërarchie van de logische modellen is een aantal vuistregels gebruikt.

- De top van de hiërarchie van een logisch model wordt bepaald door de scope van de implementatiecomponent. De *Zorgaanbiederslijst*, bijvoorbeeld, somt allereerst de *Zorgaanbieders* op. Vanuit dat "logische centrum" wordt de hiërarchie van boven naar beneden afgelopen, zonder de scope van de implementatiecomponent te overschrijden. De stap naar beneden in de hiërarchie krijgt in het logische model typisch de vorm van een uses-relatie (de gestippelde pijl).
- Onderweg wordt een compositiehiërarchie aangelegd en in elke stap een selectie gemaakt uit de in het metamodel beschikbare attributen, op basis van de scope van de implementatiecomponent. Daarbij worden logische klassen niet gecombineerd tot een grofmaziger klasse, zelfs niet als er geen enkel attribuut overblijft. De klasse-granulariteit van het logische model is dus vergelijkbaar met die van het metamodel.
- Bovendien worden, zoals hierboven beschreven, attributen die in het metamodel buiten de scope dreigen te vallen, maar wel nodig zijn, vererfd naar binnen de scope. Waar dat gebeurt, wordt de vererving gepreciseerd in de lijst van logische invarianten.
- Lagere klassen in de uses-hiërarchie vallen geheel binnen de logische scope van de hogere. Een hiërarchie creëert zo ook gesloten "name spaces". Dat betekent dat hun naamgeving eenvoudiger en korter kan dan in het metamodel , waar alle contexten juist open zijn. In de logische modellen krijgen de namen van de klassen dus pas betekenis wanneer hogere klassen mee worden beschouwd. Maar dat vereenvoudigt de implementatie. In een aparte tabel bij elk logisch model wordt voorkomen dat door deze naamwijzigingen het verband met het metamodel verloren zou gaan.
- Een enkele keer heeft het vorige punt de consequentie dat er een homoniem dreigt te ontstaan binnen één logisch model (zoals `Gegevensdienst` en `Gegevensdiensten` in de logische model van de lijsten en de rapporten). In dat geval worden de namen uitgebreid zodat hun hiërarchische context zichtbaar wordt (namelijk met `_GNL`, `_OCL`, `_ZAL`, `_BR` *en* `_PR`).

Merk op dat de uses-hiërarchie de bestaansafhankelijkheidsrelatie ondersteboven zet. In de corresponderende klassen in het metamodel wordt in de uses-relatie de gebruikte klasse boven de gebruikende geplaatst, in de logische modellen juist andersom. Dit kenmerkt het doorslaggevende verschil tussen de conceptuele denkwijze van het metamodel en de bouw-gerichte denkwijze van de logische modellen. Voor de consistentie en duurzaamheid van het MedMij Afsprakenstelsel is het zaak om in het modelbeheer het metamodel centraal te plaatsen en vervolgens de logische modellen ermee in overeenstemming te houden. Het metamodel zorgt zo ook voor de duurzame consistentie tussen de verschillende logische modellen. Van die consistentie zijn de betrouwbaarheid en interoperabiliteit afhankelijk die door het MedMij Afsprakenstelsel geleverd moet worden.

Lijsten

Logisch model



Logische invarianten

Betreft instanties van logische klasse ...	Invariant	Component
Abonneren	Voor elk *Abonneren a* geldt: *a.MaximaleDuur* <= de maximale duur van *Abonnementen* op die *Gegevensdienst* zoals in de *Catalogus* aangegeven	*Zorgaanbiederslijst*
Abonneren	Voor elk *Abonneren a* geldt: *a.SubscriptionEndpointuri* combinatie van *s.MedMijNode*. *DeelnemerNode.Node.Hostname* en *s. AuthorizationEndpointpath*, conform de adresseringsverantwoordelijkheden op de Interfaces-pagina.	*Zorgaanbiederslijst*
AuthorizationEndpoint		*Zorgaanbiederslijst*

	Voor elk *AuthorizationEndpoint a* geldt: *a.AuthorizationEndpointuri* combinatie van *a.MedMijNode.DeelnemerNode.Node.Hostname* en *a.AuthorizationEndpointpath*, conform de adresseringsverantwoordelijkheden op de Interfaces-pagina.	
Gegevensdienst_OCL	Voor elke *Gegevensdienst_OCL g* met haar corresponderende *ZorgaanbiederGegevensdienst z* geldt: *g.GegevensdienstId z.Gegevensdienst.GegevensdienstId*	*Zorgaanbiederslijst*
Gegevensdienst_ZAL	Voor elke *Gegevensdienst_ZAL g* met haar corresponderende *ZorgaanbiederGegevensdienst z* geldt: *g.GegevensdienstId z.Gegevensdienst.GegevensdienstId*	*Zorgaanbiederslijst*
Gegevensdienst_ZKL	Voor elke *Gegevensdienst_ZKL g* met haar corresponderende *ZorgaanbiederGegevensdienst z* geldt: *g.GegevensdienstId z.Gegevensdienst.GegevensdienstId*	*Zorgaanbiederskoppellijst*
Gegevensdienstnamenlijst	Er is precies één instantie hiervan.	*Gegevensdienstnamenlijst*
MedMijNode	Voor elke *MedMijNode m* geldt*: m.Hostname = m.DeelnemerNode.Node.Hostname*	*Whitelist*
MedMijNode	De hostname van een *MedMijNode* bevat een domeinnaam die een fully-qualified domain name is, conform RFC3696, sectie 2.	*Whitelist*
OAuthclient	Voor elke *OAuthclient o*: *o.OAuthclientOrganisatienaam* voldoet aan het OAuthclient-namenbeleid.	*Applicatie*
OAuthclient	*Voor elke OAuthclient o geldt: o.Hostname o.MedMijNode .Hostname*.	*OAuthclientlist*
OAuthclientlist	Er is precies één instantie hiervan.	*OAuthclientlist*
ResourceEndpoint	Voor elk *ResourceEndpoint r* geldt: *r.ResourceEndpointuri* combinatie van *r.MedMijNode.DeelnemerNode.Node.Hostname en r.ResourceEndpointpath*, conform de adresseringsverantwoordelijkheden op de Interfaces-pagina.	*Zorgaanbiederslijst*

ResourceNotificationEndpoint	Voor elk *ResourceNotificationEndpoint r* geldt: *r.ResourceNotificationEndpointuri* combinatie van *r.MedMijNode*. *DeelnemerNode.Node.Hostname* en *r. AuthorizationEndpointpath*, conform de adresseringsverantwoordelijkheden op de Interfaces-pagina.	*OAuthclientlist*
SubscriptionNotificationEndpoint	Voor elk *SubscriptionNotificationEndpoint s* geldt: *s.SubscriptionNotification Endpointuri* combinatie van *s.MedMijNode*. *DeelnemerNode.Node.Hostname* en *s. AuthorizationEndpointpath*, conform de adresseringsverantwoordelijkheden op de Interfaces-pagina.	*OAuthclientlist*
Systeemrol	Voor elke *Systeemrol s* met haar corresponderende *ZorgaanbiederGegevensdienstSysteemrol z* geldt: *s.Systeemrolcode z.Systeemrol. Systeemrolcode.*	*Zorgaanbiederslijst*
TokenEndpoint	Voor elk *TokenEndpoint t* geldt: *t. TokenEndpointuri* combinatie van *t.MedMijNode. DeelnemerNode.Node.Hostname* en *t. TokenEndpointpath*, conform de adresseringsverantwoordelijkheden op de Interfaces-pagina.	*Zorgaanbiederslijst*
Whitelist	Er is precies één instantie hiervan.	*Whitelist*
Zorgaanbiederslijst	Er is precies één instantie hiervan.	*Zorgaanbiederslijst*
Zorgaanbiederskoppellijst	Er is precies één instantie hiervan.	*Zorgaanbiederskoppellijst*

Logische basisklassen

Basisklasse	Definitie	Herkomst
Backchanneluri	Zie adresseringsverantwoordelijkheden op de Interfaces-pagina. De domeinnaam is een fully-qualified domain name, conform RFC3696, sectie 2.	logisch model
DatumTijd	Conform het type `xs:dateTime`, zoals gespecificeerd in XML Schema 1.0 en inclusief een tijdzone-indicatie.	logisch model
Frontchanneluri	Zie adresseringsverantwoordelijkheden op de Interfaces-pagina. De domeinnaam is een fully-qualified domain name, conform RFC3696, sectie 2 .	logisch model

GegevensdienstId	String van minimaal één teken en maximaal 30 tekens.	metamodel
Hostname	Zie adresseringsverantwoordelijkheden op de Interfaces-pagina.	metamodel
InterfaceversieId	String van minimaal één en maximaal 30 tekens.	metamodel
OAuthclientOrganisatienaam	Conform toepasselijk Oauthclient-namenbeleid.	metamodel
Positiefnummer	Een geheel getal ongelijk 0.	logisch model
Systeemrolcode	String van minimaal één teken en maximaal 30 tekens.	metamodel
Weergavenaam	String van minimaal drie en maximaal 50 tekens.	metamodel
Zorgaanbiedernaam	Conform toepasselijk Zorgaanbiedersnamenbeleid.	metamodel

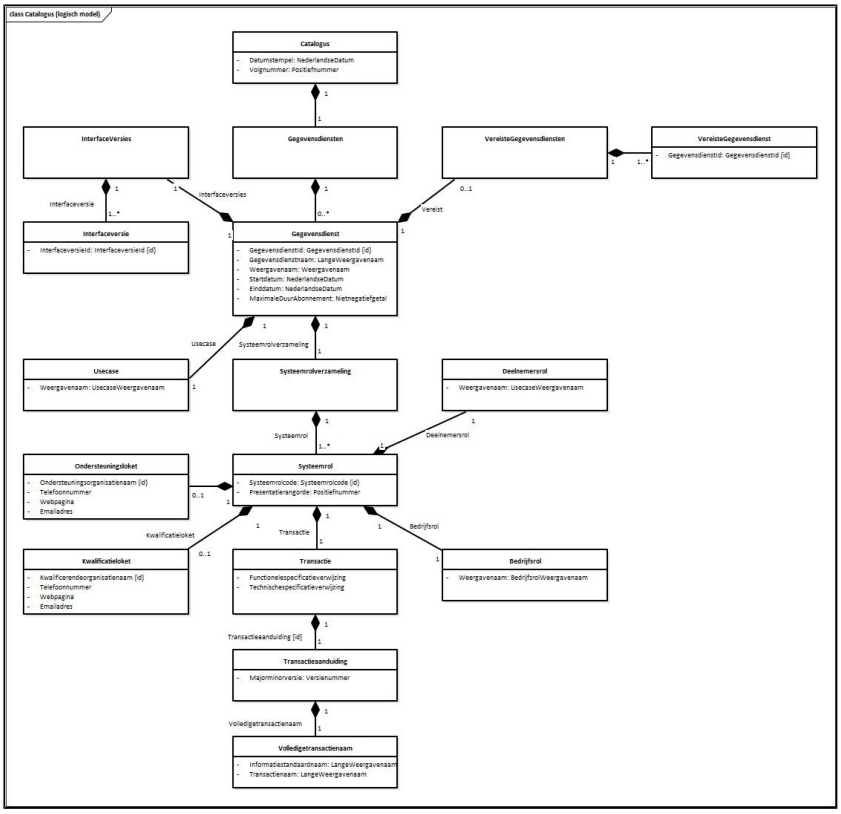
Verband met metamodel

Klasse in logisch model	Herkomstklasse in metamodel
Abonneren	*ZorgaanbiederAbonnerenOpGevensdienstInterfaceversie*
AuthorizationEndpoint	*AuthorizationEndpoint*
Gegevensdienst_GNL	*Gegevensdienst*
Gegevensdienst_OCL	*OAuthclientGegevensdienstInterfaceversie*
Gegevensdienst_ZAL	*ZorgaanbiederGegevensdienstInterfaceversie*
Interfaceversie_OCL	*OAuthclientInterfaceversie*
MedMijNode	*MedMijNode*
OAuthclient	*OAuthclient*
ResourceEndpoint	*ResourceEndpoint*
ResourceNotificationEndpoint	*ResourceNotificationEndpoint*
SubscriptionNotificationEndpoint	*SubscriptionNotificationEndpoint*
Systeemrol	*ZorgaanbiederGegevensdienstInterfaceversieSysteemrol*
TokenEndpoint	*TokenEndpoint*
Zorgaanbieder_ZAL	*Zorgaanbieder*
Zorgaanbieder_ZKL	*Zorgaanbieder*

De klasse Interfaceversie_ZAL in het logisch model heeft een corresponderende conceptuele klasse "ZorgaanbiederInterfaceversie" die nog niet is opgenomen in het metamodel. Deze klasse is een associatie van de klassen "Zorgaanbieder" en "Interfaceversie".

Catalogus

Logisch model



Logische invarianten

Betreft instanties van klasse ...	Invariant	Component	Toelichting	Aard	Herkomst
Catalogus	Er is precies één instantie hiervan.	*Catalogus*	Dit is een eenling in het model.	getalsverhouding	logisch model
Systeemrol	Voor elke *Systeemrol s* geldt: *s.Presentatievolgorde* wordt bepaald door de relatieve positie van de systeemrol in de tijdsvolgorde waarin *s. Transactie* binnen de uitvoering van *s. Systeemrolverzameling. Gegevensdienst.Usecase* zijn werk moet doen. Daarbij gelden als elkaar aanvullende richtlijnen:	*Catalogus*	De volgorde waarin die *Systeemrolcodes* bij een *Gegevensdienst* staan opgesomd is formeel om het even, maar voor de presentatie wel relevant. Die volgorde van presentatie komt overeen met de	lokale afhankelijkheid	logisch model

	• een *Transactie t* met *t. Bedrijfsrol*: *PatiëntBedrijfsrol* gaat vooraf aan een *Transactie t* met *t. Bedrijfsrol* : *ZorgaanbiederBedrijfsrol* ; • bij meerdere *Transacties* van hetzelfde type: in tijdsvolgorde van de transactie.		tijdsvolgorde waarin de betreffende *Systeemrollen* hun werk moeten doen.		

Logische basisklassen

Basisklasse	Definitie	Herkomst
BedrijfsrolWeergavenaam	String met de waarde "Patiënt" of "Zorgaanbieder".	logisch model
DeelnemersrolWeergavenaam	String met de waarde "Dienstverlener persoon" of "Dienstverlener zorgaanbieder".	logisch model
Emailadres	Semantiek: e-mailadres volgens sectie 3.4.1 van IETF RFC 5322. Syntax: string van een of meer tekens, gevolgd door het teken @, gevolgd door een of meer tekens, gevolgd door het teken `.`, gevolgd door twee of meer tekens. Witruimte (spatie, tab, line feed of carriage return) is niet toegestaan.	metamodel
GegevensdienstId	String van minimaal één teken en maximaal 30 tekens.	metamodel
HttpsUrl	Semantiek: adres van een resource die via het internet benaderbaar is volgens het HTTPS-protocol. Syntax: string die altijd start met `https://` en daarna ten minste vier karakters bevat, niet zijnde witruimtekarakters (spatie, tab, line feed of carriage return) bevat.	metamodel
LangeWeergavenaam	String van minimaal één en maximaal 125 tekens.	metamodel
NederlandseDatum	Semantiek: datum volgens lokale Nederlandse tijd. Syntax: datum volgens het type `xs:date`, zoals gespecificeerd in XML Schema 1.0, zonder tijdzone-indicatie.	metamodel
Nietnegatiefgetal	Conform het type `xs:nonNegativeInteger`, zoals gespecificeerd in XML Schema 1.0.	metamodel
Positiefnummer	Een geheel getal ongelijk 0.	logisch model

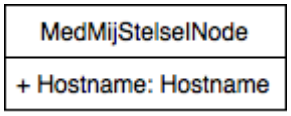
Systeemrolcode	String van minimaal één teken en maximaal 30 tekens.	metamodel
Telefoonnummer	Semantiek: internationaal telefoonnummer volgens Recommendation ITU-T E.164 (11/2010). Syntax: string die altijd start met + en vervolgens bestaat uit maximaal vijftien cijfers (0 tot en met 9).	metamodel
UsecaseWeergavenaam	String met de waarde "Verzamelen" of "Delen".	logisch model
Versienummer	String van minimaal één en maximaal 30 tekens.	metamodel
Weergavenaam	String van minimaal drie en maximaal 50 tekens.	metamodel

Verband met metamodel

Klasse/waarde in logisch model	Herkomstklasse in metamodel
Gegevensdienst	*Gegevensdienst*
Usecase	*Usecase*
Interfaceversie	*Interfaceversie*
Transactie	*Transactie*
Bedrijfsrol	*Bedrijfsrol*
Ondersteuningsloket	*Ondersteuningsloket*
Kwalificatieloket	*Kwalificatieloket*
Transactieaanduiding	*Transactieaanduiding*
Volledigetransactienaam	*Volledigetransactienaam*
Deelnemersrol	*Deelnemersrol*
VereisteGegevensdienst	*Gegevensdienst*

MedMijStelselNode

Logisch model



Logische invarianten

Betreft instanties van klasse ...	Invariant	Component	Toelichting	Aard
MedMijStelselNode	Voor de *MedMijStelselNode m*	*MedMijStelselNode*	Zo erft de *MedMijStelselNode*,	vererving

	geldt: *m.Hostname m. Node.Hostname*		van de *Node* die het is, de *Hostname*.	

Logische basisklassen

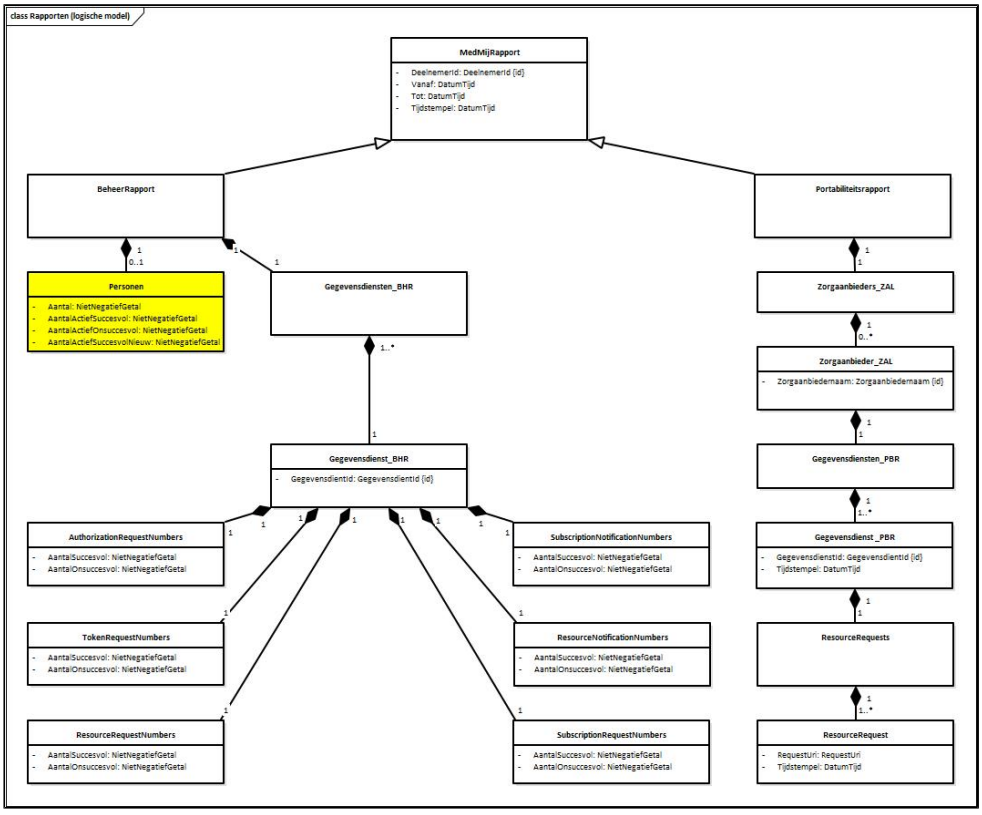
Basisklasse	Definitie	Herkomst
Hostname	Zie adresseringsverantwoordelijkheden op de Interfaces-pagina.	metamodel

Verband met metamodel

Klasse in logisch model	Herkomstklasse in metamodel
MedMijStelselNode	*MedMijStelselNode*

Rapporten

Logisch model



Logische invarianten

Betreft instanties van logische klasse ...	Invariant	Component	Toelichting	Aard
Beheerrapport	Er is precies één instantie hiervan.	*Beheerrapport*	Dit is een eenling in het model.	getalsve

Gegevensdienst_BR	Voor elke *Gegevensdienst_BR g* met haar corresponderende *ZorgaanbiederGegevensdienst z* geldt: *g.GegevensdienstId z. Gegevensdienst. GegevensdienstId*	*Beheerrapport*	Zo erft het *Beheerrapport* de *GegevensdienstId* 's van de *Catalogus* .	verervin
Gegevensdienst_PR	Voor elke *Gegevensdienst_PR g* met haar corresponderende *ZorgaanbiederGegevensdienst z* geldt: *g.GegevensdienstId z. Gegevensdienst. GegevensdienstId*	*Portabiliteitsrapport*	Zo erft het *Portabiliteitsrapport* de *GegevensdienstId* 's van de *Catalogus* .	verervin
Portabiliteitsrapport	Er is precies één instantie hiervan.	*Portabiliteitsrapport*	Dit is een eenling in het model.	getalsve

Logische basisklassen

Basisklasse	Definitie	Herkomst
DatumTijd	Conform het type `xs:dateTime`, zoals gespecificeerd in XML Schema 1.0 en inclusief een tijdzone-indicatie.	logisch model
DeelnemerId	String van minimaal één en maximaal 30 tekens.	metamodel
GegevensdienstId	String van minimaal één teken en maximaal 30 tekens.	metamodel
Nietnegatiefgetal	Conform het type `xs:nonNegativeInteger`, zoals gespecificeerd in XML Schema 1.0.	logisch model
RequestUri	String van minimaal twaalf en maximaal 2048 tekens.	metamodel
Zorgaanbiedernaam	Conform toepasselijk Zorgaanbiedersnamenbeleid.	metamodel

Verband met metamodel

Klasse in logisch model	Herkomstklasse in metamodel
Gegevensdienst_BR	*Gegevensdienst*
Gegevensdienst_PR	*Gegevensdienst*
ResourceRequest	*ResourceRequest*
Zorgaanbieder	*Zorgaanbieder*

XML-schema's

Inleiding

Op deze pagina staan de XML-schema's van:

- de lijsten die door *MedMij Beheer* aan *Bron* en *Uitgever* voor uiteenlopende doelen ter beschikking worden gesteld;
- de rapporten die door *Deelnemers* moeten kunnen worden opgeleverd;
- de *Catalogus.*

De XML-schema's zijn een implementatie van de relevante logische modellen in XML-syntax en vervullen daarom de rol van technisch model. XML past bij de hiërarchische structurering waarop al in de logische modellen is ingezet.

Net als op het conceptuele niveau van het metamodel en op het logisch niveau van het logische model, verschijnen op het technische niveau ook invarianten. XML is zelfs in staat om sommige van die invarianten geautomatiseerd te controleren. In zulke XML-validatie wordt gecontroleerd of een zeker XML-bestand voldoet aan de structuur van een zeker XML-schema. Ook het MedMij Afsprakenstelsel maakt van deze gelegenheid gebruik door van ontvanger van de vier lijsten te eisen zo'n validatie uit te voeren. De XML-schema's daarvoor worden als onderdeel van het MedMij Afsprakenstelsel beschikbaar gesteld. Deze validatie biedt extra zekerheid over de juistheid van de verspreide lijsten en draagt zo bij aan de betrouwbaarheid van het functioneren van het MedMij-netwerk.

Toch zijn er nog verschillende manieren om het logische model van de lijsten in hun XML-schema's te vertalen. In het MedMij Afsprakenstelsel zijn daarbij de volgende afwegingen gebruikt:

- Alle typen en elementen die worden gebruikt voor een van de lijsten of rapporten, zijn in het XML-schema van de betreffende lijst of het betreffende rapport gedefinieerd. Er is dus geen gebruik gemaakt van een basisschema. Zo wordt de afhankelijkheid tussen de XML-schema's beperkt en wordt het gemakkelijker een van de schema's aan te passen zonder dat de andere schema's gewijzigd worden. De definities moeten echter blijven passen bij het metamodel en het logische model ; een aanpassing in een van deze modellen maakt aanpassing noodzakelijk van alle XML-schema's die door de wijziging geraakt worden.
- Bij het logische model van de lijsten en rapporten horen vier technische componenten. De hoogste klasse van elke component wordt het rootelement van het betreffende XML-schema. De attributen van de abstracte klassen bovenaan (*MedMijBeheerlijst* en *MedMijRapport*) worden over de technische modellen van de vier lijsten, respectievelijk de twee rapporten, verspreid. Er is dus voor elke lijst of rapport een apart XML-schema. Daardoor is de homonymie van `Gegevensdienst` en `Gegevensdiensten` geen probleem meer en kunnen in de namen de achtervoegsels `_ZAL`, `_GNL`, `_OCL`, `_BR` en `_PR` achterwege blijven.
- De *Catalogus* vormt kent een zelfstandig logisch model. De klasse *Catalogus* uit het logisch model dient als root element van het XML-schema van de *Catalogus*.
- Net als in de stap van het metamodel naar de logische modellen blijft de granulariteit van de klassen hetzelfde: er worden geen klassen samengenomen om een compacter schema te maken.
- Alle klassen en attributen uit het logische model zijn gemodelleerd als elementen in het XML-schema. Daarmee is een eenduidige vertaling mogelijk van het logische model; er behoeft geen onderscheid tussen elementen en attributen te worden aangebracht. Elementen bieden meer mogelijkheden dan attributen en genieten daarom (als generieke keuze) de voorkeur.

Schema's

> De verschillende schema's die zijn opgesteld voor versie 1.5.0 van het afsprakenstelsel gelden ook voor deze versie (1.5.1). Daarom wordt in de verschillende schema's nog verwezen naar versie 1.5.0.

Lijst of rapport	Bestandsnaam	Release	Versie bestand
Whitelist	MedMij_Whitelist.1.5.0.xsd	2	13
Zorgaanbiederslijst	MedMij_Zorgaanbiederslijst.1.5.0.xsd	3	12
OAuthclientlist	MedMij_OAuthclientlist.1.5.0.xsd	5	14
Gegevensdienstnamenlijst	MedMij_Gegevensdienstnamenlijst.1.5.0.xsd	1	11
Beheerrapport	MedMij_Beheerrapport.1.5.0.xsd	2	7
Portabiliteitsrapport	MedMij_Portabiliteitsrapport.1.5.0.xsd	1	8
Zorgaanbiederskoppellijst	MedMij_Zorgaanbiederskoppellijst.1.5.0.xsd	1	4

Alleen de hierboven genoemde bestanden, met de aangegeven release en versie, mogen worden gebruikt in deze release van het MedMij Afsprakenstelsel.

Voorbeeldbestanden

> De verschillende voorbeeldbestanden die zijn opgesteld voor versie 1.5.0 van het afsprakenstelsel gelden ook voor deze versie (1.5.1). Daarom wordt in de verschillende voorbeeldbestanden nog verwezen naar versie 1.5.0.

Van elke lijst is een voorbeeldbestand beschikbaar. Dit bestand maakt geen deel uit van de formele specificaties van het MedMij Afsprakenstelsel. De *Catalogus* kent geen voorbeeldbestand.

Lijst	Bestandsnaam	Versie voorbeeldbestand	Behorend b XML-schen van de lijst met releasenum
Whitelist	MedMij_Whitelist_example.1.5.0.xml	9	2
Zorgaanbiederslijst	MedMij_Zorgaanbiederslijst_example.1.5.0.xml	9	3
OAuthclientlist	MedMij_OAuthclientlist_example.1.5.0.xml	11	5
Gegevensdienstnamenlijst	MedMij_Gegevensdienstnamenlijst_example.1.5.0.xml	8	1
Beheerrapport	MedMij_Beheerrapport_example.1.5.0.xml	9	2
Portabiliteitsrapport	MedMij_Portabiliteitsrapport_example.1.5.0.xml	9	1
Zorgaanbiederkoppellijst	MedMij_Zorgaanbiederskoppellijst_example.1.5.0.xml	5	1

Tijdaspect

Het metamodel en de logische modellen, met hun invarianten, werken "door de tijd". Zij beschrijven hoe de klassen samenhangen op elk moment. De XML-bestanden voor de lijsten zijn echter specifieke momentopnames van de instanties van de klassen. Er moet daarom een tijdselement worden toegevoegd om lijsten die op verschillende momenten zijn gegenereerd, uit elkaar te kunnen houden, en om in retrospectief de geldigheidstermijn van een lijst te kunnen vaststellen.

- Elk XML-bestand kent een versie-aanduiding. Hiertoe wordt de combinatie van een `Volgnummer` en een `Tijdstempel` gebruikt. Hiermee wordt aan drie informatiebehoeften tegemoet gekomen:
  - Wanneer twee lijsten (van hetzelfde type) met opeenvolgende `Volgnummers` beschikbaar zijn, kan de geldigheidstermijn van de oudere lijst worden vastgesteld. Dat helpt bij de interpretatie van audit logs of foutopsporing.
  - Lijsten kunnen uniek worden geïdentificeerd. Dit kan aan de hand van `Volgnummer` of `Tijdstempel`, waarbij `Volgnummer` voor menselijke gebruikers vaak de meest intuïtieve zal zijn.
  - Per lijst kan worden nagegaan wanneer de laatste mutatie heeft plaatsgevonden. Dit zal in de regel een 'functionele' mutatie betreffen, geen foutherstel. Hieruit kan door vergelijking van opeenvolgende versies worden afgeleid wanneer de actuele lijst voor het laatst is gewijzigd; dat kan zinvol zijn bij het beoordelen van de effecten van changes of bij foutopsporing.
- `Tijdstempel` bestaat uit Datum, Tijd en Tijdzone-aanduiding, gebaseerd op `xs:dateTime`-type. Door voor een native XML-datatype te kiezen, wordt de implementatie vergemakkelijkt. Er geldt wel een restrictie op het element, dat afdwingt dat er altijd een Tijdzone-aanduiding wordt meegegeven.
- Voor de *Catalogus* geldt een uitzondering, en wordt gebruikgemaakt van een uitdrukking van de lokale Nederlandse datum (`xs:date`-type zonder tijdzone-aanduiding).

Releasebeheer

De bestandsnamen van de XML-schema's en XML-voorbeeldbestanden zijn zo gekozen dat zij niet wijzigen wanneer de inhoud van het XML-schema wijzigt. Dit vergemakkelijkt de implementatie van changes. Het is gebruikelijk om meta-informatie niet in de bestandsnaam op te nemen, maar in de XML-bestanden zelf (met name in de header). Daarom is het niet nodig om naast de informatie in het bestand, ook de bestandsnaam in te zetten voor versie-aanduiding.

Elk van de XML-schema's kent een eigen releasenummering. Zij kunnen daarmee onafhankelijk van elkaar worden aangepast. Daarmee wordt onnodige implementatielast bij een wijziging voorkomen. Het releasenummer is een geheel getal, om redenen van eenvoud. Altijd en alleen indien een XML-schema is gewijzigd, wordt het releasenummer met één opgehoogd.

De XML-schema's zijn integraal onderdeel van het afsprakenstelsel. Een wijziging van de XML-schema's leidt dan ook tot een nieuwe release van het afsprakenstelsel. Omgekeerd hoeft het niet zo te zijn dat een wijziging in de overige afspraken binnen het afsprakenstelsel, een wijziging van het XML-schema noodzakelijk maakt.

Omdat een wijziging in een XML-schema al snel tot incompatibiliteit met andere versies leidt (XML-bestanden die gebaseerd zijn op verschillende versies van het XML-schema zullen niet door het 'andere' XML-schema worden gevalideerd), is ervoor gekozen om het releasenummer op te nemen in de aanduiding van de namespace. Daarmee draagt een XML-bestand in de verwijzing naar de namespace tevens het releasenummer in zich. Zo wordt geborgd dat XML-bestanden niet met een verkeerde versie van het XML-schema worden gevalideerd.

De XML-schema's en de voorbeeld-XML-bestanden krijgen daarnaast een versienummer mee. Het versienummer is een geheel getal en wordt bij elke wijziging in het bestand met één opgehoogd. Met behulp van versienummering kunnen bestandsversies gedurende de ontwikkeling uit elkaar worden gehouden. Het nummer is ook aanwezig in productieversies; het is daarmee niet noodzakelijk om bij een statuswijziging van een release van het MedMij Afsprakenstelsel de XML-producten aan te passen, ook als die inhoudelijk niet gewijzigd zijn. Het versienummer wordt opgenomen als commentaar in het bestand, omdat dat niet machine-

leesbaar hoeft te zijn en er op deze manier een eenduidige systematiek bestaat voor de XML-schema's en de XML-voorbeeldbestanden. Het commentaar heeft de vorm: `<!--File version: [versienummer]-->` en bevindt zich op de tweede regel van een bestand. De versienummering is, om redenen van eenvoud en duidelijkheid, onafhankelijk van de releasenummering van de XML-schema's.

Namespaces

Voor de aanduiding van namespaces wordt gebruikgemaakt van een URL. Dit is de gemakkelijkste optie, omdat dit - anders dan bij een URN - geen namespaceregistratie bij IANA vereist. De namespace-URL kent de volgende opbouw: `xmlns://afsprakenstelsel.medmij.nl/[naamLijst|naamRapport|"catalogus"]/release[releasenummer]` .

- Een namespace-URL gebruikt `xmlns://` als schema-aanduiding. Daarmee wordt duidelijk gemaakt dat het slechts een identificatie betreft, en dat de URL niet is bedoeld voor dereferencing (bijvoorbeeld om het XML-schema te downloaden).
- Het domein `afsprakenstelsel.medmij.nl` is een unieke hostname op het internet. Gebruik daarvan biedt zowel voldoende herkenbaarheid als uniciteit.
- De `naamLijst` kent één van de volgende waarden: `Whitelist`, `OAuthclientlist`, `Zorgaanbiederslijst` of `Gegevensdienstnamenlijst`.
- De `naamRapport` kent één van de volgende waarden: `Beheerrapport` of `Portabiliteitsrapport`.
- De aanduiding `release` is toegevoegd voor de menselijke leesbaarheid en daarmee duidelijkheid.

Waar het metamodel geen namen heeft gedefinieerd, kiezen we om redenen van consistentie en elegantie voor lowercase in de opbouw van de URL. Er wordt gebruikgemaakt van `elementFormDefault = "qualified"`. Dit vergroot de leesbaarheid van de XML-schema's omdat er geen prefixes nodig zijn bij het definiëren van elementen, en doet niet af aan enige functionaliteit.

Syntactische keuzes

De XML-schema's gaan uit van XML 1.0 en XML Schema 1.0 (opgebouwd uit specificaties aangaande structuur en datatypes). Deze versies bieden voldoende functionaliteit en kennen een zeer brede implementatie en ondersteuning.

De bestandsnaam van een XML-schema kent de opbouw `MedMij_[naamLijst].xsd`. De variabele `naamLijst` betreft één van de volgende waarden: `Whitelist`, `OAuthclientlist`, `Zorgaanbiederslijst` of `Gegevensdienstnamenlijst.`

De XML-schema's bevatten de XML Declaration `<?xml version="1.0" encoding="UTF-8"?>`. De aanwezigheid van een declaratie wordt aanbevolen door XML 1.0. De encoding is optioneel bij het gebruik van UTF-8. De encoding is echter toch expliciet omdat dit mogelijke onzekerheid over de bedoeling of het correct volgen van de specificaties voorkomt. Er wordt geen gebruik gemaakt van het pseudo-attribuut `standalone`, omdat er gebruik gemaakt wordt van XML-schema's in plaats van DTD's.

Omwille van de leesbaarheid zijn de XML-schema's pretty-printed; door het gebruik van regeleinden en inspringing wordt de leesbaarheid vergroot. Verder kent elk XML-schema een standaardvolgorde in haar opbouw:

- Het rootelement, voorafgegaan door de commentaartekst `<!--Rootelement-->`.
- De definitie van de logische klassen, voorafgegaan door de commentaartekst `<!–Logische klassen-->`.
- De definitie van de basisklassen, voorafgegaan door de commentaartekst `<!--Basisklassen-->`.

De volgorde waarin de klassen worden gedefinieerd is hierbinnen vrij.

De XML-schema's bevatten geen Byte Order Mark. Het gebruik van een Byte Order Mark is volgens XML 1.0 optioneel bij UTF-8. RFC 3629, hoofdstuk 6, stelt dat het Byte Order Mark verboden moet worden, daar waar UTF-8 verplicht wordt gesteld.

Inleiding

Op deze pagina staan de XML-schema's van:

- de lijsten die door *MedMij Beheer* aan *Bron* en *Uitgever* voor uiteenlopende doelen ter beschikking worden gesteld;
- de rapporten die door *Deelnemers* moeten kunnen worden opgeleverd;
- de *Catalogus.*

De XML-schema's zijn een implementatie van de relevante logische modellen in XML-syntax en vervullen daarom de rol van technisch model. XML past bij de hiërarchische structurering waarop al in de logische modellen is ingezet.

Net als op het conceptuele niveau van het metamodel en op het logisch niveau van het logische model, verschijnen op het technische niveau ook invarianten. XML is zelfs in staat om sommige van die invarianten geautomatiseerd te controleren. In zulke XML-validatie wordt gecontroleerd of een zeker XML-bestand voldoet aan de structuur van een zeker XML-schema. Ook het MedMij Afsprakenstelsel maakt van deze gelegenheid gebruik door van ontvanger van de vier lijsten te eisen zo'n validatie uit te voeren. De XML-schema's daarvoor worden als onderdeel van het MedMij Afsprakenstelsel beschikbaar gesteld. Deze validatie biedt extra zekerheid over de juistheid van de verspreide lijsten en draagt zo bij aan de betrouwbaarheid van het functioneren van het MedMij-netwerk.

Toch zijn er nog verschillende manieren om het logische model van de lijsten in hun XML-schema's te vertalen. In het MedMij Afsprakenstelsel zijn daarbij de volgende afwegingen gebruikt:

- Alle typen en elementen die worden gebruikt voor een van de lijsten of rapporten, zijn in het XML-schema van de betreffende lijst of het betreffende rapport gedefinieerd. Er is dus geen gebruik gemaakt van een basisschema. Zo wordt de afhankelijkheid tussen de XML-schema's beperkt en wordt het gemakkelijker een van de schema's aan te passen zonder dat de andere schema's gewijzigd worden. De definities moeten echter blijven passen bij het metamodel en het logische model ; een aanpassing in een van deze modellen maakt aanpassing noodzakelijk van alle XML-schema's die door de wijziging geraakt worden.
- Bij het logische model van de lijsten en rapporten horen vier technische componenten. De hoogste klasse van elke component wordt het rootelement van het betreffende XML-schema. De attributen van de abstracte klassen bovenaan (*MedMijBeheerlijst* en *MedMijRapport*) worden over de technische modellen van de vier lijsten, respectievelijk de twee rapporten, verspreid. Er is dus voor elke lijst of rapport een apart XML-schema. Daardoor is de homonymie van `Gegevensdienst` en `Gegevensdiensten` geen probleem meer en kunnen in de namen de achtervoegsels `_ZAL`, `_GNL`, `_OCL`, `_BR` en `_PR` achterwege blijven.
- De *Catalogus* vormt kent een zelfstandig logisch model. De klasse *Catalogus* uit het logisch model dient als root element van het XML-schema van de *Catalogus*.
- Net als in de stap van het metamodel naar de logische modellen blijft de granulariteit van de klassen hetzelfde: er worden geen klassen samengenomen om een compacter schema te maken.
- Alle klassen en attributen uit het logische model zijn gemodelleerd als elementen in het XML-schema. Daarmee is een eenduidige vertaling mogelijk van het logische model; er behoeft geen onderscheid tussen elementen en attributen te worden aangebracht. Elementen bieden meer mogelijkheden dan attributen en genieten daarom (als generieke keuze) de voorkeur.

Schema's

Lijst of rapport	Bestandsnaam	Release	Versie bestand

Whitelist	MedMij_Whitelist.1.5.0.xsd	2	13
Zorgaanbiederslijst	MedMij_Zorgaanbiederslijst.1.5.0.xsd	3	12
OAuthclientlist	MedMij_OAuthclientlist.1.5.0.xsd	5	14
Gegevensdienstnamenlijst	MedMij_Gegevensdienstnamenlijst.1.5.0.xsd	1	11
Beheerrapport	MedMij_Beheerrapport.1.5.0.xsd	2	7
Portabiliteitsrapport	MedMij_Portabiliteitsrapport.1.5.0.xsd	1	8
Zorgaanbiederskoppellijst	MedMij_Zorgaanbiederskoppellijst.1.5.0.xsd	1	4

Alleen de hierboven genoemde bestanden, met de aangegeven release en versie, mogen worden gebruikt in deze release van het MedMij Afsprakenstelsel.

Voorbeeldbestanden

Van elke lijst is een voorbeeldbestand beschikbaar. Dit bestand maakt geen deel uit van de formele specificaties van het MedMij Afsprakenstelsel. De *Catalogus* kent geen voorbeeldbestand.

Lijst	Bestandsnaam	Versie voorbeeldbestand	Behorend b XML-schen van de lijst met releasenum
Whitelist	MedMij_Whitelist_example.1.5.0.xml	9	2
Zorgaanbiederslijst	MedMij_Zorgaanbiederslijst_example.1.5.0.xml	9	3
OAuthclientlist	MedMij_OAuthclientlist_example.1.5.0.xml	11	5
Gegevensdienstnamenlijst	MedMij_Gegevensdienstnamenlijst_example.1.5.0.xml	8	1
Beheerrapport	MedMij_Beheerrapport_example.1.5.0.xml	9	2
Portabiliteitsrapport	MedMij_Portabiliteitsrapport_example.1.5.0.xml	9	1
Zorgaanbiederkoppellijst	MedMij_Zorgaanbiederskoppellijst_example.1.5.0.xml	5	1

Tijdaspect

Het metamodel en de logische modellen, met hun invarianten, werken "door de tijd". Zij beschrijven hoe de klassen samenhangen op elk moment. De XML-bestanden voor de lijsten zijn echter specifieke momentopnames van de instanties van de klassen. Er moet daarom een tijdselement worden toegevoegd om lijsten die op verschillende momenten zijn gegenereerd, uit elkaar te kunnen houden, en om in retrospectief de geldigheidstermijn van een lijst te kunnen vaststellen.

- Elk XML-bestand kent een versie-aanduiding. Hiertoe wordt de combinatie van een `Volgnummer` en een `Tijdstempel` gebruikt. Hiermee wordt aan drie informatiebehoeften tegemoet gekomen:

    - Wanneer twee lijsten (van hetzelfde type) met opeenvolgende `Volgnummers` beschikbaar zijn, kan de geldigheidstermijn van de oudere lijst worden vastgesteld. Dat helpt bij de interpretatie van audit logs of foutopsporing.
    - Lijsten kunnen uniek worden geïdentificeerd. Dit kan aan de hand van `Volgnummer` of `Tijdstempel`, waarbij `Volgnummer` voor menselijke gebruikers vaak de meest intuïtieve zal zijn.
    - Per lijst kan worden nagegaan wanneer de laatste mutatie heeft plaatsgevonden. Dit zal in de regel een 'functionele' mutatie betreffen, geen foutherstel. Hieruit kan door vergelijking van opeenvolgende versies worden afgeleid wanneer de actuele lijst voor het laatst is gewijzigd; dat kan zinvol zijn bij het beoordelen van de effecten van changes of bij foutopsporing.
- `Tijdstempel` bestaat uit Datum, Tijd en Tijdzone-aanduiding, gebaseerd op `xs:dateTime`-type. Door voor een native XML-datatype te kiezen, wordt de implementatie vergemakkelijkt. Er geldt wel een restrictie op het element, dat afdwingt dat er altijd een Tijdzone-aanduiding wordt meegegeven.
- Voor de *Catalogus* geldt een uitzondering, en wordt gebruikgemaakt van een uitdrukking van de lokale Nederlandse datum (`xs:date`-type zonder tijdzone-aanduiding).

Releasebeheer

De bestandsnamen van de XML-schema's en XML-voorbeeldbestanden zijn zo gekozen dat zij niet wijzigen wanneer de inhoud van het XML-schema wijzigt. Dit vergemakkelijkt de implementatie van changes. Het is gebruikelijk om meta-informatie niet in de bestandsnaam op te nemen, maar in de XML-bestanden zelf (met name in de header). Daarom is het niet nodig om naast de informatie in het bestand, ook de bestandsnaam in te zetten voor versie-aanduiding.

Elk van de XML-schema's kent een eigen releasenummering. Zij kunnen daarmee onafhankelijk van elkaar worden aangepast. Daarmee wordt onnodige implementatielast bij een wijziging voorkomen. Het releasenummer is een geheel getal, om redenen van eenvoud. Altijd en alleen indien een XML-schema is gewijzigd, wordt het releasenummer met één opgehoogd.

De XML-schema's zijn integraal onderdeel van het afsprakenstelsel. Een wijziging van de XML-schema's leidt dan ook tot een nieuwe release van het afsprakenstelsel. Omgekeerd hoeft het niet zo te zijn dat een wijziging in de overige afspraken binnen het afsprakenstelsel, een wijziging van het XML-schema noodzakelijk maakt.

Omdat een wijziging in een XML-schema al snel tot incompatibiliteit met andere versies leidt (XML-bestanden die gebaseerd zijn op verschillende versies van het XML-schema zullen niet door het 'andere' XML-schema worden gevalideerd), is ervoor gekozen om het releasenummer op te nemen in de aanduiding van de namespace. Daarmee draagt een XML-bestand in de verwijzing naar de namespace tevens het releasenummer in zich. Zo wordt geborgd dat XML-bestanden niet met een verkeerde versie van het XML-schema worden gevalideerd.

De XML-schema's en de voorbeeld-XML-bestanden krijgen daarnaast een versienummer mee. Het versienummer is een geheel getal en wordt bij elke wijziging in het bestand met één opgehoogd. Met behulp van versienummering kunnen bestandsversies gedurende de ontwikkeling uit elkaar worden gehouden. Het nummer is ook aanwezig in productieversies; het is daarmee niet noodzakelijk om bij een statuswijziging van een release van het MedMij Afsprakenstelsel de XML-producten aan te passen, ook als die inhoudelijk niet gewijzigd zijn. Het versienummer wordt opgenomen als commentaar in het bestand, omdat dat niet machine-leesbaar hoeft te zijn en er op deze manier een eenduidige systematiek bestaat voor de XML-schema's en de XML-voorbeeldbestanden. Het commentaar heeft de vorm: `<!--File version: [versienummer]-->` en bevindt zich op de tweede regel van een bestand. De versienummering is, om redenen van eenvoud en duidelijkheid, onafhankelijk van de releasenummering van de XML-schema's.

Namespaces

Voor de aanduiding van namespaces wordt gebruikgemaakt van een URL. Dit is de gemakkelijkste optie, omdat dit - anders dan bij een URN - geen namespaceregistratie bij IANA vereist. De namespace-URL kent de volgende opbouw: `xmlns://afsprakenstelsel.medmij.nl/[naamLijst|naamRapport|"catalogus"]/release[releasenummer]` .

- Een namespace-URL gebruikt `xmlns://` als schema-aanduiding. Daarmee wordt duidelijk gemaakt dat het slechts een identificatie betreft, en dat de URL niet is bedoeld voor dereferencing (bijvoorbeeld om het XML-schema te downloaden).
- Het domein `afsprakenstelsel.medmij.nl` is een unieke hostname op het internet. Gebruik daarvan biedt zowel voldoende herkenbaarheid als uniciteit.
- De `naamLijst` kent één van de volgende waarden: `Whitelist`, `OAuthclientlist`, `Zorgaanbiederslijst` of `Gegevensdienstnamenlijst`.
- De `naamRapport` kent één van de volgende waarden: `Beheerrapport` of `Portabiliteitsrapport`.
- De aanduiding `release` is toegevoegd voor de menselijke leesbaarheid en daarmee duidelijkheid.

Waar het metamodel geen namen heeft gedefinieerd, kiezen we om redenen van consistentie en elegantie voor lowercase in de opbouw van de URL. Er wordt gebruikgemaakt van `elementFormDefault = "qualified"`. Dit vergroot de leesbaarheid van de XML-schema's omdat er geen prefixes nodig zijn bij het definiëren van elementen, en doet niet af aan enige functionaliteit.

Syntactische keuzes

De XML-schema's gaan uit van XML 1.0 en XML Schema 1.0 (opgebouwd uit specificaties aangaande structuur en datatypes). Deze versies bieden voldoende functionaliteit en kennen een zeer brede implementatie en ondersteuning.

De bestandsnaam van een XML-schema kent de opbouw `MedMij_[naamLijst].xsd`. De variabele `naamLijst` betreft één van de volgende waarden: `Whitelist`, `OAuthclientlist`, `Zorgaanbiederslijst` of `Gegevensdienstnamenlijst.`

De XML-schema's bevatten de XML Declaration `<?xml version="1.0" encoding="UTF-8"?>`. De aanwezigheid van een declaratie wordt aanbevolen door XML 1.0. De encoding is optioneel bij het gebruik van UTF-8. De encoding is echter toch expliciet omdat dit mogelijke onzekerheid over de bedoeling of het correct volgen van de specificaties voorkomt. Er wordt geen gebruik gemaakt van het pseudo-attribuut `standalone`, omdat er gebruik gemaakt wordt van XML-schema's in plaats van DTD's.

Omwille van de leesbaarheid zijn de XML-schema's pretty-printed; door het gebruik van regeleinden en inspringing wordt de leesbaarheid vergroot. Verder kent elk XML-schema een standaardvolgorde in haar opbouw:

- Het rootelement, voorafgegaan door de commentaartekst `<!--Rootelement-->`.
- De definitie van de logische klassen, voorafgegaan door de commentaartekst `<!–Logische klassen-->`.
- De definitie van de basisklassen, voorafgegaan door de commentaartekst `<!--Basisklassen-->`.

De volgorde waarin de klassen worden gedefinieerd is hierbinnen vrij.

De XML-schema's bevatten geen Byte Order Mark. Het gebruik van een Byte Order Mark is volgens XML 1.0 optioneel bij UTF-8. RFC 3629, hoofdstuk 6, stelt dat het Byte Order Mark verboden moet worden, daar waar UTF-8 verplicht wordt gesteld.

XML-bestanden voor lijsten

De XML-bestanden waarmee MedMij Beheer de *Zorgaanbiederslijst*, de *Whitelist*, de *OAuth Client List*, de *Gegevensdienstnamenlijst en de Catalogus* ontsluit voldoen aan enkele eisen, zodat *PGO Server*, *Authorization Server, MedMijNode* en anderen weten waarop zij kunnen rekenen voor de goede verwerking van deze lijsten.

1.	Het XML-bestand van de *Zorgaanbiederslijst* heet `MedMij_Zorgaanbiederslijst.xml`. Het XML-bestand van de *Whitelist* heet `MedMij_Whitelist.xml`. Het XML-bestand van de *OAuth Client List* heet `MedMij_OAuthclientlist.xml`. Het XML-bestand van de *Gegevensdienstnamen* heet `MedMij_Gegevensdienstnamenlijst.xml`. Het XML-bestand van de *Catalogus* heet `MedMij_Catalogus.xml`.
2.	Bij een wijziging in een lijst die tot hernieuwde publicatie leidt, wordt het volgnummer van de lijst met één opgehoogd. De bestandsnamen van de lijsten zijn zo gekozen dat zij niet wijzigen wanneer de inhoud van het XML-schema wijzigt. Dit vergemakkelijkt de implementatie van changes. Het is gebruikelijk om meta-informatie niet uit de bestandsnaam te halen, maar uit de XML-bestanden zelf (met name uit de header). Daarom is het niet nodig om naast de informatie in het bestand, ook nog eens de bestandsnaam in te zetten voor versie-aanduiding.
3.	De in verantwoordelijkheid 1 bedoelde XML-bestanden maken gebruik van een default namespace, zijnde de namespace waarin het bijpassende XML-schema is gedefinieerd, zonder prefix. De afwezigheid van (onnodige) prefixes komt de leesbaarheid ten goede en voorkomt dat bij de implementatie gebruik wordt gemaakt van namespace-aanduidingen en prefixes die in de toekomst mogelijk wijzigen.
4.	De in verantwoordelijkheid 1 bedoelde XML-bestanden: • voldoen aan XML 1.0 en XML Schema 1.0. • zijn pretty-printed (verplicht gebruik van regeleinden en inspringing). • bevatten de XML Declaration `<?xml version="1.0" encoding="UTF-8"?>`. • bevatten geen Byte Order Mark. Deze vier eisen gelden ook voor de op de XML-bestanden van toepassing zijnde XML-schema's. Voor de toelichting ervan zij daarom verwezen naar die op de pagina over die XML-schema's.

Normenkader informatiebeveiliging

Alle deelnemers dienen in het bezit te zijn van een geldige NEN 7510-certificering, ongeacht hun grootte en of ze dienstverlener in het persoonsdomein of aanbiedersdomein zijn. Ook de beheerorganisatie zal voor de uitvoering van haar diensten binnen het MedMij netwerk gebonden zijn aan de NEN 7510 norm. Gebruik van NEN 7510:2011 voor certificatiedoeleinden onder accreditatie blijft mogelijk tot medio 2020, te weten 2 jaar na publicatie van het certificatieschema NCS 7510:2018. Dit nieuwe certificatieschema behorend bij NEN 7510-1:2017 is begin juni 2018 gepubliceerd. MedMij stelt de volgende eisen aan een NEN 7510-certificering voor deelnemers:

- De Dienstverlener aanbieder moet de aanbieders als belangrijke belanghebbenden hebben geïdentificeerd in het uitvoeren/herijken van de risicoanalyse (zie ook hetgeen over de de rollen en verantwoordelijkheden ten opzichte van de verwerking van persoonsgegevens is opgenomen in de Juridische context);
- Bij de selectie van de van toepassing zijnde maatregelen dienen ten minste de maatregelen uit het normenkader informatiebeveiliging te zijn opgenomen;
- Indien de maatregel een implementatie voorschrijft, dient de maatregel op deze wijze te worden geïmplementeerd. De deelnemer heeft dit middels een self assessment gecontroleerd en onderbouwd. Hiervoor kan het format voor de onderbouwende rapportage als hulpmiddel dienen.

De deelnemer toont jaarlijks met een Aanvullende auditverklaring en onderbouwende rapportage (download hier) aan te voldoen aan het normenkader MedMij. Voor de onderbouwende rapportage bij de auditverklaring wordt door MedMij een format beschikbaar gesteld. Blijkt uit de aanvullende auditverklaring dat de deelnemer niet (meer) voldoet, dan beoordeelt de Stichting MedMij op basis van de onderbouwende rapportage of en op welke manier het Nalevingsbeleid moet worden toegepast.

De NEN 7510-certificering en de aanvullende auditverklaring met rapportage dienen te worden afgegeven door een Conformiteit Beoordelende Instelling (CBI), die NEN 7510 geaccrediteerd is door de Raad voor Accreditatie of een NEN 7510 licentieovereenkomst heeft met NEN. Aan de uitvoerend auditor die de verklaring afgeeft worden daarmee dus dezelfde eisen gesteld door de CBI als voor de afgifte van het NEN 7510 certificaat. Tevens dient het NEN 7510 certificaat te zijn opgenomen in het door NEN beheerde nationale certificatenregister NEN 7510. Voor het NEN 7510 certificaat gelden de door NEN aangehouden termijnen voor hercertificering. Voor vragen van CBI's over het normenkader kan contact worden opgenomen via secmgt@medmij.nl.

Normenkader

Beheersmaatregel	DVP	DVA	BO	Implementatie
A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	✓	✓		Opgeslagen persoonlijke gezondheidsgegevens MOETEN beschermd worden door middel van encryptie. Hiervoor wordt verwezen naar de aanbevelingen die gelden voor 'near term protection' en 'long-term protection' in de aanbevelingen, zie https://www.keylength.com/.
A.12.1.2 (1) Wijzigingsbeheer	✓	✓	✓	De IT-beheerprocessen MOETEN aansluiten op het MedMij Change- en releasebeleid.
A.12.1.2 (2) Wijzigingsbeheer	✓	✓	✓	Niet-standaard wijzigingen op de IT componenten die gebruikt worden binnen de scope van MedMij MOETEN op basis van het vier-ogen-principe worden uitgevoerd.

A.12.1.2 (3) Wijzigingsbeheer	✓	✓	✓	Indien er wijzigingen plaatsvinden die mogelijk significante impact hebben op de informatiebeveiliging, MOET de penetratietest zoals benoemd in A.18.2.3 (1) Beoordeling van technische naleving voor deze componenten opnieuw uitgevoerd worden.
A.12.1.3 (1) Capaciteitsbeheer		✓		Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in Token interface en Resource interface.
A.12.1.3 (2) Capaciteitsbeheer			✓	Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in Interfaces lijsten.
A.12.3.1 Back-up van informatie	✓			Er MOETEN maatregelen zijn geïmplementeerd waardoor het gegevensverlies van persoonlijke gezondheidsinformatie maximaal 24 uur bedraagt. Daarnaast moet een herstelprocedure zijn ingericht waardoor de gegevens van een persoon binnen 24 uur terug kunnen worden geplaatst in geval van een incident. Deze herstelprocedure wordt minimaal jaarlijks getest.
A.12.4.1 Gebeurtenissen registreren	✓	✓		Logging MOET plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie Functies en gegevens, Core onder Logging) Daarnaast MOETEN de volgende acties ten minste 12 maanden onweerlegbaar en controleerbaar worden gelogd: • De actie waarbij de persoon via de DVP bij de DVA gegevens wil opvragen • De acties waarbij de persoon toestemming geeft voor de uitwisseling conform de specificaties in het afsprakenstelsel (indien uitgevoerd onder verantwoordelijkheid van de DVA)
A.12.4.3 Logbestanden van beheerders en operators	✓	✓		1. Het gebruik van toegangsrechten op IT-componenten waar persoonlijke gezondheidsgegevens worden verwerkt MOET worden gelogd; 2. Deze logging MOET ten minste maandelijks worden gecontroleerd. Dit geldt ook voor eventuele onderaannemers; 3. Hierbij MOET functiescheiding gewaarborgd zijn; 4. Tijdens deze controle moet aandacht zijn voor onterecht/onnodig gebruik door medewerkers (met aantoonbare opvolging).

A.12.4.4 Kloksynchronisatie	✓	✓	✓	De klokken van IT componenten die communiceren via MedMij en logging in het kader van MedMij bijhouden, MOETEN worden gesynchroniseerd met pool.ntp.org. Het is toegestaan te synchroniseren met een alternatieve NTP-server, wanneer maatregelen zijn getroffen om de afwijking met pool.ntp.org niet groter dan plus of min 500 ms te laten zijn.
A.12.6.1 Beheer van technische kwetsbaarheden	✓	✓	✓	De processen MOETEN aansluiten op de Operationele processen in het MedMij Afsprakenstelsel ten aanzien van het beheer van technische kwetsbaarheden. Dit dient te omvatten: • Identificeren van kwetsbaarheden in de eigen technologie, onderzoeken van relevantie van door de beheerorganisatie geïdentificeerde kwetsbaarheden + terugkoppeling naar de beheerorganisatie hieromtrent; • Het patchen van systemen of anderzijds mitigeren van de kwetsbaarheid; • Het tijdig kunnen doorlopen van de gehele procedure bij hoog risico-kwetsbaarheden.
A.14.2.1 Beleid voor beveiligd ontwikkelen	✓	✓	✓	Bij het vaststellen voor het beleid voor beveiligd ontwikkelen MOETEN de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC uit het "Uitvoeringsdomein" overwogen worden (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties). Voor mobiele applicaties MOETEN de Beveiligingsrichtlijnen voor mobiele applicaties van het NCSC overwogen worden (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beveiligingsrichtlijnen-voor-mobiele-apparaten).
A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	✓	✓	✓	Organisaties MOETEN relevante MedMij beheersmaatregelen contractueel beleggen bij hun leveranciers.
A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers	✓	✓	✓	Organisaties MOETEN toezien op correcte naleving van de relevante MedMij beheersmaatregelen die bij een leverancier belegd zijn.
A.16.1.1 Verantwoordelijkheden en	✓	✓	✓	

procedures				De processen voor het behandelen van incidenten en calamiteiten moeten aansluiten op de Operationele processen in het afsprakenstelsel.
A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	✓	✓	✓	Kwetsbaarheden en incidenten die betrekking hebben op persoonlijke gezondheidsgegevens of het functioneren van het MedMij stelsel MOETEN binnen 48 uur gemeld te worden bij het centrale incident management team. Zie Deelnemersovereenkomsten. DVZA maken hierover zonodig afspraken met de aangesloten ZA's.
A.16.1.7 Verzamelen van bewijsmateriaal	✓	✓	✓	Medewerking MOET worden verleend aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties. DVA maken hierover zonodig afspraken met de aangesloten Aanbieders.
A.18.2.3 (1) Beoordeling van technische naleving	✓	✓		Tenminste jaarlijks MOET een whitebox applicatiepenetratietesten worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie. De volgende specifieke MedMij eisen moeten ook aantoonbaar getoetst zijn in de pentest rapportage; • DNSSEC zie core.dns.300 en core.dns.301 • TLS zie verantwoordelijkheid core.tls.301 in combinatie met core.tls.302 en core.tls.304 • NCSC webapplicatie richtlijnen U/PW.02, U/PW.03, U/WA.03, U/WA.04 NB deze zijn voor DigiD assessments al verplicht. Zie NOREA Handreiking DigiD assessments **Voor toetreding** heeft deze minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost. Voor penetratietesten die worden uitgevoerd na toetreding, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's (CVSS-score (Common Vulnerability Scoring System) van 4,0 of hoger) ten aanzien van de MedMij dienstverlening. Dit actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd.
A.18.2.3 (2) Beoordeling			✓	

van technische naleving				Tenminste jaarlijks MOET een greybox applicatiepenetratietest worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie. *De externe koppelvlakken zijn:* • *DVP: Burgerfrontend, OAuth Client Redirect* • *DVA: Resourceserver koppelvlak, Autorization server interface(s) eindgebruiker en voor de DVP.* • *BO: Stelselnode en administratieve front-end* ***Voor toetreding** heeft een whitebox applicatiepentratietest minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost.* ***Bij grootschalige wijziging of herbouw** vereisen eenmalig een whitebox applicatiepenetratietest.* Voor penetratietesten die worden uitgevoerd **na toetreding**, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's ten aanzien van de MedMij dienstverlening. Dit actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd.
A. 5.1.1 Beleidsregels voor informatiebeveiliging	✓	✓	✓	De beleidsdocumenten MOETEN de beleidsmaatregelen die van toepassing zijn op MedMij (onder andere gespecificeerd in Privacy- en informatiebeveiligingsbeleid) specifiek benoemen.
A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	✓	✓	✓	De (eind)verantwoordelijkheid voor informatiebeveiliging MOET belegd zijn. Deze functionaris(sen) dient/dienen mandaat te hebben om bij (een dreiging van) een crisis spoedbesluiten te nemen ten aanzien van MedMij en deze besluiten met spoed te kunnen (laten) realiseren. De verantwoordelijke en operationele functionaris (sen) (inclusief eventuele onderaannemers) dient/ dienen hiervoor tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur.
A. 7.2.2 (1) Bewustzijn, opleiding en training ten	✓	✓	✓	De verantwoordelijke functionaris(sen) zoals benoemd in A. 6.1.1 Rollen en

aanzien van informatiebeveiliging				verantwoordelijkheden bij informatiebeveiliging MOET(EN) deelgenomen hebben aan de training over de algemene werking van het stelsel.
A. 7.2.2 (2) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	✓	✓	✓	Overige medewerkers die werkzaamheden verrichten gerelateerd aan MedMij MOETEN een training hebben gevolgd over de algemene werking van het stelsel en op de voor hem/haar van toepassing zijnde beveiligingsmaatregelen.
A. 8.2.1 Classificatie van informatie	✓	✓	✓	De gegevens die binnen het stelsel worden verwerkt MOETEN worden behandeld conform het Informatieclassificatiebeleid (van MedMij).
A. 9.1.1 Beleid voor toegangsbeveiliging	✓	✓	✓	Er MOETEN technische en organisatorische maatregelen worden genomen om inzage van persoonlijke gezondheidsgegevens door medewerkers te voorkomen. De organisatie dient minimaal elk halfjaar en na grote wijzigingen een self-assessment uit te voeren om vast te stellen dat deze maatregelen nog effectief zijn. In (zeer) uitzonderlijke gevallen is inzage in persoonlijke gezondheidsgegevens niet te voorkomen. Hiervoor dient de organisatie een (nood)procedure te documenteren. Deze procedure dient in te gaan op: • Functiescheiding tussen vragen van toestemming voor inzage en het geven van toestemming door een verantwoordelijke functionaris; • Randvoorwaarden en maatregelen met als doel dat inzage plaatsvindt op een gecontroleerde en zo beperkt mogelijke (in tijd en hoeveelheid gegevens) wijze; • Borging dat de deelnemer voldoet wordt aan wet- en regelgeving (AVG, Meldplicht Datalekken) en de geldende versie van het MedMij Afsprakenstelsel; • Vastlegging en verantwoording van de getroffen acties.
A. 9.2.5 Beoordeling van toegangsrechten van gebruikers	✓	✓	✓	1. Toegangsrechten die zijn verstrekt op IT-componenten waar persoonlijke gezondheidsgegevens worden worden verwerkt MOETEN ten minste maandelijks worden gecontroleerd. 2. Hierbij MOET functiescheiding gewaarborgd zijn. 3. Dit geldt ook voor eventuele onderaannemers. 4. Tijdens deze controle moet aandacht zijn voor medewerkers die geen gebruik (meer)

maken van de toegangsrechten (met aantoonbare opvolging).

A. 9.4.1 Beperking toegang tot informatie	✓	Authenticatie van personen (eindgebruikers) MOET plaatsvinden op basis van minimaal twee factoren. Na succesvolle authenticatie krijgen personen alleen toegang tot hun eigen persoonlijke gezondheidsgegevens of de gegevens van de vertegenwoordigde. Scope: Dit geldt voor het gehele MedMij PGO en voor alle gebruikers die hier toegang toe krijgen. Dit is onafhankelijk of deze gebruikers MedMij uitwisselingen gebruiken of niet. Naast SMS MOET een deelnemer ook een sterkere tweede factor aanbieden. De Persoon bepaalt zelf welke tweede factor wordt gebruikt. In deze versie van het Afsprakenstelsel wordt SMS als tweede factor nog geaccepteerd. Het voornemen is deze methode te schrappen. Dit kan, op het moment dat grotere beveiligingsrisico's optreden, via een snel door te voeren patch van het Afsprakenstelsel.

Wijzigingen ten opzichte van release 1.2.0

Norm A.10.1: Encryptie is niet meer beperkt tot disk en/of database encryptie maar er wordt nu verwezen naar de aanbevelingen in https://www.keylength.com/ en geldt voor alle persoonlijke gezondheidsgegevens.

Alle deelnemers dienen in het bezit te zijn van een geldige NEN 7510-certificering, ongeacht hun grootte en of ze dienstverlener in het persoonsdomein of aanbiedersdomein zijn. Ook de beheerorganisatie zal voor de uitvoering van haar diensten binnen het MedMij netwerk gebonden zijn aan de NEN 7510 norm. Gebruik van NEN 7510:2011 voor certificatiedoeleinden onder accreditatie blijft mogelijk tot medio 2020, te weten 2 jaar na publicatie van het certificatieschema NCS 7510:2018. Dit nieuwe certificatieschema behorend bij NEN 7510-1:2017 is begin juni 2018 gepubliceerd. MedMij stelt de volgende eisen aan een NEN 7510-certificering voor deelnemers:

- De Dienstverlener aanbieder moet de aanbieders als belangrijke belanghebbenden hebben geïdentificeerd in het uitvoeren/herijken van de risicoanalyse (zie ook hetgeen over de de rollen en verantwoordelijkheden ten opzichte van de verwerking van persoonsgegevens is opgenomen in de Juridische context);
- Bij de selectie van de van toepassing zijnde maatregelen dienen ten minste de maatregelen uit het normenkader informatiebeveiliging te zijn opgenomen;
- Indien de maatregel een implementatie voorschrijft, dient de maatregel op deze wijze te worden geïmplementeerd. De deelnemer heeft dit middels een self assessment gecontroleerd en onderbouwd. Hiervoor kan het format voor de onderbouwende rapportage als hulpmiddel dienen.

De deelnemer toont jaarlijks met een Aanvullende auditverklaring en onderbouwende rapportage (download hier) aan te voldoen aan het normenkader MedMij. Voor de onderbouwende rapportage bij de auditverklaring wordt door MedMij een format beschikbaar gesteld. Blijkt uit de aanvullende auditverklaring dat de deelnemer niet (meer) voldoet, dan beoordeelt de Stichting MedMij op basis van de onderbouwende rapportage of en op welke manier het Nalevingsbeleid moet worden toegepast.

De NEN 7510-certificering en de aanvullende auditverklaring met rapportage dienen te worden afgegeven door een Conformiteit Beoordelende Instelling (CBI), die NEN 7510 geaccrediteerd is door de Raad voor Accreditatie of een NEN 7510 licentieovereenkomst heeft met NEN. Aan de uitvoerend auditor die de verklaring afgeeft worden daarmee dus dezelfde eisen gesteld door de CBI als voor de afgifte van het NEN 7510 certificaat. Tevens dient het NEN 7510 certificaat te zijn opgenomen in het door NEN beheerde nationale certificatenregister NEN 7510. Voor het NEN 7510 certificaat gelden de door NEN aangehouden termijnen voor hercertificering. Voor vragen van CBI's over het normenkader kan contact worden opgenomen via secmgt@medmij.nl.

Normenkader

Beheersmaatregel	DVP	DVA	BO	Implementatie
A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	✓	✓		Opgeslagen persoonlijke gezondheidsgegevens MOETEN beschermd worden door middel van encryptie. Hiervoor wordt verwezen naar de aanbevelingen die gelden voor 'near term protection' en 'long-term protection' in de aanbevelingen, zie https://www.keylength.com/.
A.12.1.2 (1) Wijzigingsbeheer	✓	✓	✓	De IT-beheerprocessen MOETEN aansluiten op het MedMij Change- en releasebeleid.
A.12.1.2 (2) Wijzigingsbeheer	✓	✓	✓	Niet-standaard wijzigingen op de IT componenten die gebruikt worden binnen de scope van MedMij MOETEN op basis van het vier-ogen-principe worden uitgevoerd.
A.12.1.2 (3) Wijzigingsbeheer	✓	✓	✓	Indien er wijzigingen plaatsvinden die mogelijk significante impact hebben op de informatiebeveiliging, MOET de penetratietest zoals benoemd in A.18.2.3 (1) Beoordeling van technische naleving voor deze componenten opnieuw uitgevoerd worden.
A.12.1.3 (1) Capaciteitsbeheer		✓		Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in Token interface en Resource interface.
A.12.1.3 (2) Capaciteitsbeheer			✓	Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in Interfaces lijsten.
A.12.3.1 Back-up van informatie	✓			Er MOETEN maatregelen zijn geïmplementeerd waardoor het gegevensverlies van persoonlijke gezondheidsinformatie maximaal 24 uur bedraagt.

				Daarnaast moet een herstelprocedure zijn ingericht waardoor de gegevens van een persoon binnen 24 uur terug kunnen worden geplaatst in geval van een incident. Deze herstelprocedure wordt minimaal jaarlijks getest.
A.12.4.1 Gebeurtenissen registreren	✓	✓		Logging MOET plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie Functies en gegevens, Core onder Logging) Daarnaast MOETEN de volgende acties ten minste 12 maanden onweerlegbaar en controleerbaar worden gelogd: • De actie waarbij de persoon via de DVP bij de DVA gegevens wil opvragen • De acties waarbij de persoon toestemming geeft voor de uitwisseling conform de specificaties in het afsprakenstelsel (indien uitgevoerd onder verantwoordelijkheid van de DVA)
A.12.4.3 Logbestanden van beheerders en operators	✓	✓		1. Het gebruik van toegangsrechten op IT-componenten waar persoonlijke gezondheidsgegevens worden verwerkt MOET worden gelogd; 2. Deze logging MOET ten minste maandelijks worden gecontroleerd. Dit geldt ook voor eventuele onderaannemers; 3. Hierbij MOET functiescheiding gewaarborgd zijn; 4. Tijdens deze controle moet aandacht zijn voor onterecht/onnodig gebruik door medewerkers (met aantoonbare opvolging).
A.12.4.4 Kloksynchronisatie	✓	✓	✓	De klokken van IT componenten die communiceren via MedMij en logging in het kader van MedMij bijhouden, MOETEN worden gesynchroniseerd met pool.ntp.org. Het is toegestaan te synchroniseren met een alternatieve NTP-server, wanneer maatregelen zijn getroffen om de afwijking met pool.ntp.org niet groter dan plus of min 500 ms te laten zijn.
A.12.6.1 Beheer van technische kwetsbaarheden	✓	✓	✓	De processen MOETEN aansluiten op de Operationele processen in het MedMij Afsprakenstelsel ten aanzien van het beheer van technische kwetsbaarheden. Dit dient te omvatten:

				• Identificeren van kwetsbaarheden in de eigen technologie, onderzoeken van relevantie van door de beheerorganisatie geïdentificeerde kwetsbaarheden + terugkoppeling naar de beheerorganisatie hieromtrent; • Het patchen van systemen of anderzijds mitigeren van de kwetsbaarheid; • Het tijdig kunnen doorlopen van de gehele procedure bij hoog risico-kwetsbaarheden.
A.14.2.1 Beleid voor beveiligd ontwikkelen	✓	✓	✓	Bij het vaststellen voor het beleid voor beveiligd ontwikkelen MOETEN de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC uit het "Uitvoeringsdomein" overwogen worden (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties). Voor mobiele applicaties MOETEN de Beveiligingsrichtlijnen voor mobiele applicaties van het NCSC overwogen worden (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beveiligingsrichtlijnen-voor-mobiele-apparaten).
A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	✓	✓	✓	Organisaties MOETEN relevante MedMij beheersmaatregelen contractueel beleggen bij hun leveranciers.
A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers	✓	✓	✓	Organisaties MOETEN toezien op correcte naleving van de relevante MedMij beheersmaatregelen die bij een leverancier belegd zijn.
A.16.1.1 Verantwoordelijkheden en procedures	✓	✓	✓	De processen voor het behandelen van incidenten en calamiteiten moeten aansluiten op de Operationele processen in het afsprakenstelsel.
A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	✓	✓	✓	Kwetsbaarheden en incidenten die betrekking hebben op persoonlijke gezondheidsgegevens of het functioneren van het MedMij stelsel MOETEN binnen 48 uur gemeld te worden bij het centrale incident management team. Zie Deelnemersovereenkomsten. DVZA maken hierover zonodig afspraken met de aangesloten ZA's.
A.16.1.7 Verzamelen van bewijsmateriaal	✓	✓	✓	Medewerking MOET worden verleend aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties. DVA maken hierover zonodig afspraken met de aangesloten Aanbieders.

A.18.2.3 (1) Beoordeling van technische naleving	✓	✓	Tenminste jaarlijks MOET een whitebox applicatiepenetratietesten worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie. De volgende specifieke MedMij eisen moeten ook aantoonbaar getoetst zijn in de pentest rapportage; • DNSSEC zie core.dns.300 en core.dns.301 • TLS zie verantwoordelijkheid core.tls.301 in combinatie met core.tls.302 en core.tls.304 • NCSC webapplicatie richtlijnen U/PW.02, U/PW.03, U/WA.03, U/WA.04 NB deze zijn voor DigiD assessments al verplicht. Zie NOREA Handreiking DigiD assessments **Voor toetreding** heeft deze minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost. Voor penetratietesten die worden uitgevoerd na toetreding, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's (CVSS-score (Common Vulnerability Scoring System) van 4,0 of hoger) ten aanzien van de MedMij dienstverlening. Dit actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd.
A.18.2.3 (2) Beoordeling van technische naleving		✓	Tenminste jaarlijks MOET een greybox applicatiepenetratietest worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie. *De externe koppelvlakken zijn:* • *DVP: Burgerfrontend, OAuth Client Redirect* • *DVA: Resourceserver koppelvlak, Autorization server interface(s) eindgebruiker en voor de DVP.* • *BO: Stelselnode en administratieve front-end* ***Voor toetreding** heeft een whitebox applicatiepentratietest minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost.*

				Bij grootschalige wijziging of herbouw *vereisen eenmalig een whitebox applicatiepenetratietest.* Voor penetratietesten die worden uitgevoerd **na toetreding**, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's ten aanzien van de MedMij dienstverlening. Dit actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd.
A. 5.1.1 Beleidsregels voor informatiebeveiliging	✓	✓	✓	De beleidsdocumenten MOETEN de beleidsmaatregelen die van toepassing zijn op MedMij (onder andere gespecificeerd in Privacy- en informatiebeveiligingsbeleid) specifiek benoemen.
A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	✓	✓	✓	De (eind)verantwoordelijkheid voor informatiebeveiliging MOET belegd zijn. Deze functionaris(sen) dient/dienen mandaat te hebben om bij (een dreiging van) een crisis spoedbesluiten te nemen ten aanzien van MedMij en deze besluiten met spoed te kunnen (laten) realiseren. De verantwoordelijke en operationele functionaris (sen) (inclusief eventuele onderaannemers) dient/ dienen hiervoor tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur.
A. 7.2.2 (1) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	✓	✓	✓	De verantwoordelijke functionaris(sen) zoals benoemd in A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging MOET(EN) deelgenomen hebben aan de training over de algemene werking van het stelsel.
A. 7.2.2 (2) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	✓	✓	✓	Overige medewerkers die werkzaamheden verrichten gerelateerd aan MedMij MOETEN een training hebben gevolgd over de algemene werking van het stelsel en op de voor hem/haar van toepassing zijnde beveiligingsmaatregelen.
A. 8.2.1 Classificatie van informatie	✓	✓	✓	De gegevens die binnen het stelsel worden verwerkt MOETEN worden behandeld conform het Informatieclassificatiebeleid (van MedMij).
A. 9.1.1 Beleid voor toegangsbeveiliging	✓	✓	✓	Er MOETEN technische en organisatorische maatregelen worden genomen om inzage van persoonlijke gezondheidsgegevens door medewerkers te voorkomen. De organisatie dient

				minimaal elk halfjaar en na grote wijzigingen een self-assessment uit te voeren om vast te stellen dat deze maatregelen nog effectief zijn. In (zeer) uitzonderlijke gevallen is inzage in persoonlijke gezondheidsgegevens niet te voorkomen. Hiervoor dient de organisatie een (nood)procedure te documenteren. Deze procedure dient in te gaan op: • Functiescheiding tussen vragen van toestemming voor inzage en het geven van toestemming door een verantwoordelijke functionaris; • Randvoorwaarden en maatregelen met als doel dat inzage plaatsvindt op een gecontroleerde en zo beperkt mogelijke (in tijd en hoeveelheid gegevens) wijze; • Borging dat de deelnemer voldoet wordt aan wet- en regelgeving (AVG, Meldplicht Datalekken) en de geldende versie van het MedMij Afsprakenstelsel; • Vastlegging en verantwoording van de getroffen acties.
A. 9.2.5 Beoordeling van toegangsrechten van gebruikers	✓	✓	✓	1. Toegangsrechten die zijn verstrekt op IT-componenten waar persoonlijke gezondheidsgegevens worden worden verwerkt MOETEN ten minste maandelijks worden gecontroleerd. 2. Hierbij MOET functiescheiding gewaarborgd zijn. 3. Dit geldt ook voor eventuele onderaannemers. 4. Tijdens deze controle moet aandacht zijn voor medewerkers die geen gebruik (meer) maken van de toegangsrechten (met aantoonbare opvolging).
A. 9.4.1 Beperking toegang tot informatie	✓			Authenticatie van personen (eindgebruikers) MOET plaatsvinden op basis van minimaal twee factoren. Na succesvolle authenticatie krijgen personen alleen toegang tot hun eigen persoonlijke gezondheidsgegevens of de gegevens van de vertegenwoordigde. Scope: Dit geldt voor het gehele MedMij PGO en voor alle gebruikers die hier toegang toe krijgen. Dit is onafhankelijk of deze gebruikers MedMij uitwisselingen gebruiken of niet. Naast SMS MOET een deelnemer ook een sterkere tweede factor aanbieden.

De Persoon bepaalt zelf welke tweede factor wordt gebruikt.

> In deze versie van het Afsprakenstelsel wordt SMS als tweede factor nog geaccepteerd. Het voornemen is deze methode te schrappen. Dit kan, op het moment dat grotere beveiligingsrisico's optreden, via een snel door te voeren patch van het Afsprakenstelsel.

Wijzigingen ten opzichte van release 1.2.0

Norm A.10.1: Encryptie is niet meer beperkt tot disk en/of database encryptie maar er wordt nu verwezen naar de aanbevelingen in https://www.keylength.com/ en geldt voor alle persoonlijke gezondheidsgegevens.

A. 5.1.1 Beleidsregels voor informatiebeveiliging

Norm

Rationale	Deze maatregel borgt dat het Afsprakenstelsel wordt toegepast in beleid en maatregelen bij de deelnemers.
Implementatie	De beleidsdocumenten MOETEN de beleidsmaatregelen die van toepassing zijn op MedMij (onder andere gespecificeerd in Privacy- en informatiebeveiligingsbeleid) specifiek benoemen.
NEN 7510-1: 2017	A.5.1.1 Beleidsregels voor informatiebeveiliging
NEN 7510: 2011	A.5.1.1 Beleidsdocument voor informatiebeveiliging

Beoordeling

Auditmethode	• Stel vast dat in de beleidsdocumenten het privacy en informatiebeveiligingsbeleid van MedMij specifiek is opgenomen. • Stel vast dat dit beleid is uitgewerkt in maatregelen. • Stel minimaal door middel van interviews met de betrokken medewerkers vast of de maatregelen worden toegepast. Dit geldt ook voor eventuele onderaannemers.
Verificatie	• Welke beleidsdocumenten (incl. versienummer) zijn onderzocht. • Welke documenten zijn onderzocht die de maatregelen beschrijven. • Met wie gesproken is ter bevestiging van toepassing van de maatregelen.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging

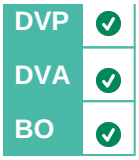
Norm

Rationale	Deze maatregel borgt dat bij (dreiging van) calamiteiten door alle partijen daadkrachtig kan worden gereageerd. Zie ook A.12.4.1 Gebeurtenissen registreren en A.16.1.1 Verantwoordelijkheden en procedures.
Implementatie	De (eind)verantwoordelijkheid voor informatiebeveiliging MOET belegd zijn. Deze functionaris(sen) dient/dienen mandaat te hebben om bij (een dreiging van) een crisis spoedbesluiten te nemen ten aanzien van MedMij en deze besluiten met spoed te kunnen (laten) realiseren. De verantwoordelijke en operationele functionaris(sen) (inclusief eventuele onderaannemers) dient/ dienen hiervoor tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur.
Toelichting	Conform de betreffende Deelnemersovereenkomsten.
NEN 7510-1: 2017	A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging
NEN 7510: 2011	A.6.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging A.8.1.1 Rollen en verantwoordelijkheden

Beoordeling

Auditmethode	• Stel op basis van evidence vast dat de genoemde functionaris(sen) is/zijn aangewezen. • Stel vast dat een procedure is ingericht zodat de genoemde beschikbaarheid, tijdens kantooruren binnen een uur en buiten kantooruren binnen drie uur, te allen tijde gegarandeerd is op dit onderwerp. Indien van toepassing dient deze procedure onderaannemers te omvatten. • De beschikbaarheid dient tevens gegarandeerd te zijn bij geplande en ongeplande afwezigheid. • Stel door middel van interviews vast dat de functionaris(sen) op de hoogte is/zijn van hun taken en verantwoordelijkheden t.a.v. de beschikbaarheid en het juiste mandaat hebben.
Verificatie	• In welke documentatie de verantwoordelijkheden en bevoegdheden zijn belegd. • Welke procedure (incl. versienummer) is ingezien m.b.t. de beschikbaarheid. • Met wie gesproken is ter bevestiging van de implementatie.

Rollen



DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A. 7.2.2 (1) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Norm

Rationale	Deze maatregel borgt dat medewerkers zich bewust zijn van de werking van MedMij en de ketenverantwoordelijkheden.
Implementatie	De verantwoordelijke functionaris(sen) zoals benoemd in A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging MOET(EN) deelgenomen hebben aan de training over de algemene werking van het stelsel.
Toelichting	Deze training wordt door de beheerorganisatie beheerd en gefaciliteerd.
NEN 7510-1: 2017	A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
NEN 7510: 2011	A.8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Beoordeling

Auditmethode	Verkrijg een overzicht van verantwoordelijke functionarissen en stel op basis van het bewijs van deelname vast dat alle personen de training gegeven door de beheerorganisatie hebben gevolgd.
Verificatie	• Het overzicht van contactpersonen. • Evidence m.b.t. de gevolgde training.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A. 7.2.2 (2) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Norm

Rationale	Deze maatregel borgt dat medewerkers zich bewust zijn van de werking van MedMij en de ketenverantwoordelijkheden.
Implementatie	Overige medewerkers die werkzaamheden verrichten gerelateerd aan MedMij MOETEN een training hebben gevolgd over de algemene werking van het stelsel en op de voor hem/haar van toepassing zijnde beveiligingsmaatregelen.
Toelichting	1. Deze training mag door de deelnemer zelf beheerd en gefaciliteerd worden; 2. Deze norm mag ook ingevuld worden doordat de medewerkers deelnemen aan de training gegeven door de beheerorganisatie.
Toetsing	Stel vast dat de partij maatregelen heeft getroffen die borgen dat relevante medewerkers over de noodzakelijke kennis beschikken.
NEN 7510: 2017	A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
NEN 7510: 2011	A.8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Beoordeling

Auditmethode	• Verkrijg een overzicht van alle overige medewerkers die betrokken zijn bij MedMij gerelateerde werkzaamheden. Stel op basis van het bewijs van deelname vast dat deze personen ofwel de training hebben gevolgd die wordt gegeven door de beheerorganisatie, ofwel een training hebben gevolgd gegeven door de contactpersoon. • Stel vast dat de training gegeven door de contactpersoon de volgende aspecten voldoende behandeld: de werking van MedMij, de ketenverantwoordelijkheden en de voor de medewerker van toepassing zijnde beveiligingsmaatregelen.
Verificatie	• Het overzicht van overige medewerkers. • Evidence m.b.t. de gevolgde training.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A. 8.2.1 Classificatie van informatie

Norm

Rationale	Deze maatregel borgt dat informatie die binnen het stelsel wordt gebruikt, door deelnemers met dezelfde voorzichtigheid wordt behandeld.
Implementatie	De gegevens die binnen het stelsel worden verwerkt MOETEN worden behandeld conform het Informatieclassificatiebeleid (van MedMij).
Toetsing	Door middel van interviews en/of het tonen van evidence (zoals het informatieclassificatieschema of -beleid van de partij).
NEN 7510-1: 2017	A.8.2.1 Classificatie van informatie
NEN 7510: 2011	A.7.2.1 Richtlijnen voor classificatie

Beoordeling

Auditmethode	• Stel vast dat de classificatie van gegevens binnen de organisatie, voor de gegevens die binnen het stelsel worden uitgewisseld, overeenstemt met de classificatie zoals door MedMij benoemd in het Informatieclassificatiebeleid van MedMij • Stel vast dat de verwerking van de gegevens door de deelnemer daadwerkelijk plaatsvindt conform het Informatieclassificatiebeleid van MedMij. Hierbij ligt de focus op: gezondheidsgegevens, metagegevens, operationele gegevens, risicoanalyses, pentestrapporten en de whitelist. Dit geldt ook voor eventuele onderaannemers.
Verificatie	Welk document (incl. versienummer) is ingezien.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A. 9.1.1 Beleid voor toegangsbeveiliging

Norm

Rationale	Deze maatregel borgt dat persoonlijke gezondheidsgegevens alleen toegankelijk zijn voor de zorgaanbieder en de zorggebruiker (zie ook A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen).
Implementatie	Er MOETEN technische en organisatorische maatregelen worden genomen om inzage van persoonlijke gezondheidsgegevens door medewerkers te voorkomen. De organisatie dient minimaal elk halfjaar en na grote wijzigingen een self-assessment uit te voeren om vast te stellen dat deze maatregelen nog effectief zijn. In (zeer) uitzonderlijke gevallen is inzage in persoonlijke gezondheidsgegevens niet te voorkomen. Hiervoor dient de organisatie een (nood)procedure te documenteren. Deze procedure dient in te gaan op: • Functiescheiding tussen vragen van toestemming voor inzage en het geven van toestemming door een verantwoordelijke functionaris; • Randvoorwaarden en maatregelen met als doel dat inzage plaatsvindt op een gecontroleerde en zo beperkt mogelijke (in tijd en hoeveelheid gegevens) wijze; • Borging dat de deelnemer voldoet wordt aan wet- en regelgeving (AVG, Meldplicht Datalekken) en de geldende versie van het MedMij Afsprakenstelsel; • Vastlegging en verantwoording van de getroffen acties.
NEN 7510: 2017	A.9.1.1 Beleid voor toegangsbeveiliging
NEN 7510: 2011	A.11.1.1 Toegangsbeleid

Beoordeling

Auditmethode	• Stel vast dat het technisch onmogelijk is gemaakt dat (medewerkers van) partijen zich inzage kunnen verschaffen in persoonlijke gezondheidsgegevens. Dit geldt ook voor eventuele onderaannemers • Stel vast dat self assessment minimaal elk halfjaar en na grote wijzigingen is uitgevoerd. • Stel vast dat de (nood)procedure is opgesteld en effectief is (m.a.w. geen toegang is verkregen zonder toepassing van de procedure). • Indien inzage heeft plaatsgevonden: Controleer de vastlegging en verantwoording
Verificatie	Welke documenten (incl. versienummers) zijn ingezien.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A. 9.2.5 Beoordeling van toegangsrechten van gebruikers

Norm

Rationale	Deze maatregel borgt dat partijen regelmatig controleren of alleen gerechtigde gebruikers toegang hebben tot relevante IT-componenten (waaronder servers, databases en netwerkinfrastructuur).
Implementatie	1. Toegangsrechten die zijn verstrekt op IT-componenten waar persoonlijke gezondheidsgegevens worden worden verwerkt MOETEN ten minste maandelijks worden gecontroleerd. 2. Hierbij MOET functiescheiding gewaarborgd zijn. 3. Dit geldt ook voor eventuele onderaannemers. 4. Tijdens deze controle moet aandacht zijn voor medewerkers die geen gebruik (meer) maken van de toegangsrechten (met aantoonbare opvolging).
NEN 7510: 2017	A.9.2.5 Beoordeling van toegangsrechten van gebruikers
NEN 7510: 2011	A.11.2.4 Beoordeling van toegangsrechten van gebruikers

Beoordeling

Auditmethode	• Stel op basis van de procedures vast dat toegangsrechten op servers, databases en netwerkinfrastructuur waar persoonlijke gezondheidsgegevens worden opgeslagen of worden verwerkt maandelijks gecontroleerd worden. Dit geldt ook voor eventuele onderaannemers. • Stel vast dat de functionaris(sen) die deze controle uitvoert/uitvoeren geen toegangs-rechten verstrekken en/of zelf (beheer)toegang hebben tot de IT-componenten. • De controle van toegangsrechten mag ook geautomatiseerd plaatsvinden. Stel dan vast dat configureren van de geautomatiseerde controle(s) juist en volledig plaatsvindt
Verificatie	Welke procedures (incl. versienummers) zijn ingezien.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A. 9.4.1 Beperking toegang tot informatie

Norm

Rationale	Deze maatregel borgt dat authenticatie van personen en autorisatie tot hun persoonlijke gegevens betrouwbaar plaatsvindt.
Implementatie	Authenticatie van personen (eindgebruikers) MOET plaatsvinden op basis van minimaal twee factoren. Na succesvolle authenticatie krijgen personen alleen toegang tot hun eigen persoonlijke gezondheidsgegevens of de gegevens van de vertegenwoordigde. Scope: Dit geldt voor het gehele MedMij PGO en voor alle gebruikers die hier toegang toe krijgen. Dit is onafhankelijk of deze gebruikers MedMij uitwisselingen gebruiken of niet. Naast SMS MOET een deelnemer ook een sterkere tweede factor aanbieden. De Persoon bepaalt zelf welke tweede factor wordt gebruikt. In deze versie van het Afsprakenstelsel wordt SMS als tweede factor nog geaccepteerd. Het voornemen is deze methode te schrappen. Dit kan, op het moment dat grotere beveiligingsrisico's optreden, via een snel door te voeren patch van het Afsprakenstelsel.
NEN 7510: 2017	A.9.4.1 Beperking toegang tot informatie
NEN 7510: 2011	A.11.5.2 Gebruikersindentificatie en -authenticatie

Beoordeling

Auditmethode	• Stel vast dat (minimaal) twee-factorauthenticatie van personen technisch afgedwongen wordt
	• Stel vast dat voldoende maatregelen zijn ingericht die waarborgen dat na succesvolle authenticatie de personen alleen toegang krijgen tot hun eigen persoonlijke gezondheidsgegevens. Ondersteunende evidence omvat bijvoorbeeld gedocumenteerde usecases of het uitvoeren van een ‘walk through’ vanuit het perspectief van de eindgebruiker
	
	Ten aanzien van de in het eerste punt bedoelde twee factoren gelden de volgende twee richtlijnen.
	
	Ten eerste moeten de factoren uit verschillende van de volgende categorieën gebruikt worden.
	
	• drie categorieën van zogenoemde "authenticatiefactoren": factoren waarvan is bevestigd dat deze gebonden zijn aan een persoon.
	  • op **bezit** gebaseerde authenticatiefactoren: authenticatiefactoren waarvan de betrokkene moet aantonen dat deze in zijn bezit is;
	  • op **kennis** gebaseerde authenticatiefactoren: authenticatiefactoren waarvan de betrokkene moet aantonen dat hij ervan kennis draagt;

  - **inherente** authenticatiefactoren: authenticatiefactoren die op een fysiek kenmerk van een natuurlijke persoon is gebaseerd en waarbij de betrokkene moet aantonen dat hij dat fysieke kenmerk bezit;
- dynamische authenticatie: een elektronisch proces, dat met gebruikmaking van cryptografie of een andere techniek de middelen biedt om op verzoek een elektronisch bewijs op te maken dat de betrokkene de controle heeft over of in het bezit is van de identificatiegegevens, en dat verandert telkens als authenticatie plaatsvindt tussen de betrokkene en het systeem dat diens identiteit verifieert;

Twee factoren

Bijvoorbeeld, wanneer er tijdens het inloggen zowel een TouchID als een FaceID gebruikt wordt, dan is er geen sprake van two-factor, omdat het beide inherente authenticatiefactoren zijn.

Ten tweede moet het gebruik van beide factoren tijdens het inloggen achter elkaar plaatsvinden en in het inlog-proces onlosmakelijk aan elkaar verbonden zijn.

Twee factoren

Bijvoorbeeld, wanneer FaceID gebruikt wordt om met de iCloud password manager een wachtwoord in te voeren is er geen sprake van twee-factorauthenticatie, omdat het wachtwoord ook handmatig ingevoerd kan worden.

Deze tabel toont voorbeelden van veelgebruikte authenticatiefactoren.

categorie	factor	beschrijving
bezit	kaart of pas	Bij de authenticatie is een fysieke, losse kaart betrokken bijvoorbeeld een bankkaart.
	SMS	Als onderdeel van de authenticatie wordt een dynamische SMS-code gecontroleerd. De SMS-code is voldoende lang en steeds een andere. Naast SMS MOET een deelnemer ook een sterkere tweede factor aan kunnen bieden.
	push notifications	Als onderdeel van de authenticatie wordt er een melding ontvangen op de telefoon. De gebruiker bevestigt de melding.
	keychain	Deze controle is niet zichtbaar voor de gebruiker. Op de mobiele telefoon wordt een secure enclave of keychain gebruikt om bezit van de telefoon aan te tonen.
kennis	pincode	Als onderdeel van de authenticatie wordt een pincode ingevoerd. Een pincode is altijd verbonden aan een kaart of een app (licatie). Na een beperkt aantal foutpogingen wordt de kaart of app geblokkeerd.
	wachtwoord	

			Als onderdeel van de authenticatie wordt een wachtwoord ingevoerd. Voor de eisen aan het wachtwoord, de levensduur en het toegestane aantal foutpogingen is wachtwoordbeleid aanwezig.
	inherent	vingerafdruk	Als onderdeel van de authenticatie wordt een vingerafdruk gecontroleerd, zoals TouchID.
		gezichtsherkenning	Als onderdeel van de authenticatie wordt het gezicht gecontroleerd, zoals FaceID.
		irisscan	Als onderdeel van de authenticatie wordt het oog gecontroleerd.

Verificatie	Welke documenten (incl. versienummers) zijn ingezien.

Eindgebruikers moeten worden beschermd. De eindgebruiker van een PGO moet er vanuit kunnen gaan dat gegevens op een goede manier toegankelijk worden gemaakt. Eindgebruikers moeten kunnen vertrouwen dat hun medische informatie veilig wordt opgeslagen.

Rollen

DVP	✓
DVA	
BO	

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen

Norm

Rationale	Persoonlijke gezondheidsgegevens moeten versleuteld worden opgeslagen. Dit heeft als doel dat de vertrouwelijkheid en integriteit van de gezondheidsgegevens gewaarborgd is, ook indien: · Een onbevoegd persoon toegang krijgt tot de datadrager (het hardware medium) · Een onbevoegd persoon toegang verkrijgt tot de logische dataopslag (de database of het gegevensbestand)
Implementatie	Opgeslagen persoonlijke gezondheidsgegevens MOETEN beschermd worden door middel van encryptie. Hiervoor wordt verwezen naar de aanbevelingen die gelden voor 'near term protection' en 'long-term protection' in de aanbevelingen, zie https://www.keylength.com/.
Toelichting	1. Deze maatregel mag uitgesloten worden indien DVA onder zijn verantwoording geen persoonlijke gezondheidsgegevens opslaat. 2. Een overzicht van publicaties is te vinden op https://www.keylength.com/ 3. Er kan gebruik gemaakt worden van de ECRYPT-CSA aanbevelingen, NIST of BSI aanbevelingen 4. Deze norm betreft alle opgeslagen persoonlijke gezondsheidsgegevens, inclusief logfiles, backups en/of archieven.
NEN 7510: 2017	A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen
NEN 7510: 2011	A.12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen

Beoordeling

Auditmethode	• Stel op basis van de architectuurdiagrammen vast of er wordt voldaan aan de aanbevelingen die gelden voor 'near term protection' en 'long-term protection' volgens de door deelnemer gekozen invulling van encryptie standaarden en sleutels bijvoorbeeld ECRYPT-CSA,NIST of BSI (zie https://www.keylength.com/). De deelnemer zal moeten aangeven welke encryptiestandaarden en sleutellengtes etc er gekozen zijn voor de opslag van gezondheidsgegevens. • Stel op basis van een steekproef vast of aanbevelingen ook daadwerkelijk geïmplementeerd zijn.
Verificatie	• Welke versie van de aanbevelingen is gehanteerd. • Welke versie van de architectuurdiagrammen zijn ingezien. • Evidence m.b.t. de daadwerkelijke implementatie.

Rollen

DVP	✓
DVA	✓
BO	

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.12.1.2 (1) Wijzigingsbeheer

Norm

Rationale	Deze maatregel borgt dat wijzigingen binnen de keten beheerst verlopen.
Implementatie	De IT-beheerprocessen MOETEN aansluiten op het MedMij Change- en releasebeleid.
NEN 7510-1:2017	A.12.1.2 Wijzigingsbeheer
NEN 7510:2011	A.10.1.2 Wijzigingsbeheer

Beoordeling

Auditmethode	• Stel vast dat IT-beheerprocessen van de organisatie aansluiten op het Change- en releasebeleid van MedMij. • Stel op basis van een steekproef vast dat de IT-beheerprocessen voor MedMij juist worden uitgevoerd.
Verificatie	• Welke procedures (incl. versienummers) zijn ingezien. • Evidence m.b.t. de daadwerkelijke implementatie.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.12.1.2 (2) Wijzigingsbeheer

Norm

Rationale	Deze maatregel borgt dat er altijd twee medewerkers betrokken zijn bij werkzaamheden aan systemen (configuratiewijzigingen, onderhoud, installatie van updates) die direct impact (kunnen) hebben op de beschikbaarheid, integriteit of vertrouwelijkheid van de keten. De maatregel vermindert het risico op onbeschikbaarheid van of kwetsbaarheden binnen de keten.
Implementatie	Niet-standaard wijzigingen op de IT componenten die gebruikt worden binnen de scope van MedMij MOETEN op basis van het vier-ogen-principe worden uitgevoerd.
Toelichting	Het gaat hier niet om achterliggende systemen (zoals EPD) maar om de aansluitende systemen en netwerkcomponenten (zoals firewalls).
NEN 7510-1: 2017	A.12.1.2 Wijzigingsbeheer
NEN 7510: 2011	A.10.1.2 Wijzigingsbeheer

Beoordeling

Auditmethode	• Stel vast dat een overzicht van standaard en niet-standaard wijzigingen is gedocumenteerd. Ga na of standaardwijzigingen geen midden/hoog risico hebben op op de beschikbaarheid, integriteit of vertrouwelijkheid van de keten. • Stel vast dat vier-ogen-principe is ingericht voor niet-standaard wijzigingen. • Stel door middel van interview met de betrokken medewerkers vast of de procedures worden nageleefd.
Verificatie	• Welke procedures (incl. versienummers) zijn ingezien. • Met wie gesproken is ter bevestiging van de implementatie.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.12.1.2 (3) Wijzigingsbeheer

Norm

Rationale	Deze maatregel borgt dat wijzigingen binnen de keten beheerst verlopen.
Implementatie	Indien er wijzigingen plaatsvinden die mogelijk significante impact hebben op de informatiebeveiliging, MOET de penetratietest zoals benoemd in A.18.2.3 (1) Beoordeling van technische naleving voor deze componenten opnieuw uitgevoerd worden.
NEN 7510-1: 2017	A.12.1.2 Wijzigingsbeheer
NEN 7510: 2011	A.10.1.2 Wijzigingsbeheer

Beoordeling

Auditmethode	Zie A.18.2.3 (1) Beoordeling van technische naleving
Verificatie	Zie A.18.2.3 (1) Beoordeling van technische naleving

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.12.1.3 (1) Capaciteitsbeheer

Norm

Rationale	Deze maatregel borgt dat alle systemen in de keten voldoen aan de afgesproken eisen omtrent beschikbaarheid.
Implementatie	Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in Token interface en Resource interface.
NEN 7510-1: 2017	A.12.1.3 Capaciteitsbeheer
NEN 7510: 2011	A.10.3.1 Capaciteitsbeheer

Beoordeling

Auditmethode	Stel op basis van IT-monitoring en/of service level rapportages vast dat over een periode van drie maanden voorafgaand aan de auditdatum voldaan is aan de beschikbaarheidseisen.
Verificatie	Evidence m.b.t. de rapportages.

Rollen

DVP	
DVA	✓
BO	

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.12.1.3 (2) Capaciteitsbeheer

Norm

Rationale	Deze maatregel borgt dat alle systemen in de keten voldoen aan de afgesproken eisen omtrent beschikbaarheid.
Implementatie	Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in Interfaces lijsten.
NEN 7510-1: 2017	A.12.1.3 Capaciteitsbeheer
NEN 7510: 2011	A.10.3.1 Capaciteitsbeheer

Beoordeling

Auditmethode	Stel op basis van IT-monitoring en/of service level rapportages vast dat over een periode van drie maanden voorafgaand aan de auditdatum voldaan is aan de beschikbaarheidseisen.
Verificatie	Evidence m.b.t. de rapportages.

Rollen

DVP	
DVA	
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.12.3.1 Back-up van informatie

Norm

Rationale	Deze maatregel borgt dat deelnemers beschikken over een bruikbare back-up.
Implementatie	Er MOETEN maatregelen zijn geïmplementeerd waardoor het gegevensverlies van persoonlijke gezondheidsinformatie maximaal 24 uur bedraagt. Daarnaast moet een herstelprocedure zijn ingericht waardoor de gegevens van een persoon binnen 24 uur terug kunnen worden geplaatst in geval van een incident. Deze herstelprocedure wordt minimaal jaarlijks getest.
Toelichting	Deze maatregel MAG worden uitgesloten door een DVP indien de persoonlijke gezondheidsinformatie niet centraal wordt opgeslagen.
NEN 7510-1: 2017	A.12.3.1 Back-up van informatie
NEN 7510: 2011	A.10.5.1 Reservekopieën (back-ups)

Beoordeling

Auditmethode	• Stel vast dat de organisatie maatregelen heeft ingericht waardoor gegevensverlies is beperkt tot maximaal 24 uur. Dit zijn bijvoorbeeld back-ups en/of heet repliceren van gegevens. • Stel vast dat de herstelprocedure binnen 24u uitgevoegd kan worden en minimaal jaarlijks wordt getest. • Stel daarnaast via monitoring en rapportages vast dat de leverancier voldoet
Verificatie	• Welke procedures (incl. versienummers) zijn ingezien. • Evidence m.b.t. de (minimaal) jaarlijkse test.

Rollen

DVP	✓
DVA	
BO	

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.12.4.1 Gebeurtenissen registreren

Norm

Rationale	Deze maatregel borgt dat relevante security gebeurtenissen in systemen van de deelnemers en de beheerorganisatie (zoals het verlenen van toestemming aan aanbieder door de persoon, het inzien of wijzigen van een PGO of het wijzigen aan loggen van gebruikers aan hun PGO) ten minste 12 maanden inzichtelijk blijven.
Implementatie	Logging MOET plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie Functies en gegevens, Core onder Logging) Daarnaast MOETEN de volgende acties ten minste 12 maanden onweerlegbaar en controleerbaar worden gelogd: • De actie waarbij de persoon via de DVP bij de DVA gegevens wil opvragen • De acties waarbij de persoon toestemming geeft voor de uitwisseling conform de specificaties in het afsprakenstelsel (indien uitgevoerd onder verantwoordelijkheid van de DVA)
NEN 7510-1: 2017	A.12.4.1 Gebeurtenissen registreren
NEN 7510: 2011	A.10.10.1 Aanmaken audit-logbestanden A.10.10.2 Controle van systeemgebruik

Beoordeling

Auditmethode	• Stel vast of de logbestanden voldoen aan de voorwaarden van het afsprakenstelsel (zie Processen en informatie onder Logging). • Stel vast hoe de onweerlegbaarheid en controleerbaarheid van de logs over personen is ingericht. Stel vast dat deze altijd minimaal 12 maanden beschikbaar blijven.
Verificatie	• Evidence m.b.t. de logbestanden. • Evidence m.b.t. aansluiting.

Rollen

DVP	✓
DVA	✓
BO	

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.12.4.3 Logbestanden van beheerders en operators

Norm

Rationale	Deze maatregel borgt dat partijen regelmatig controleren of alleen gerechtigde gebruikers toegang hebben tot relevante IT-componenten (waaronder servers, databases en netwerkinfrastructuur).
Implementatie	1. Het gebruik van toegangsrechten op IT-componenten waar persoonlijke gezondheidsgegevens worden verwerkt MOET worden gelogd; 2. Deze logging MOET ten minste maandelijks worden gecontroleerd. Dit geldt ook voor eventuele onderaannemers; 3. Hierbij MOET functiescheiding gewaarborgd zijn; 4. Tijdens deze controle moet aandacht zijn voor onterecht/onnodig gebruik door medewerkers (met aantoonbare opvolging).
NEN 7510-1: 2017	A.9.2.5 Beoordeling van toegangsrechten van gebruikers
NEN 7510: 2011	A.11.2.4 Beoordeling van toegangsrechten van gebruikers

Beoordeling

Auditmethode	• Stel op basis van de procedures vast dat de logging van servers, databases en netwerkinfrastructuur waar persoonlijke gezondheidsgegevens worden opgeslagen of worden verwerkt maandelijks gecontroleerd worden. • Stel vast dat de functionaris(sen) die deze controle uitvoert/uitvoeren geen toegangsrechten verstrekken en/of zelf (beheer)toegang hebben tot de IT-componenten. • De controle van logging mag ook geautomatiseerd plaatsvinden. Stel dan vast dat configureren van de geautomatiseerde controle(s) juist en volledig plaatsvindt.
Verificatie	Welke documenten/registraties (incl. versienummers) zijn ingezien.

Rollen

DVP	✓
DVA	✓
BO	

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.12.4.4 Kloksynchronisatie

Norm

Rationale	Deze maatregel borgt dat tijdsvermeldingen in logbestanden gelijklopen, wanneer deze worden gebruikt om misbruik in de keten op te sporen. Zie ook A.16.1.7 Verzamelen van bewijsmateriaal.
Implementatie	De klokken van IT componenten die communiceren via MedMij en logging in het kader van MedMij bijhouden, MOETEN worden gesynchroniseerd met pool.ntp.org. Het is toegestaan te synchroniseren met een alternatieve NTP-server, wanneer maatregelen zijn getroffen om de afwijking met pool.ntp.org niet groter dan plus of min 500 ms te laten zijn.
NEN 7510-1: 2017	A.12.4.4 Kloksynchronisatie
NEN 7510: 2011	A.10.10.6 Synchronisatie van systeemklokken

Beoordeling

Auditmethode	Stel voor de relevante systemen voor het MedMij afsprakenstelsel vast via de logging*- en /of configuratie-instellingen dat de synchronisatie met pool.ntp.org ten minste 1x per 24 uur plaats vindt. Dan wel middels een verklaring van een lokale NTP server over de synchronisatieprocedure met genoemde NTP-server.
Verificatie	Evidence m.b.t. de logbestanden en/ of configuratie instellingen.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.12.6.1 Beheer van technische kwetsbaarheden

Norm

Rationale	Deze maatregel borgt dat deelnemers in staat zijn tijdig te reageren op meldingen van (vermeende) kwetsbaarheden in het MedMij stelsel. Zie ook A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging.
Implementatie	De processen MOETEN aansluiten op de Operationele processen in het MedMij Afsprakenstelsel ten aanzien van het beheer van technische kwetsbaarheden. Dit dient te omvatten: • Identificeren van kwetsbaarheden in de eigen technologie, onderzoeken van relevantie van door de beheerorganisatie geïdentificeerde kwetsbaarheden + terugkoppeling naar de beheerorganisatie hieromtrent; • Het patchen van systemen of anderzijds mitigeren van de kwetsbaarheid; • Het tijdig kunnen doorlopen van de gehele procedure bij hoog risico-kwetsbaarheden.
NEN 7510-1: 2017	A.12.6.1 Beheer van technische kwetsbaarheden
NEN 7510: 2011	A.12.6.1 Beheersing van technische kwetsbaarheden

Beoordeling

Auditmethode	• Stel vast dat de organisatie in haar procedures aansluit op het proces van beheren van technische kwetsbaarheden uit het afsprakenstelsel van MedMij. • Stel door middel van interview met de betrokken medewerkers vast of de procedures worden nageleefd.
Verificatie	• Welke procedures (incl. versienummers) zijn ingezien. • Met wie gesproken is ter bevestiging van de implementatie.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.14.2.1 Beleid voor beveiligd ontwikkelen

Norm

Rationale	Deze maatregel borgt dat deelnemers en beheerorganisatie beveiligingsstandaarden toepassen bij het ontwikkelen van software en systemen die aan het internet gekoppeld worden. Dit voorkomt dat bekende programmeerfouten worden gemaakt.
Implementatie	Bij het vaststellen voor het beleid voor beveiligd ontwikkelen MOETEN de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC uit het "Uitvoeringsdomein" overwogen worden (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties). Voor mobiele applicaties MOETEN de Beveiligingsrichtlijnen voor mobiele applicaties van het NCSC overwogen worden (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beveiligingsrichtlijnen-voor-mobiele-apparaten).
NEN 7510: 2011	Deze maatregel bestond nog niet in NEN 7510:2011

Beoordeling

Auditmethode	• Stel vast dat de organisatie in haar beleid met betrekking tot de ontwikkeling, de door NCSC gedefinieerde minimale beveiligingsstandaarden (‘Uitvoeringsdomein’) in overweging heeft genomen. • Stel vast dat deze zijn toegepast.
Verificatie	• Welke procedures (incl. versienummers) zijn ingezien. • Met wie gesproken is ter bevestiging van de toepassing van de procedures.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten

Norm

Rationale	Deze maatregel borgt dat MedMij beheersmaatregelen die door een leverancier worden uitgevoerd contractueel vastgelegd worden.
Implementatie	Organisaties MOETEN relevante MedMij beheersmaatregelen contractueel beleggen bij hun leveranciers.
Toelichting	Deze maatregel mag worden uitgesloten indien er voor de MedMij-dienstverlening geen gebruik wordt gemaakt van externe leveranciers.
NEN 7510-1: 2017	A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
NEN 7510: 2011	6.2.3 Beveiliging in overeenkomsten met een derde partij

Beoordeling

Auditmethode	Stel vast dat de organisatie de uitbestede maatregelen contractueel heeft geborgd met de leverancier(s).
Verificatie	Welke documenten (incl. versienummers) zijn ingezien.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers

Norm

Rationale	Deze maatregel borgt dat er controle plaatsvindt op de naleving van MedMij beheersmaatregelen die door een leverancier worden uitgevoerd.
Implementatie	Organisaties MOETEN toezien op correcte naleving van de relevante MedMij beheersmaatregelen die bij een leverancier belegd zijn.
Toelichting	Deze maatregel mag worden uitgesloten indien er voor de MedMij-dienstverlening geen gebruik wordt gemaakt van externe leveranciers.
NEN 7510-1: 2017	A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers
NEN 7510: 2011	10.2.2 Controle en beoordeling van dienstverlening door een derde partij.

Beoordeling

Auditmethode	Stel vast (bijvoorbeeld door het inzien van auditrapportages of leveranciersbeoordelingen) dat de organisatie heeft vastgesteld dat de leverancier de relevante maatregelen naar behoren heeft geïmplementeerd/uitgevoerd.
Verificatie	Welke documenten (incl. versienummers) zijn ingezien.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.16.1.1 Verantwoordelijkheden en procedures

Norm

Rationale	Deze maatregel borgt dat deelnemers en beheerorganisatie volgens hetzelfde proces handelen in geval van incidenten en calamiteiten. Zie ook A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging.
Implementatie	De processen voor het behandelen van incidenten en calamiteiten moeten aansluiten op de Operationele processen in het afsprakenstelsel.
NEN 7510-1: 2017	A.16.1.1 Verantwoordelijkheden en procedures
NEN 7510: 2011	A.13.2.1 Verantwoordelijkheden en procedures

Beoordeling

Auditmethode	• Stel vast dat de organisatie in haar procedures aansluit op het proces van incidenten en calamiteiten uit het afsprakenstelsel van MedMij. • Stel vast de procedures worden nageleefd.
Verificatie	• Welke procedures (incl. versienummers) zijn ingezien. • Met wie gesproken is ter bevestiging van de implementatie. • Evidence m.b.t. de daadwerkelijke implementatie.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging

Norm

Rationale	Deze maatregel borgt dat alle partijen elkaar tijdig op de hoogte brengen wanneer zij kennis hebben over kwetsbaarheden, die relevant kan zijn voor het MedMij stelsel. Het kan hier bijvoorbeeld gaan om informatie verkregen via het NCSC, penetratietesten of een Responsible Disclosure-melding). Zie ook A.12.6.1 Beheer van technische kwetsbaarheden.
Implementatie	Kwetsbaarheden en incidenten die betrekking hebben op persoonlijke gezondheidsgegevens of het functioneren van het MedMij stelsel MOETEN binnen 48 uur gemeld te worden bij het centrale incident management team. Zie Deelnemersovereenkomsten. DVZA maken hierover zonodig afspraken met de aangesloten ZA's.
NEN 7510-1: 2017	A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging
NEN 7510: 2011	A.13.1.2 Rapportage van zwakke plekken in de beveiliging

Beoordeling

Auditmethode	• Stel vast dat de organisatie in haar procedures aansluit op het proces van incidenten en calamiteiten en proces beheren technische kwetsbaarheden uit het afsprakenstelsel van MedMij. • Stel door middel van interview met de betrokken medewerkers en waar mogelijk onderbouwd met evidence vast of de procedures worden nageleefd. • Stel door middel van interview en evidence vast of de deelnemer alle ontdekte kwetsbaarheden tijdig heeft gemeld aan MedMij.
Verificatie	• Welke procedures (incl. versienummers) zijn ingezien. • Met wie gesproken is ter bevestiging van de implementatie. • Evidence m.b.t. ontdekte kwetsbaarheden en tijdige melding aan MedMij.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.16.1.7 Verzamelen van bewijsmateriaal

Norm

Rationale	Deze maatregel borgt dat alle partijen moeten meewerken aan forensische onderzoeken, bijvoorbeeld in de nasleep van een stelselincident of fraude. Het zal meestal gaan om het opleveren van logfiles (zie A.12.4.1 Gebeurtenissen registreren).
Implementatie	Medewerking MOET worden verleend aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties. DVA maken hierover zonodig afspraken met de aangesloten Aanbieders.
NEN 7510-1: 2017	A.16.1.7 Verzamelen van bewijsmateriaal
NEN 7510: 2011	A.13.2.3 Verzamelen van bewijsmateriaal

Beoordeling

Auditmethode	• Stel vast dat de organisatie in haar procedures het verlenen van medewerking aan (forensische) onderzoeken heeft opgenomen. • Stel vast datg de procedures worden nageleefd.
Verificatie	• Welke procedures (incl. versienummers) zijn ingezien. • Met wie gesproken is ter bevestiging van de implementatie. • Evidence m.b.t. de implementatie.

Rollen

DVP	✓
DVA	✓
BO	✓

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.18.2.3 (1) Beoordeling van technische naleving

Norm

Rationale	Deze maatregel borgt dat deelnemers en de beheerorganisatie met regelmaat (en gebruikmakend van verschillende partijen) hun software, systemen en infrastructuur laten toetsen op bekende kwetsbaarheden.
Implementatie	Tenminste jaarlijks MOET een whitebox applicatiepenetratietesten worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie. De volgende specifieke MedMij eisen moeten ook aantoonbaar getoetst zijn in de pentest rapportage; • DNSSEC zie core.dns.300 en core.dns.301 • TLS zie verantwoordelijkheid core.tls.301 in combinatie met core.tls.302 en core.tls.304 • NCSC webapplicatie richtlijnen U/PW.02, U/PW.03, U/WA.03, U/WA.04 NB deze zijn voor DigiD assessments al verplicht. Zie NOREA Handreiking DigiD assessments **Voor toetreding** heeft deze minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost. Voor penetratietesten die worden uitgevoerd na toetreding, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's (CVSS-score (Common Vulnerability Scoring System) van 4,0 of hoger) ten aanzien van de MedMij dienstverlening. Dit actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd.
Toelichting	Een whitebox penetratietest houdt in dat de penetratietester zoveel mogelijk inzicht heeft in de applicatie. Dit kan onder meer inhouden: • Toegang tot architectuur/ontwerpdocumentatie; • Toegang tot broncode; • Inloggegevens voor verschillende rollen. Het is niet nodig om een penetratietest uit te voeren op de gehele architectuur en/of alle programmacode. Het gaat met name om de beveiliging van de gegevens die over internet worden uitgewisseld, de focus moet dus liggen op de beveiliging van de externe koppelvlakken. Een app of een web portaal is ook een extern koppelvlak!
NEN 7510-1: 2017	A.18.2.3 Beoordeling van technische naleving
NEN 7510: 2011	A.15.2.2 Controle op technische naleving

Beoordeling

Auditmethode	Stel op basis van de meest recente rapportages vast of er wordt voldaan aan de jaarlijkse whitebox applicatiepenetratietesten op de externe koppelvlakken conform de architectuur en specificaties van MedMij (en louter binnen de scope van het MedMij afsprakenstelsel).
Verificatie	

- Evidence m.b.t. de uitgevoerde jaarlijkse testen.
- Met wie gesproken is ter bevestiging van de implementatie.
- Evidence m.b.t. het melden van kwetsbaarheden

Rollen

DVP	✓
DVA	✓
BO	

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

A.18.2.3 (2) Beoordeling van technische naleving

Norm

Rationale	Deze maatregel borgt dat deelnemers en de beheerorganisatie met regelmaat (en gebruikmakend van verschillende partijen) hun software, systemen en infrastructuur laten toetsen op bekende kwetsbaarheden.
Implementatie	Tenminste jaarlijks MOET een greybox applicatiepenetratietest worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie. *De externe koppelvlakken zijn:* • *DVP: Burgerfrontend, OAuth Client Redirect* • *DVA: Resourceserver koppelvlak, Autorization server interface(s) eindgebruiker en voor de DVP.* • *BO: Stelselnode en administratieve front-end* ***Voor toetreding** heeft een whitebox applicatiepentratietest minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost.* ***Bij grootschalige wijziging of herbouw** vereisen eenmalig een whitebox applicatiepenetratietest.* Voor penetratietesten die worden uitgevoerd **na toetreding**, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's ten aanzien van de MedMij dienstverlening. Dit actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd.
NEN 7510-1: 2017	A.18.2.3 Beoordeling van technische naleving
NEN 7510: 2011	A.15.2.2 Controle op technische naleving

Beoordeling

Auditmethode	Stel op basis van de meest recente rapportages vast of er wordt voldaan aan de jaarlijkse blackbox-applicatiepenetratietesten op de externe koppelvlakken conform de architectuur en specificaties van MedMij (en louter binnen de scope van het MedMij afsprakenstelsel).
Verificatie	• Evidence m.b.t. de uitgevoerde jaarlijkse testen. • Met wie gesproken is ter bevestiging van de implementatie. • Evidence m.b.t. het melden van kwetsbaarheden

Rollen

DVP	
DVA	
BO	✔

DVP = Dienstverlener persoon, DVA = Dienstverlener aanbieder, BO = Beheerorganisatie

Aanvullende auditverklaring en onderbouwende rapportage

Organisatiegegevens

De gegevens van de (aspirant) MedMij deelnemer.

Naam	
Adres	
Vertegenwoordigd door	
Rol	DVP/DVA

Certificatiegegevens

De gegevens van het onderliggende NEN 7510-certificaat.

Norm	NEN 7510-1:2017
Scope	
Certificaatnummer	
Vervaldatum	

Auditgegevens

Gegevens over de audit.

CBI	
Bezochte locatie(s)	
Lead auditor	
Overige teamleden	

Rapport

Gegevens over dit rapport.

Datum rapport	
Status rapport	Concept/Definitief
Bijlagen bij dit rapport	

Onderbouwende rapportage

Beheersmaatregel	DVP	DVA	BO	Implementatie	Voldoet	C
A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	✓	✓		Opgeslagen persoonlijke gezondheidsgegevens MOETEN beschermd worden door middel van encryptie. Hiervoor wordt verwezen naar de aanbevelingen die gelden voor 'near term protection' en 'long-term protection' in de aanbevelingen, zie https://www.keylength.com/.		
A.12.1.2 (1) Wijzigingsbeheer	✓	✓	✓	De IT-beheerprocessen MOETEN aansluiten op het MedMij Change- en releasebeleid.		
A.12.1.2 (2) Wijzigingsbeheer	✓	✓	✓	Niet-standaard wijzigingen op de IT componenten die gebruikt worden binnen de scope van MedMij MOETEN op basis van het vier-ogen-principe worden uitgevoerd.		
A.12.1.2 (3) Wijzigingsbeheer	✓	✓	✓	Indien er wijzigingen plaatsvinden die mogelijk significante impact hebben op de informatiebeveiliging, MOET de penetratietest zoals benoemd in A.18.2.3 (1) Beoordeling van technische naleving voor deze componenten opnieuw uitgevoerd worden.		
A.12.1.3 (1) Capaciteitsbeheer		✓		Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in Token interface en Resource interface.		
A.12.1.3 (2) Capaciteitsbeheer			✓	Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in Interfaces lijsten.		
A.12.3.1 Back-up van informatie	✓			Er MOETEN maatregelen zijn geïmplementeerd waardoor het gegevensverlies van persoonlijke gezondheidsinformatie maximaal 24 uur bedraagt. Daarnaast moet een herstelprocedure zijn ingericht waardoor de gegevens van een persoon binnen 24 uur terug kunnen worden geplaatst in geval		

				van een incident. Deze herstelprocedure wordt minimaal jaarlijks getest.
A.12.4.1 Gebeurtenissen registreren	✓	✓		Logging MOET plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie Functies en gegevens, Core onder Logging) Daarnaast MOETEN de volgende acties ten minste 12 maanden onweerlegbaar en controleerbaar worden gelogd: • De actie waarbij de persoon via de DVP bij de DVA gegevens wil opvragen • De acties waarbij de persoon toestemming geeft voor de uitwisseling conform de specificaties in het afsprakenstelsel (indien uitgevoerd onder verantwoordelijkheid van de DVA)
A.12.4.3 Logbestanden van beheerders en operators	✓	✓		1. Het gebruik van toegangsrechten op IT-componenten waar persoonlijke gezondheidsgegevens worden verwerkt MOET worden gelogd; 2. Deze logging MOET ten minste maandelijks worden gecontroleerd. Dit geldt ook voor eventuele onderaannemers; 3. Hierbij MOET functiescheiding gewaarborgd zijn; 4. Tijdens deze controle moet aandacht zijn voor onterecht /onnodig gebruik door medewerkers (met aantoonbare opvolging).
A.12.4.4 Kloksynchronisatie	✓	✓	✓	De klokken van IT componenten die communiceren via MedMij en logging in het kader van MedMij bijhouden, MOETEN worden gesynchroniseerd met pool.ntp.org.

				Het is toegestaan te synchroniseren met een alternatieve NTP-server, wanneer maatregelen zijn getroffen om de afwijking met pool.ntp.org niet groter dan plus of min 500 ms te laten zijn.
A.12.6.1 Beheer van technische kwetsbaarheden	✓	✓	✓	De processen MOETEN aansluiten op de Operationele processen in het MedMij Afsprakenstelsel ten aanzien van het beheer van technische kwetsbaarheden. Dit dient te omvatten: • Identificeren van kwetsbaarheden in de eigen technologie, onderzoeken van relevantie van door de beheerorganisatie geïdentificeerde kwetsbaarheden + terugkoppeling naar de beheerorganisatie hieromtrent; • Het patchen van systemen of anderzijds mitigeren van de kwetsbaarheid; • Het tijdig kunnen doorlopen van de gehele procedure bij hoog risico-kwetsbaarheden.
A.14.2.1 Beleid voor beveiligd ontwikkelen	✓	✓	✓	Bij het vaststellen voor het beleid voor beveiligd ontwikkelen MOETEN de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC uit het "Uitvoeringsdomein" overwogen worden (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties). Voor mobiele applicaties MOETEN de Beveiligingsrichtlijnen voor mobiele applicaties van het NCSC overwogen worden (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beveiligingsrichtlijnen-voor-mobiele-apparaten).
A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	✓	✓	✓	Organisaties MOETEN relevante MedMij beheersmaatregelen contractueel beleggen bij hun leveranciers.
A.15.2.1 Monitoring en	✓	✓	✓	

beoordeling van dienstverlening van leveranciers				Organisaties MOETEN toezien op correcte naleving van de relevante MedMij beheersmaatregelen die bij een leverancier belegd zijn.
A.16.1.1 Verantwoordelijkheden en procedures	✓	✓	✓	De processen voor het behandelen van incidenten en calamiteiten moeten aansluiten op de Operationele processen in het afsprakenstelsel.
A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	✓	✓	✓	Kwetsbaarheden en incidenten die betrekking hebben op persoonlijke gezondheidsgegevens of het functioneren van het MedMij stelsel MOETEN binnen 48 uur gemeld te worden bij het centrale incident management team. Zie Deelnemersovereenkomsten. DVZA maken hierover zonodig afspraken met de aangesloten ZA's.
A.16.1.7 Verzamelen van bewijsmateriaal	✓	✓	✓	Medewerking MOET worden verleend aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties. DVA maken hierover zonodig afspraken met de aangesloten Aanbieders.
A.18.2.3 (1) Beoordeling van technische naleving	✓	✓		Tenminste jaarlijks MOET een whitebox applicatiepenetratietesten worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie. De volgende specifieke MedMij eisen moeten ook aantoonbaar getoetst zijn in de pentest rapportage; • DNSSEC zie core.dns.300 en core.dns.301 • TLS zie verantwoordelijkheid core.tls.301 in combinatie met core.tls.302 en core.tls.304 • NCSC webapplicatie richtlijnen U/PW.02, U/PW.03, U/WA.03, U/WA.04 NB deze zijn voor DigiD

assessments al verplicht. Zie NOREA Handreiking DigiD assessments

Voor toetreding heeft deze minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost.

Voor penetratietesten die worden uitgevoerd na toetreding, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's (CVSS-score (Common Vulnerability Scoring System) van 4,0 of hoger) ten aanzien van de MedMij dienstverlening. Dit actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd.

A.18.2.3 (2) Beoordeling van technische naleving

Tenminste jaarlijks MOET een greybox applicatiepenetratietest worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie.

De externe koppelvlakken zijn:

- *DVP: Burgerfrontend, OAuth Client Redirect*
- *DVA: Resourceserver koppelvlak, Autorization server interface(s) eindgebruiker en voor de DVP.*
- *BO: Stelselnode en administratieve front-end*

***Voor toetreding** heeft een whitebox applicatiepentratietest minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost.*

***Bij grootschalige wijziging of herbouw** vereisen eenmalig een whitebox applicatiepenetratietest.*

				Voor penetratietesten die worden uitgevoerd **na toetreding**, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's ten aanzien van de MedMij dienstverlening. Dit actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd.
A. 5.1.1 Beleidsregels voor informatiebeveiliging	✓	✓	✓	De beleidsdocumenten MOETEN de beleidsmaatregelen die van toepassing zijn op MedMij (onder andere gespecificeerd in Privacy- en informatiebeveiligingsbeleid) specifiek benoemen.
A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	✓	✓	✓	De (eind)verantwoordelijkheid voor informatiebeveiliging MOET belegd zijn. Deze functionaris(sen) dient /dienen mandaat te hebben om bij (een dreiging van) een crisis spoedbesluiten te nemen ten aanzien van MedMij en deze besluiten met spoed te kunnen (laten) realiseren. De verantwoordelijke en operationele functionaris(sen) (inclusief eventuele onderaannemers) dient/ dienen hiervoor tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur.
A. 7.2.2 (1) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	✓	✓	✓	De verantwoordelijke functionaris (sen) zoals benoemd in A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging MOET(EN) deelgenomen hebben aan de training over de algemene werking van het stelsel.
A. 7.2.2 (2) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	✓	✓	✓	Overige medewerkers die werkzaamheden verrichten gerelateerd aan MedMij MOETEN een training hebben gevolgd over de algemene werking van het stelsel en op de voor hem/haar van toepassing zijnde beveiligingsmaatregelen.
A. 8.2.1 Classificatie van	✓	✓	✓	

informatie				De gegevens die binnen het stelsel worden verwerkt MOETEN worden behandeld conform het Informatieclassificatiebeleid (van MedMij).
A. 9.1.1 Beleid voor toegangsbeveiliging	✓	✓	✓	Er MOETEN technische en organisatorische maatregelen worden genomen om inzage van persoonlijke gezondheidsgegevens door medewerkers te voorkomen. De organisatie dient minimaal elk halfjaar en na grote wijzigingen een self-assessment uit te voeren om vast te stellen dat deze maatregelen nog effectief zijn. In (zeer) uitzonderlijke gevallen is inzage in persoonlijke gezondheidsgegevens niet te voorkomen. Hiervoor dient de organisatie een (nood)procedure te documenteren. Deze procedure dient in te gaan op: • Functiescheiding tussen vragen van toestemming voor inzage en het geven van toestemming door een verantwoordelijke functionaris; • Randvoorwaarden en maatregelen met als doel dat inzage plaatsvindt op een gecontroleerde en zo beperkt mogelijke (in tijd en hoeveelheid gegevens) wijze; • Borging dat de deelnemer voldoet wordt aan wet- en regelgeving (AVG, Meldplicht Datalekken) en de geldende versie van het MedMij Afsprakenstelsel; • Vastlegging en verantwoording van de getroffen acties.
A. 9.2.5 Beoordeling van toegangsrechten van gebruikers	✓	✓	✓	1. Toegangsrechten die zijn verstrekt op IT-componenten waar persoonlijke gezondheidsgegevens worden worden verwerkt MOETEN ten minste maandelijks worden gecontroleerd. 2. Hierbij MOET functiescheiding gewaarborgd zijn.

		3. Dit geldt ook voor eventuele onderaannemers. 4. Tijdens deze controle moet aandacht zijn voor medewerkers die geen gebruik (meer) maken van de toegangsrechten (met aantoonbare opvolging).
A. 9.4.1 Beperking toegang tot informatie	✓	Authenticatie van personen (eindgebruikers) MOET plaatsvinden op basis van minimaal twee factoren. Na succesvolle authenticatie krijgen personen alleen toegang tot hun eigen persoonlijke gezondheidsgegevens of de gegevens van de vertegenwoordigde. Scope: Dit geldt voor het gehele MedMij PGO en voor alle gebruikers die hier toegang toe krijgen. Dit is onafhankelijk of deze gebruikers MedMij uitwisselingen gebruiken of niet. Naast SMS MOET een deelnemer ook een sterkere tweede factor aanbieden. De Persoon bepaalt zelf welke tweede factor wordt gebruikt. In deze versie van het Afsprakenstelsel wordt SMS als tweede factor nog geaccepteerd. Het voornemen is deze methode te schrappen. Dit kan, op het moment dat grotere beveiligingsrisico's optreden, via een snel door te voeren patch van het Afsprakenstelsel.

Ondertekening

Hierbij verklaren ondergetekenden (auditor en vertegenwoordiger CBI) dat bovengenoemde Organisatie **wel /niet** voldoet aan het aanvullend normenkader informatiebeveiliging, release 1.5.1 MedMij Afsprakenstelsel, zoals door Stichting MedMij is uitgegeven.

(Naam auditor, datum, handtekening)

(Naam vertegenwoordiger CBI, datum, handtekening)

Beleid

Het beleid gaat in op de vraag hoe Stichting MedMij omgaat met een aantal belangrijke besturingsthema's en vormt de basis voor de Operationele processen. Het beleid is richtinggevend voor het optreden van Stichting MedMij. Het bevat tevens verantwoordelijkheden voor deelnemers. Indien de situatie daarom vraagt, mag Stichting MedMij na belangenafweging afwijken van het beleid.

Beleid inzake gecontroleerde livegang

Stichting MedMij biedt *Deelnemers* de gelegenheid om, wanneer zij zich gekwalificeerd hebben voor een specifieke *Gegevensdienst*, gefaseerd live te gaan met die *Gegevensdienst* op het MedMij-netwerk. Gedurende een zogenoemde 'gecontroleerde livegang' wordt tijdelijk afgedongen op het principe dat, indien een zekere *Aanbieder* een zekere *Gegevensdienst* aanbiedt op het MedMij-netwerk, alle daarvoor gekwalificeerde *Dienstverleners persoon* deze *Gegevensdienst* ook van deze *Aanbieder* moeten kunnen afnemen. Tijdens een gecontroleerde livegang is een *Aanbieder*, via diens *Dienstverlener aanbieder*, in de gelegenheid om die toegang te beperken tot een beperkte groep *Dienstverleners persoon*.

Zo wordt weliswaar afgedongen op een cruciaal principe van MedMij, maar staat dit in dienst van datzelfde principe: gecontroleerde livegangen zijn tijdelijk en beogen de inbedding van betrokkenen in het MedMij-netwerk waarin het principe volop geldig is.

Een gecontroleerde livegang wordt gekarakteriseerd door:

- één *Gegevensdienst*;
- één of meer *Aanbieders* die met deze *Gegevensdienst* gecontroleerd live willen gaan;
- één of meer *Dienstverleners aanbieder* die deze *Gegevensdienst* voor deze *Aanbieder(s)* ontsluiten;
- één of meer *Dienstverleners persoon* tot wie de toegang tot deze *Gegevensdienst* van deze *Aanbieder (s)* beperkt wordt gedurende de gecontroleerde livegang. *Dienstverleners persoon* kunnen desgewenst een deel van hun gebruikerskring afzonderen voor de gecontroleerde livegang, maar de organisatie en implementatie daarvan valt geheel binnen hun eigen verantwoordelijkheid.

Gecontroleerde livegangen worden alleen toegestaan op de *Interfaceversie* die hoort bij de op dat moment verplichte release. Zie Change- en releasebeleid. Bij het verouderen van een tot dan toe verplichte release stopt de gecontroleerde livegang. Het is daarom aanbevelenswaardig gecontroleerde livegangen te starten kort na een releasemoment.

Gedurende een gecontroleerde livegang kunnen *Aanbieders*, *Dienstverleners aanbieder* en *Dienstverleners persoon* toetreden tot en uitreden uit een gecontroleerde livegang. Wanneer de laatste *Aanbieder*, de laatste *Dienstverlener aanbieder* of de laatste *Dienstverlener persoon* zou uittreden, wordt de gecontroleerde livegang definitief beëindigd. Uittreding van een *Aanbieder* kan gepaard gaan met een promotie, dat wil zeggen, met het opgaan van die *Aanbieder* met de betreffende *Gegevensdienst* in het MedMij-netwerk, buiten die gecontroleerde livegang. Promotie van alle deelnemende *Aanbieders* is het uiteindelijke doel van elke gecontroleerde livegang, maar geen verplichting. Promotie is een vrije keus van de betreffende *Aanbieder* en vereist geen nadere kwalificatie of acceptatie.

Een gecontroleerde livegang wordt na drie maanden definitief beëindigd. Op gezamenlijk verzoek van betrokken partijen is hierop een eenmalig uitstel van één maand mogelijk. Een *Aanbieder* mag op eenzelfde *Gegevensdienst* niet deelnemen in een gecontroleerde livegang wanneer hij minder dan drie maanden geleden ook al betrokken was bij een gecontroleerde livegang op die *Gegevensdienst*. Stichting MedMij behoudt zich het recht voor op te treden tegen situaties waarin een *Dienstverlener persoon* concurrentieel voordeel ontleent of beoogt te ontlenen aan de tijdelijke exclusiviteit die hem gedurende een gecontroleerde livegang wordt gegund in het afnemen van de betreffende *Gegevensdienst* van een betrokken *Aanbieder*.

Op een controleerde livegang zijn onverminderd alle verantwoordelijkheden van toepassing die betrokken partijen dragen uit hoofde van hun deelname aan MedMij. Gecontroleerde livegangen worden langs geheel administratieve weg georganiseerd door de MedMij Beheerorganisatie. Van de betreffende *Gegevensdienst* wordt een kopie-*Gegevensdienst* gecreëerd en in de *Catalogus* opgenomen, waarop alleen bij de gecontroleerde livegang betrokken *Dienstverleners* erkend worden, onder de voorwaarde dat zij gekwalificeerd zijn op de originele *Gegevensdienst*. Een kopie-*Gegevensdienst* kan geen origineel zijn voor een volgende kopie. Er kunnen van één origineel-Gegevensdienst onbeperkt veel kopieën bestaan, na elkaar of tegelijkertijd. Na beëindiging van de geldigheid van een kopie-*Gegevensdienst* wordt deze nooit opnieuw geldig.

De kopie-*Gegevensdienst* is alleen geldig gedurende de gecontroleerde livegang, maar nooit buiten de geldigheidsduur van de origineel-*Gegevensdienst*. In de *OAuth Client List* en de *Aanbiederslijst* verschijnen de betrokken partijen met de kopie-*Gegevensdienst*, net zoals ze met de origineel-*Gegevensdienst* zouden verschijnen. Een gecontroleerde livegang is dus weliswaar besloten, maar niet geheim. Alle uitwisselingen in het kader van een gecontroleerde livegang worden net zo behandeld als alle andere MedMij-uitwisselingen.

Een gecontroleerde livegang is dus geen proef-deelname, maar in alle opzichten een deelname aan het MedMij-netwerk, waarin evenwel een *Gegevensdienst* voor een *Aanbieder* gefaseerd live kan worden ontsloten naar alle daartoe gekwalificeerde *Dienstverleners persoon*.

Change- en releasebeleid

Het MedMij Afsprakenstelsel evolueert voortdurend. Ontwikkelingen binnen en rondom MedMij kunnen aanleiding geven om afspraken uit het stelsel te wijzigen.

Releasecyclus

De wijzigingen aan het stelsel vinden zoveel mogelijk plaats aan de hand van een vaste releasecyclus en een releaseplanning met release momenten in april en oktober. Stichting MedMij speelt hierbij een aanjagende en faciliterende rol met een aantal verantwoordelijkheden, namelijk: het samenstellen van samenhangende releases, het ophalen van input bij belanghebbenden, het uitvoeren van impactanalyses, het organiseren van de besluitvorming en de informatievoorziening eromheen en het bewaken van ontwikkelingen in de omgeving (bijvoorbeeld veranderende wetgeving). Ook is zij voortdurend attent op wijzigingen in gebruikte normen en standaarden en heroverweegt in voorkomend geval het hergebruik.

Jaarlijks stelt Stichting MedMij samen met de verschillende belanghebbenden een releaseplanning op. De releaseplanning bevat een overzicht van geplande releases voor de periode van een jaar, geeft aan wat de belangrijkste voorgenomen wijzigingen zijn per release en duidt per geplande release de mijlpalen van het ontwikkel- en implementatietraject aan. Wijzigingen betreffende de inhoud van het afsprakenstelsel moeten passen binnen deze releaseplanning. De releaseplanning moet op haar beurt weer passen binnen de strategische kaders. Het bestuur van Stichting MedMij stelt de releaseplanning vast.

Dakpansgewijze releases

Om het ritme van de voortdurende ontwikkeling van het MedMij Afsprakenstelsel voor *Deelnemers* zo voorspelbaar mogelijk te maken, en *Deelnemers* daarbinnen ruimte te geven voor een proactief of reactief implementatiebeleid, zijn er op elk moment twee releases van het MedMij Afsprakenstelsel *actief*.
Alleen actieve releases mogen actief zijn op het operationele MedMij-netwerk. Van die twee actieve releases is er altijd één *verplicht*. Dat wil zeggen dat alle *Deelnemers* op zijn minst deze verplichte versie moeten ondersteunen. De andere actieve release heet *gepubliceerd*. Implementatie daarvan is vooralsnog niet verplicht, maar wel toegestaan op het operationele MedMij-netwerk. Omdat de Interfaces, Gegevensuitwisseling, Core in het MedMij Afsprakenstelsel geversioneerd zijn, kunnen deze tegelijkertijd actief zijn. De gepubliceerde release is de opvolger van de verplichte. Elke *Deelnemer* kan zelf kiezen wanneer hij de gepubliceerde versie implementeert, desgewenst naast de verplichte.

Wanneer een nieuwe release uitkomt van het MedMij Afsprakenstelsel, krijgt:

- de tot dan toe verplichte release de status *verouderd*, hetgeen wil zeggen dat deze release niet meer actief is;
- de tot dan toe gepubliceerde release de status *verplicht*. Deze release blijft dus actief, maar verliest haar optionele status;
- de nieuwe release de status *gepubliceerd*. Deze release wordt dus actief.

Steeds schuift dus de nieuwste release (de gepubliceerde) als een nieuwe dakpan half bovenop de (dan) verplichte. Alleen de bovenste twee dakpannen zijn actief. Hun overlap symboliseert het tegelijkertijd actief zijn op het MedMij-netwerk. Omdat MedMij een vast release-ritme hanteert (van eens per half jaar), is die overlap een halve dakpan groot. Onder de verplichte release liggen de verouderde releases, als inactieve geschiedenis van het MedMij Afsprakenstelsel.

Dakpansgewijze aanpak

Op Gegevensdiensten is tevens dakpansgewijs releasen van toepassing. Dit staat beschreven in het Gegevensdienstenbeleid.

Implicaties voor NEN-certificering

Met de publicatie van een nieuwe versie van het Afsprakenstelsel komt er ook een nieuw aanvullend normenkader beschikbaar. Om een balans te hebben tussen de benodigde tijd die deelnemers nodig hebben voor het maken van aanpassingen enerzijds, en het (te) lang moeten wachten met het verscherpen van de normen rond beveiliging anderzijds, wordt een periode van vier maanden in acht gehouden voordat de nieuwe versie van het aanvullende normenkader toegepast wordt in de NEN certificatie. Dit betekent dat de gepubliceerde versie van het aanvullend normenkader eerder verplicht en algemeen wordt dan de overige delen van het Afsprakenstelsel.

Totstandkoming releases

Alle belanghebbenden, waaronder in ieder geval de deelnemers, gebruikers en Stichting MedMij, kunnen invloed uitoefenen op (de totstandkoming van) wijzigingen in het afsprakenstelsel. Een Request For Change (RFC) kan door een belanghebbende voorzien van motivatie worden ingediend voor behandeling. Stichting MedMij doet een eerste beoordeling van ingediende RFC's door deze te toetsen aan de vigerende wet- en regelgeving, architectuur en grondslagen, strategische koers, het jaarplan en de releasekalender. Hierbij wordt onder andere beoordeeld of het daadwerkelijk gaat om een wijziging, of de wijziging niet al eerder is ingediend en wat de urgentie is. Stichting MedMij zorgt, indien nodig, voor de nadere verkenning van RFC's door wijzigingsverzoeken te laten uitwerken, de benodigde expertise en vertegenwoordiging bij elkaar te brengen, de afstemming met partijen rondom het stelsel te kanaliseren, te zorgen dat de impact van een wijziging op het stelsel en de deelnemers wordt onderzocht en indien nodig een business case wordt opgesteld met betrokkenen. Ook controleert zij of de voorgestelde oplossing vrij en kosteloos voor de deelnemers te gebruiken is.

In principe mogen betrokkenen bij het ontwikkelproces ontwikkelinformatie vrij met elkaar delen zonder aanvullende bescherming. Alleen voor informatie over kwetsbaarheden geldt dat verspreiding beperkt is tot de direct betrokkenen en alleen mag plaatsvinden met extra bescherming (zie Informatieclassificatiebeleid). Mochten belanghebbenden gedurende het change- en releaseproces bijdragen aan de uitwerking van een wijziging, dan ziet Stichting MedMij erop toe dat zij over de juiste auteursrechten komt te beschikken om de documentatie te kunnen publiceren (zie Intellectueel eigendomsbeleid).

Het afsprakenstelsel bestaat uit een samenhangende set van producten (juridisch kader, overeenkomsten, architectuur en technische specificaties, etc.) met veel onderlinge afhankelijkheden. Aanpassing van een van de onderdelen vraagt altijd om een impactanalyse op de rest van de producten. Het afsprakenstelsel wordt daarom altijd in haar geheel gereleaset. Deze releases bestaan uit een consistente set van RFC's en kunnen daarnaast verbeteringen van niet-inhoudelijke aard bevatten.

Verschillende typen releases, en correcties

Releases voor het afsprakenstelsel worden als volgt aangeduid:

1. **Major releases:** releases met grotere (functionele) wijzigingen. Deze releases worden opgenomen in de releaseplanning;
2. **Minor releases:** releases met twee soorten correctief onderhoud:
    a. Wijzigingen die nodig zijn om een onmiddellijke dreiging voor de continuïteit van of het vertrouwen in het MedMij Afsprakenstelsel/-netwerk af te wenden;
    b. Verbeteringen waarvan de baten van spoedig doorvoeren significant groter zijn dan de implementatie-inspanningen, en die op breed draagvlak onder de deelnemers kunnen rekenen.

De aanduiding van releases is opgebouwd uit drie nummers, namelijk x.y.z (bijvoorbeeld 1.3.2). Bij een major release wordt de combinatie x.y opgehoogd. Daarbij zijn twee opties, ofwel y wordt met een verhoogd

waarna z op 0 wordt gezet (bijvoorbeeld van 1.3.2 naar 1.4.0), ofwel x wordt met een verhoogd waarna y en z op 0 worden gezet (bijvoorbeeld van 1.3.2 naar 2.0.0). De keuze hiertussen is afhankelijk van aard en omvang van de release. Bij een minor release wordt z met een verhoogd (bijvoorbeeld van 1.3.2 naar 1.3.3).

Major release vinden twee maal per jaar plaats. De inhoud van een major release wordt samengesteld op basis van uitgewerkte wijzigingsvoorstellen (RFC's). Minor releases zijn niet bij voorbaat gepland; zij worden alleen indien nodig tussen major releases uitgebracht, op een datum die in overleg met *Deelnemers* wordt vastgesteld.

Daarnaast kunnen correcties op het MedMij Afsprakenstelsel worden aangebracht zonder dat deze leiden tot een nieuwe release. Deze doen bijvoorbeeld acute reparaties, verwijderen inconsistenties of passen voorbeeldberichten aan. Een correctie tast de juridische en technische strekking van het MedMij Afsprakenstelsel niet aan; waar dit wel het geval zou zijn, vereist de wijziging een nieuwe release. Correcties worden op een aparte pagina in het MedMij Afsprakenstelsel aangegeven.

Besluitvorming releases

Bij major releases legt Stichting MedMij de release eerst voor aan de deelnemersraad, die hierover een zwaarwegend advies afgeeft. Het bestuur is niet gehouden aan dit advies, maar dient het advies van de raad wel serieus te nemen en een afwijking te onderbouwen. De besluitvorming over de release door het bestuur behoeft de goedkeuring van de eigenaarsraad. De eigenaarsraad dient hierbij geïnformeerd te worden over het advies van de deelnemersraad en eventueel over de motivatie van het bestuur om van dit advies af te wijken.

Indien het bestuur van Stichting MedMij wijzigingen eerder wil laten implementeren dan in de releaseplanning mogelijk is, dan kan worden besloten tot invoering middels een minor release. Er wordt dan een tussentijdse release van het afsprakenstelsel gecreëerd die niet eerder was gepland. Bij minor releases is het aan het bestuur of en op welke wijze belanghebbenden worden betrokken bij de totstandkoming. Goedkeuring van de eigenaarsraad en advisering van de deelnemersraad zijn bij een minor release niet noodzakelijk.

Implementatie releases

Zodra het besluit over een release van het afsprakenstelsel is genomen, bepaalt Stichting MedMij in overleg met de deelnemers en eigenaren welke aanpak de minste impact en verstoringen veroorzaakt. Ook maakt de stichting de afweging of releases in productie naast elkaar kunnen bestaan en of deelnemers op enig moment meerdere releases moeten ondersteunen. Voor de implementatie van de release zijn de data in de implementatieplanning bij de release leidend. Afhankelijk van het soort release kan een implementatietermijn van toepassing zijn.

Stichting MedMij is ervoor verantwoordelijk dat het change- en releaseproces volgens afspraak wordt uitgevoerd, de planning te monitoren op risico's voor de afgesproken ingebruiknamemomenten, en waar nodig te escaleren op het juiste niveau. Ook zorgt zij voor een gestructureerde doorvoering van aanpassingen in de documentatie en het publiceren van een nieuwe release van het afsprakenstelsel (minimaal in de vorm van een pdf voor de administratie van deelnemers).

Dienstverleningsoverdrachtsbeleid

Een Dienstverlener aanbieder kan, op verzoek van de Aanbieder, het ontsluiten van een Gegevensdienst namens die Aanbieder van een andere Dienstverlener aanbieder overnemen. Deze overnemende Dienstverlener aanbieder moet in dat geval erkend zijn als ontsluiter van die gegevensdienst en bij Stichting MedMij aan kunnen tonen de overname met de latende deelnemer te hebben afgestemd. Uit de afstemming moet minimaal blijken dat het moment van overname is afgestemd, zodat de continuïteit van dienstverlening zo hoog mogelijk blijft.

Gegevensdienstenbeleid

Gegevensdiensten en de *Catalogus*

Deelnemers ontsluiten via MedMij gestandaardiseerde diensten voor gegevensuitwisseling, de zogeheten *Gegevensdiensten*. De *Gegevensdiensten* die zijn toegestaan binnen MedMij staan in de Catalogus.

Een *Gegevensdienst* wordt gevormd uit een verzameling *Systeemrollen* en één of meer usecase(-s) uit het MedMij Afsprakenstelsel. Een *Systeemrol* is een verzameling verantwoordelijkheden voor de elektronische uitwisseling van gegevens. De verantwoordelijkheden worden gedefinieerd in de bij de *Systeemrol* behorende onderdelen van een *Informatiestandaard*. De *Gegevensdiensten* worden ontsloten via bijbehorende usecases uit de architectuur van het MedMij Afsprakenstelsel. Zolang nieuwe *Gegevensdiensten* passen binnen de bestaande usecases, kunnen ze onafhankelijk van een release van het MedMij Afsprakenstelsel worden toegevoegd aan de *Catalogus*. Mocht voor een *Gegevensdienst* (een) nieuwe usecase nodig zijn, dan dient eerst deze nieuwe usecase te worden toegevoegd volgens het reguliere change- en releaseproces. Pas daarna kan ook deze nieuwe *Gegevensdienst* worden toegevoegd aan de *Catalogus*. Besluiten over de creatie, wijziging en beëindiging van een *Gegevensdienst* en de wijze waarop een *Gegevensdienst* wordt opgenomen in de *Catalogus* worden genomen door het bestuur van Stichting MedMij.

Creatie van *Gegevensdiensten*

Een *Gegevensdienst* wordt gevormd uit een verzameling *Systeemrollen* en één of meer usecase(-s) uit het MedMij Afsprakenstelsel. Stichting MedMij, de beheerder van het MedMij Afsprakenstelsel en de beheerder (s) van de *Informatiestandaarden* waarvan *Systeemrollen* tot de *Gegevensdienst* zouden gaan behoren stemmen dit af. Daarbij zijn de eigenschappen die een *Gegevensdienst* verkrijgt in de *Catalogus* (ook) onderwerp van gesprek.

De *Systeemrollen* worden voorafgaand aan de opname in een *Gegevensdienst* beoordeeld aan de hand van een serie eisen. Deze eisen dienen als hulpmiddel bij het beoordelen van de geschiktheid van de *Systeemrollen*. Ze zijn niet uitputtend (er zijn ook andere afwegingsgronden) en niet blokkerend (het niet voldoen aan een eis betekent niet als vanzelf dat de *Systeemrol* ongeschikt is).

Indien de creatie van een *Gegevensdienst* bedoeld is als opvolging van een geldige *Gegevensdienst* gebeurt dit dakpansgewijs. Dat betekent dat er maximaal 2 *Gegevensdiensten* zijn opgenomen in de *Catalogus* op basis van dezelfde *Transactienaam*. De actuele *Catalogus* bevat een *Gegevensdienst* die op dat moment geldig is en de basis vormt voor ontsluiting op het MedMij Netwerk. De creatie van de zogenaamd aankomende *Gegevensdienst* zal plaatsvinden in het daarvoor bestemde onderdeel van de *Catalogus.* Deze *Gegevensdienst* krijgt een toekomstige ingangsdatum van de geldigheid die overeenkomt met de releasedatum van het MedMij Afsprakenstelsel. Hier kan worden van afgeweken indien een situatie daarom vraagt, een dergelijk besluit wordt genomen door het bestuur van Stichting MedMij.

Mutaties van *Gegevensdiensten*

Mutaties van *Gegevensdiensten* door Stichting MedMij zijn toegestaan, met uitzondering van:

- Het wijzigen van de *Systeemrolverzameling* of de daarin opgenomen *Systeemrollen*.
- Het wijzigen van de *Usecase*.
- Het wijzigen van het *GegevensdienstId*.
- Het wijzigen van de verzameling Gegevensdiensten die wordt *Vereist*.

De concepten zijn precies gedefinieerd in het metamodel.

Uitfaseren van *Gegevensdiensten*

Een *Gegevensdienst* kan worden uitgefaseerd.

De volgende triggers kunnen leiden tot het uitfaseren van *Gegevensdiensten*:

- De *Systeemrollen* worden niet langer als geschikt beoordeeld;
- Een aankomende *Gegevensdienst* geldig wordt die de *Gegevensdienst Vervangt*;
- De *Gegevensdienst* is niet langer compatibel met de operationeel bruikbare versies van het MedMij Afsprakenstelsel.

Het moment van uitfaseren van een *Gegevensdienst* wordt kenbaar gemaakt door een einddatum van de betreffende gegevensdienst op te nemen in de Catalogus.

Gegevensdiensten die elkaar vereisen of vervangen

Stichting MedMij kan in de *Catalogus* aangeven dat de ene *Gegevensdienst* de andere vereist wanneer *Zorgaanbieders* die de ene *Gegevens-dienst*aanbieden, verplicht worden om ook de andere aan te bieden. Dit is vaak het geval als de *Gegevens-diensten*samen een proces vormen, zoals het verzamelen en delen van gegevens. Vereisen hoeft geen wederzijdse relatie te zijn, maar dat kan wel.

Indien een aankomende *Gegevensdienst* een geldige *Gegevensdienst* vervangt, dan komen de ingangsdatum van de geldigheid en de *Einddatum* van de te vervangen *Gegevensdienst* overeen, tenzij er zwaarwegende redenen zijn om hiervan af te wijken.

Erkenning van *Deelnemer* als ontsluiter van een *Gegevensdienst*

Deelnemers ontsluiten *Gegevensdiensten* via het MedMij-netwerk voor en namens gebruikers. Voordat een *Deelnemer* in deze rol wordt erkend, dient zij aan te tonen de *Gegevensdienst* op de juiste manier te ondersteunen. In de *Catalogus* staat per *Gegevensdienst* beschreven welke relevante *Systeemrollen* uit de bijbehorende *Informatiestandaard* en welke usecase uit de Architectuur en technische specificaties ondersteund dienen te worden. Ook geeft de *Catalogus* aan welke andere *Gegevensdiensten* vereist. Indien een *Deelnemer* nog niet over een erkenning voor een vereiste *Gegevensdienst* beschikt, dan dient deze partij eerst deze erkenning te behalen. In het Testbeleid staat verder beschreven hoe de ondersteuning van de *Gegevensdienst* en, indien nodig, de usecase, kan worden aangetoond. Stichting MedMij ziet erop toe dat aan alle voorwaarden wordt voldaan, alvorens erkenningen wordt afgegeven

Informatieclassificatiebeleid

Het informatieclassificatiebeleid beschrijft de manier waarop Stichting MedMij en de deelnemers informatie classificeren, zodat deze informatie passend kan worden behandeld vanuit het oogpunt van informatiebeveiliging. Dat betekent dat de omgang met de informatie (en de bijbehorende maatregelen rond onder meer beveiliging toegang) moet aansluiten bij het vereiste zekerheidsniveau in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

Om deze aansluiting praktisch hanteerbaar te maken, hanteert MedMij een beperkt aantal classificatieniveaus en een eenvoudige wijze van het koppelen van een niveau aan informatie. Daarmee behoeft niet voor elk afzonderlijk informatie-element een afzonderlijke inschatting op de zekerheidsaspecten, noch een afzonderlijke afweging over de bijpassende informatiebeveiligingsmaatregelen gemaakt te worden.

Classificaties

In onderstaande tabel zijn de gehanteerde classificaties opgesomd. Voor de classificatie van de zekerheidsaspecten is aangesloten bij NEN7512:2015.

		Classificatie van zekerheidsaspecten		
MedMij-classificatie	**Type informatie**	**Beschikbaarheid**	**Integriteit**	**Vertrouwelijkheid**
Gezondheid	Gegevens waaruit direct of indirect informatie over de gezondheid van een persoon uit kan worden afgeleid.	Midden	Hoog	Zeer hoog
Operationele kern	Gegevens die operationeel noodzakelijk zijn voor de gegevensuitwisseling via het MedMij-netwerk.	Midden	Hoog	Laag
Samenwerking en ontwikkeling	Gegevens die betrekking hebben op de communicatie van partijen over de huidige of toekomstige inhoud van het MedMij Afsprakenstelsel en de afsprakenset.	Laag	Midden	Laag
Kwetsbaarheid	Niet algemeen bekende gegevens over een (mogelijke) kwetsbaarheid bij een of meerdere deelnemers of de beheerorganisatie, al dan niet voortkomend uit de afsprakenset, waarmee een kwaadwillende partij inbreuk op de informatiebeveiliging van het MedMij-netwerk zou kunnen maken.	Laag	Midden	Hoog

Labeling

In onderstaande tabel is aangegeven welke typen informatie of informatieproducten volgens welke MedMij-classificatie behandeld moeten worden. De informatie zelf wordt niet afzonderlijk voorzien van een 'label'; op grond van dit beleid moet deze informatie worden behandeld conform de bijbehorende classificatie.

Voor informatieproducten die niet in deze tabel voorkomen moet na analyse ofwel

- een passende MedMij-classificatie, worden gekozen en is labeling noodzakelijk om duidelijk te maken wat de MedMij-classificatie van de informatie is; ofwel
- wanneer geen passende MedMij-classificatie voorhanden is, een afzonderlijke behandeling plaatsvinden. De drie zekerheidsaspecten moeten worden geclassificeerd, de noodzakelijke informatiebeveiligingsmaatregelen moeten worden bepaald en het moet voor degenen die toegang hebben tot de informatie duidelijk zijn hoe die informatie behandeld moet worden. Dat kan door de informatie te voorzien van een label of andere aanduiding, dan wel door langs andere weg duidelijkheid te verschaffen over de regels rond de omgang met de betreffende informatie.

Type informatie	MedMij-classificatie
Functionele logging op grond van de afspraken onder Verantwoordelijkheden, Core en de verantwoordelijkheden binnen de verschillende extensies.	Gezondheid
Alle gegevens verkregen of verstrekt in het kader van een van de interacties in het kader van de usecases uit de Architectuur en technische specificaties	Gezondheid
Aanbiederslijst	Operationele kern
Whitelist	Operationele kern
OAuthclientlist	Operationele kern
Gegevensdienstnamenlijst	Operationele kern
Inhoud van het MedMij Afsprakenstelsel	Samenwerking en ontwikkeling
Informatie ten behoeve van of aangaande doorontwikkeling	Samenwerking en ontwikkeling
Kwetsbaarheden	Kwetsbaarheid
Risicoanalyse op stelselniveau	Kwetsbaarheid
Gegevens in het kader van forensisch onderzoek, indien deze geen persoonsgegevens bevatten	Kwetsbaarheid
Gegevens in het kader van forensisch onderzoek, indien deze wel persoonsgegevens bevatten	Gezondheid
Verklaringen van auditors over de toepassing van NEN7510 en het Normenkader informatiebeveiliging, voor zover daarin opmerkingen zijn opgenomen aangaande niet-volledige compliance	Kwetsbaarheid
Rapporten van penetratietesten	Kwetsbaarheid

Maatregelen

In onderstaande tabel is indicatief (zonder de pretentie volledig te zijn) aangegeven waar de maatregelen te vinden zijn die van toepassing zijn op informatie die is gelabeld met een bepaalde MedMij-classificatie. Deze maatregelen betreffen veelal de omgang in het kader van de uitwisseling tussen partijen. Deelnemers en de beheerorganisatie zijn daarnaast op grond van het Normenkader informatiebeveiliging (maatregel A.8.2.1 Classificatie van informatie) verplicht om ook hun interne informatiebeveiliging te laten aansluiten bij de MedMij-classificatie. Dat betekent dat zij de informatie van een interne classificatie moeten voorzien die op geen van de drie zekerheidsaspecten (betrouwbaarheid, integriteit, vertrouwelijkheid) lager is dan die van de MedMij-classificatie die verbonden is aan de informatie.

MedMij-classificatie	Maatregelen
Gezondheid	Architectuur en technische specificaties: beschrijft de maatregelen om de uitwisseling van gezondheidsgegevens veilig en betrouwbaar te laten plaatsvinden. Normenkader informatiebeveiliging: beschrijft de aanvullende maatregelen die deelnemers minimaal moeten treffen om ook in het eigen domein op veilige en betrouwbare manier met gezondheidsgegevens om te gaan. Deelnemersovereenkomsten: beschrijft de juridische bepalingen tussen Stichting MedMij en de deelnemers gericht op de privacy en (informatie)beveiliging van gezondheidsgegevens (artikel 5).
Operationele kern	Architectuur en technische specificaties: beschrijft de maatregelen om op veilige en betrouwbare wijze om te gaan met de operationele uitwisselgegevens. Normenkader informatiebeveiliging: beschrijft de aanvullende maatregelen die deelnemers minimaal moeten treffen om ook in het eigen domein op veilige en betrouwbare manier met de operationele uitwisselgegevens om te gaan.
Samenwerking en ontwikkeling	Change- en releasebeleid: beschrijft hoe met ontwikkelinformatie moet worden omgegaan bij de doorontwikkeling van het MedMij Afsprakenstelsel. Samenwerkings- en escalatiebeleid: beschrijft de onderlinge samenwerking en communicatie van partijen rondom het afsprakenstelsel.
Kwetsbaarheid	Privacy- en informatiebeveiligingsbeleid: beschrijft welke maatregelen zijn ingericht om de privacy- en informatiebeveiliging van het stelsel te borgen. Operationele processen: beschrijft met het Proces beheren technische kwetsbaarheden hoe met kwetsbaarheden wordt omgegaan.

Intellectueel eigendomsbeleid

Het merk MedMij en het Afsprakenstelsel MedMij zijn intellectueel eigendom van Stichting MedMij. Dit geldt niet voor de implementaties bij deelnemers, standaarden waarnaar wordt verwezen in het afsprakenstelsel en de generieke voorzieningen, voor zover niet door of in opdracht van Stichting MedMij ontwikkeld.

Merkenrecht

Het merk MedMij is geregistreerd om op te kunnen treden tegen merkinbreuk of onrechtmatig gebruik van het merk door andere partijen. Een deelnemer aan het stelsel mag het merk MedMij, zowel woord- als beeldmerk, hanteren conform de aanwijzingen voor juist merkgebruik zoals opgenomen bij Communicatie. Gebruik van het merk buiten de vastgelegde afspraken is niet toegestaan. Deelnemers mogen alleen gebruik maken van het merk als en zolang zij deelnemer zijn. Zij worden gebonden aan deze afspraken via de deelnemersovereenkomst met Stichting MedMij. Zij zullen niets doen/nalaten waardoor de rechten van het merk kunnen worden aangetast en/of de opgebouwde goodwill negatief kan worden beïnvloed. Gebruik van het merk en beeld door andere partijen dan de deelnemers, is alleen toegestaan onder verantwoordelijkheid van een deelnemer of indien hiervoor van tevoren toestemming is verkregen van Stichting MedMij.

Communicatie bevat aanwijzingen voor het naam en merkgebruik, huisstijlafspraken en communicatierichtlijnen voor het merk MedMij. Stichting MedMij is verantwoordelijk voor het aanleveren van deze richtlijnen, standaard tekst- en beeldmateriaal en andere tools die de deelnemers bij hun dienstverlening dienen te gebruiken.

Auteursrecht

De inhoud van het MedMij Afsprakenstelsel heeft, vanuit het perspectief van de auteurswet, per definitie een auteur en rechthebbende. Zonder aanvullende afspraken hierover heeft de maker van het werk het auteursrecht. Andere partijen moeten expliciet toestemming krijgen voor het gebruik en de verspreiding van het desbetreffende werk. Gezien de aard van het afsprakenstelsel en de preconcurrentiële wijze van totstandkoming, is dit niet gepast en maakt Stichting MedMij hier aanvullende afspraken over.

Stichting MedMij dient het auteursrecht van de documentatie voor het MedMij Afsprakenstelsel te verkrijgen voorafgaand aan het maken of de doorontwikkeling. Partijen die bijdragen aan de totstandkoming van de documentatie (ook betaalde opdrachtnemers, zoals adviseurs en ontwikkelaars), dragen schriftelijk het intellectueel eigendom op hun bijdrages over aan Stichting MedMij. Voor deelnemers wordt de overdracht van het intellectueel eigendom over hun bijdrages aan de documentatie geregeld via de Deelnemersovereenkomsten. Indien bijdrages aan de documentatie van het stelsel niet door of in opdracht van Stichting MedMij worden gemaakt, dan moet het auteursrecht eerst aan de stichting worden overgedragen, alvorens het materiaal gebruikt wordt. Stichting MedMij ziet toe op de overdracht van het intellectueel eigendom/het gebruiksrecht. Deelnemers dienen zich te onthouden van inbreuken op de Intellectuele Eigendomsrechten van zaken die door, voor of namens Stichting MedMij zijn ontwikkeld.

Creative Commons-licentie

Stichting MedMij regelt de toestemming voor het gebruik en de verspreiding van het MedMij Afsprakenstelsel door de documentatie te publiceren onder de Creative Commons-licentie **Naamsvermelding-GeenAfgeleideWerken 4.0 Internationaal (CC BY-ND 4.0)**. Deze Creative Commons-licentie stelt twee voorwaarden aan het gebruik en de verspreiding:

- **Naamsvermelding.** Anderen mogen het MedMij Afsprakenstelsel kopiëren, distribueren, vertonen en opvoeren, maar uitsluitend als MedMij wordt vermeld als maker.

- **GeenAfgeleideWerken.** Anderen mogen het MedMij Afsprakenstelsel kopiëren, distribueren, vertonen en opvoeren mits het werk in de originele staat blijft. Het is niet toegestaan dat anderen het stelsel gebruiken als basis voor nieuw materiaal en/of het stelsel in aangepaste vorm verspreiden.

Klachten- en geschillenbeleid

Een klacht is een uiting van ongenoegen, gericht aan Stichting MedMij over de dienstverlening van een deelnemer of Stichting MedMij. Een geschil is een onenigheid tussen twee of meer partijen naar aanleiding van de uitvoering van een MedMij-dienst. Binnen MedMij kan sprake zijn van drie soorten klachten en geschillen:

1. Tussen de deelnemers onderling;
2. Tussen de deelnemers en Stichting MedMij.

De ambitie is om klachten en geschillen op te lossen binnen het stelsel. Wanneer betrokken partijen in onderling overleg zelf niet tot een oplossing komen, kunnen zij klachten en geschillen voorleggen aan Stichting MedMij (zie Samenwerkings- en escalatiebeleid). De klachten en geschillen moeten gerelateerd zijn aan het niet-nakomen van de afspraken/deelnemersovereenkomst door een deelnemer en/of Stichting MedMij. Stichting MedMij doet geen uitspraken over de dienstverlening van een deelnemer aan een gebruiker. De rechtsrelatie tussen de deelnemer en haar gebruikers valt buiten de scope van het MedMij Afsprakenstelsel (zie ook Overeenkomsten en rechtsrelaties).

Mocht het onverhoopt niet lukken om klachten en/of geschillen onderling tussen partijen op te lossen, dan zijn er buiten het stelsel twee routes om conflicten te beslechten. Dit zijn 1) de betrokken partijen komen een vorm van alternatieve geschillenbeslechting overeen of 2) de betrokken partijen stappen naar de rechter. P artijen wordt aangeraden om zich telkens te beraden op de mogelijkheden voor alternatieve geschillenbeslechting.

Indien gebruikers klachten hebben over de naleving van de MedMij-afspraken door een deelnemer, dan kunnen zij deze richten aan het klachtenloket van de uitvoeringsorganisatie. Stichting MedMij zal de klacht onderzoeken en de deelnemer erop aanspreken, mocht deze zich inderdaad niet aan de regels houden. De deelnemer dient daarnaast te allen tijde zelf processen ingericht te hebben om te voorkomen dat klachten die niet-gerelateerd zijn aan de MedMij-afspraken worden gericht aan Stichting MedMij.

Nalevingsbeleid

Een goede naleving van het afsprakenstelsel is onontbeerlijk voor het vertrouwen in het stelsel. Zowel deelnemers, Stichting MedMij, als indirect de wettelijke toezichthouders hebben een rol bij de instandhouding van het netwerk en de borging van het naleven van het afsprakenstelsel. In eerste instantie gebeurt de naleving zo veel mogelijk vanuit een zelfregulerend systeem en in goed onderling overleg tussen partijen in het afsprakenstelsel (zie Samenwerkings- en escalatiebeleid). In tweede instantie kan het echter noodzakelijk zijn een correcte naleving te bewerkstelligen door middel van een interventie.

De afspraken uit het MedMij Afsprakenstelsel kennen een privaatrechtelijk karakter. Het bestuur van Stichting MedMij is daarom zelf verantwoordelijk voor de controle op de naleving van deze afspraken. Deelnemers hebben zich via de ondertekende deelnemersovereenkomst verplicht tot het naleven van de stelselafspraken voor hun specifieke rol. Bij toetreding tonen deelnemers aan dat zij aan de afspraken voldoen. Ook tijdens deelname moeten *Deelnemers* aan de afspraken blijven voldoen. Daartoe kennen de testresultaten van een *Deelnemer*, waarop diens toetreding is gebaseerd, een geldigheidsduur die gemaximeerd is op 365 dagen.

Signalen over het niet naleven van de afspraken door deelnemers komen via meerdere routes bij de beheerorganisatie binnen, waaronder bij:

- Een bemiddeling door Stichting MedMij bij een escalatie in de samenwerking (zie Samenwerkings- en escalatiebeleid);
- Verzoeken tot handhaving, meldingen van misstanden of afwijkingen en klachten (Klachten- en geschillenbeleid);
- De test bij de erkenning van een deelnemer als ontsluiter van een gegevensdienst (zie Testbeleid);
- Bij de implementatie van een nieuwe release van het stelsel (zie Change- en releasebeleid);
- De jaarlijkse aanlevering van bewijsmateriaal voor de NEN 7510-certificering en de toepassing voor MedMij (zie Normenkader informatiebeveiliging).

Het handhaven van de afspraken verloopt langs privaatrechtelijke lijnen. Bij signalering van niet-naleving worden daarom de volgende stappen doorlopen:

1. **Constatering en vastlegging.** Stichting MedMij beschrijft zo concreet mogelijk welke verplichting van het MedMij Afsprakenstelsel het betreft, alsmede wat de concrete omstandigheden van het geval zijn. Voorbeelden van aanleidingen voor constateringen zijn:
    a. het verlopen van de geldigheidsduur van de testresultaten van de *Deelnemer*;
    b. het aanmelden van een entry voor op de *OAuthClientList* in relatie waarmee de *Dienstverlener persoon* niet (geheel) erkend is;
    c. het aanmelden van een entry voor op de *Aanbiederslijst* in relatie waarmee de *Dienstverlener aanbieder* niet (geheel) erkend is;
2. **Verificatie en verzoek om nadere toelichting.** De constatering van de niet-naleving wordt schriftelijk voorgelegd aan de desbetreffende deelnemer. De deelnemer dient hierop te reageren en aan te geven welke maatregelen binnen welke termijn worden getroffen om de niet-naleving op te lossen;
3. **Beoordeling nadere toelichting van deelnemer en communicatie besluit.** Op basis van de ontvangen informatie beoordeelt Stichting MedMij of, gelet op de aard en de ernst van de verplichting die niet wordt nageleefd, de door de deelnemer voorgestelde maatregelen en het benodigde tijdbestek passend zijn. Hierbij worden de criteria gehanteerd die ook worden gehanteerd bij het bepalen van de redelijke termijn bij een formele ingebrekestelling (zie hieronder). Indien de niet-naleving de veilige en betrouwbare werking van het netwerk in het geding brengen, dan kan Stichting MedMij beslissen om de overeenkomst tijdelijk op te schorten (zoals overeengekomen in artikel 7.3 van de deelnemersovereenkomst). De deelnemer wordt schriftelijk geïnformeerd over de beoordeling;
4. **Formele ingebrekestelling.** De formele ingebrekestelling is de laatste aanmaning om te voldoen aan de niet-naleving en geschiedt schriftelijk;

5. **Formele beëindiging deelnemersovereenkomst.** Nadat de termijn is verstreken die in de ingebrekestelling is opgenomen, is de deelnemer in verzuim. Op dat moment kan de deelnemersovereenkomst door Stichting MedMij worden ontbonden.

Tijdens elk van deze stappen kan door Stichting MedMij worden geconstateerd dat er ofwel geen sprake (meer) is van niet-naleving, ofwel dat er voldoende zicht is op naleving. Indien er geen sprake (meer) is van niet-naleving, dan wordt de procedure beëindigd. Bij voldoende zicht op naleving, wordt nog vinger aan de pols gehouden.

De tenuitvoerlegging van het nalevingsbeleid is een zaak van Stichting MedMij. Besluiten over opschorting of uitsluiting van deelname lopen via Stichting MedMij.

Stichting MedMij gaat vertrouwelijk om met dossiers aangaande lopende en afgesloten nalevingszaken. Besluiten over opschorting en uitsluiting van deelname zijn daarentegen openbaar.

Formele ingebrekestelling

De ingebrekestelling is een schriftelijke sommatie waarin de deelnemer door Stichting MedMij wordt gesommeerd een voor hem geldende verplichting uit het MedMij Afsprakenstelsel, binnen een bepaalde termijn, na te komen. De ingebrekestelling is de laatste mogelijkheid die de deelnemer wordt geboden om de niet-naleving op te heffen. Indien de gestelde termijn wordt overschreden is de deelnemer in verzuim. Op het moment dat de deelnemer in verzuim is, kan de overeenkomst door Stichting MedMij worden ontbonden.

In de wet is niet aangegeven wat onder een redelijke termijn wordt verstaan, alleen dat een redelijke termijn moet worden gesteld. Of een bepaalde termijn redelijk is, wordt uiteindelijk bepaald door de rechter, gelet op de concrete omstandigheden van het geval. Voor Stichting MedMij betekent dit dat per geval voor de desbetreffende deelnemer, gelet op de verplichting die hij niet nakomt, moet worden bepaald wat een haalbare termijn is om de desbetreffende verplichting alsnog na te komen. De criteria die Stichting MedMij hanteert in haar afweging bij het bepalen van een redelijke termijn zijn:

- de kans dat het vertrouwen in het merk MedMij wordt geschaad;
- de kans dat de niet-naleving (imago)schade voor het merk MedMij oplevert;
- de kans dat de niet-naleving (imago)schade voor de overige deelnemers in het MedMij Afsprakenstelsel oplevert;
- de kans dat het afsprakenstelsel MedMij als geheel beveiligingsrisico’s loopt;
- de gangbare doorlooptijd voor een bepaalde actie;
- of, en zo ja, welke ((inter)nationale) afspraken er worden gehanteerd voor de invoering /implementatie van een bepaalde actie.

OAuthclient-namenbeleid

Binnen de OAuth-flow wordt aan de Persoon toestemming gevraagd voor de gegevensuitwisseling tussen een Aanbieder en de OAuthclient van de Dienstverlener persoon (zie Toestemmingsverklaring). Om in de bijbehorende toestemmingsverklaring een gebruiksvriendelijke naam voor de OAuthclient te kunnen presenteren, is de OAuth Client List in het leven geroepen. Met deze lijst kan de Dienstverlener aanbieder de gebruiksvriendelijke naam van de OAuthclient vinden en gebruiken in de toestemmingsverklaring.

Het OAuthclient-namenbeleid beschrijft hoe een Dienstverlener persoon een voor de persoon herkenbare naam kiest, zonder dat door een te grote variëteit aan namen voor de Persoon onduidelijkheid ontstaat over de toestemming.

Wie kiest de OAuthclient-naam?

De Dienstverlener persoon bepaalt de gekozen naam en geeft deze door aan Stichting MedMij. Stichting MedMij stelt de naam vast.

Waar moet de OAuthclient-naam aan voldoen?

1. De naam moet gelijk zijn aan een handelsnaam van de Dienstverlener persoon, zoals opgenomen in het handelsregister;
2. De naam is minimaal drie en maximaal 50 karakters lang;
3. De naam mag niet te herleiden zijn tot een persoon;
4. De naam mag het merk MedMij niet negatief beïnvloeden.

Performancebeleid

De totale performance van het MedMij-netwerk hangt af van de individuele prestaties van deelnemers en *MedMij Registratie*. Aangezien de persoon binnen MedMij de regie voert over de uitwisseling van gegevens, initieert de *Dienstverlener persoon* bij de functies Verzamelen en Delen de interacties en reageert de Dienstverlener aanbieder. Om die reden zijn er afspraken opgenomen over de beschikbaarheid en reactietijd van Dienstverleners zorgaanbieder (zie Token interface en Resource interface). Bij de overige usecases voor het opvragen van de lijsten initiëren deelnemers en reageert MedMij Registratie. Er zijn daarom ook afspraken opgenomen over de beschikbaarheid van MedMij Registratie (zie Interfaces lijsten).

Mochten deelnemers bij elkaar constateren dat de performance achterblijft of dat er fouten ontstaan in de onderlinge interacties, dan wordt van hen naar redelijkheid verwacht dat ze inspanning verrichten om dit onderling aanhangig te maken en te kijken of het daarmee opgelost kan worden. Stichting MedMij kan hierbij faciliteren en mediëren (zie ook Samenwerkings- en escalatiebeleid). Deelnemers gebruiken alle aanwezige logging, tevens naar redelijkheid, om een probleem te helpen oplossen.

> **Toelichting**
>
> Om fouten in de eerste productieversie van het stelsel tijdig op te sporen, organiseert Stichting MedMij een platform om fouten op te sporen en op te lossen. Deelnemers leveren hieraan actief een bijdrage.

Mochten de prestaties van een deelnemer achterblijven en/of een deelnemer toont onvoldoende inzet om problemen op te lossen, dan treedt het Nalevingsbeleid in werking.

Privacy- en informatiebeveiligingsbeleid

Aangezien gezondheidsgegevens van personen erg privacygevoelige gegevens zijn, zijn privacy en informatiebeveiliging belangrijke thema's binnen MedMij. De privacy en informatieveiligheid is, in aanvulling op de wet- en regelgeving die per definitie van toepassing is op de deelnemer, op drie manieren geborgd in het stelsel:

- Door de gegevensuitwisseling tussen deelnemers in hoge mate van detail te beschrijven en belangrijke maatregelen op het gebied van privacy en informatiebeveiliging hierin op te nemen (zie de Architectuur en technische specificaties);
- Door strenge eisen te stellen aan de privacy en informatiebeveiliging van deelnemers in het eigen domein (zie het Normenkader informatiebeveiliging);
- Door onder verantwoordelijkheid van Stichting MedMij aanvullende procedures in te richten, zoals de toetsing van deelnemers op het nakomen van de (privacy- en informatiebeveiligings)afspraken bij toetreding en gedurende deelname (zie onder andere Toetredingsbeleid en Nalevingsbeleid).

Stichting MedMij voert de regie over het in kaart brengen van privacy- en informatiebeveiligingsrisico's die individuele deelnemers overstijgen (stelselrisico's) en doet voorstellen voor maatregelen. Hiervoor vindt jaarlijks een Risicoanalyse plaats. Ook wordt, indien de aard, omvang of context van de gegevensuitwisselingen over het MedMij-netwerk of direct daaraan gerelateerde verwerkingen significant verandert, opnieuw een Privacy Impact Assessment (PIA) uitgevoerd. Op basis van deze risicoanalyse en/of PIA worden maatregelen heroverwogen en eventueel aanvullende privacy- en informatiebeveiligingsmaatregelen gedefinieerd. Dit kan resulteren in bijstelling van het Normenkader informatiebeveiliging en de Architectuur en technische specificaties. Er wordt getracht (nieuwe) afspraken zoveel mogelijk aan te laten sluiten bij eisen van andere stelsels en hergebruik van bestaande certificeringen mogelijk te maken om de implementatie-, financiële en administratieve lasten voor deelnemers zoveel mogelijk beperkt te houden.

Samen met de deelnemers wordt ook op andere wijze toegezien op de privacy en informatiebeveiliging van het stelsel. Stichting MedMij en elke afzonderlijke deelnemer wijzen ieder een verantwoordelijke voor privacy en informatiebeveiliging aan (zie Normenkader informatiebeveiliging en tussen deze verantwoordelijken is minimaal vier keer per jaar overleg. Hieromheen is een incidenten- en calamiteitenprocedure en een proces beheren technische kwetsbaarheden ingericht, zodat duidelijk is wat er van de verschillende partijen wordt verwacht in noodsituaties (zie Operationele processen). Deelnemers zijn verantwoordelijk voor het doorgeven van de juiste contactpersoon en informeren Stichting MedMij bij wijzigingen.

Ten slotte zorgt Stichting MedMij verder voor afstemming over privacy en veiligheid met bestaande partijen en ontwikkelingen in de zorg en worden de belangrijkste ontwikkelingen in de wereld op dit gebied gevolgd.

Risicoanalyse

Stichting MedMij voert elk jaar in samenspraak met deelnemers aan het MedMij Afsprakenstelsel een risicoanalyse uit. De risicoanalyse richt zich op informatieveiligheidsrisico's. Dit zijn risico's die kunnen leiden tot inbreuken op de beschikbaarheid, integriteit of vertrouwelijkheid van informatie. Compliance aan wet- en regelgeving is geen onderdeel van deze risicoanalyse (bijv. compliance m.b.t. NEN7512). Het betreft hier een risicoanalyse op stelselniveau, dat wil zeggen dat het de risico's betreft in de onderlinge relatie tussen de betrokken partijen en niet de specifieke analyse bij een betrokken partij. Het onderwerp van de risicoanalyse betreft daarmee wel alle onderdelen van het MedMij Afsprakenstelsel. Dit houdt in dat de maatregelen voortkomend uit de analyse betrekking (kunnen) hebben op de Dienstverlener persoon, Dienstverlener aanbieder en Stichting MedMij. Personen en Aanbieders (de gebruikers) zijn geen onderdeel van het afsprakenstelsel en vallen buiten de scope van de risicoanalyse. Er kunnen wel maatregelen voor de risico's worden voorgesteld aan de Dienstverlener persoon of de Dienstverlener aanbieder die van invloed kunnen zijn op de Persoon of Aanbieder.

De risicoanalyse wordt, op grond van het Informatieclassificatiebeleid, niet publiekelijk beschikbaar gesteld.

Uitgangspunten bij de risicoanalyse

1. De scope van de risicoanalyse wordt voor het belangrijkste gedeelte bepaald door de Grondslagen, met name in de Criteria en de Principes. Op basis hiervan worden uitspraken gedaan over beschikbaarheid, vertrouwelijkheid en integriteit van de informatie binnen scope van het afsprakenstelsel;
2. De risicoanalyse wordt uitgevoerd op basis van de ten tijde van uitvoering laatst gepubliceerde release van het MedMij Afsprakenstelsel. Nieuwe of aangepaste maatregelen worden meegenomen in een nieuwe release van het afsprakenstelsel;
3. In de analyse is een vertegenwoordiging van alle rollen in het afsprakenstelsel en de governance betrokken;
4. Voldoen aan geldende wet- en regelgeving is een startpunt voor alle partijen en een vereiste in de definitie van maatregelen;
5. Het bestuur van Stichting MedMij streeft naar een voor de betrokken partijen aanvaardbaar risiconiveau aan de hand van de impact op de volgende onderwerpen: gezondheid, privacy, financieel, imago en vertrouwen. Stichting MedMij bepaalt met betrokken wat dit aanvaardbare risiconiveau is. De risicoanalyse, de risicotolerantie en beveiligingsmaatregelen worden vastgesteld door Stichting MedMij.

Maatregelen

De risicoanalyse leidt tot het formuleren van drie typen maatregelen:

1. Maatregelen die direct betrekking hebben op risico's voor de werking en veiligheid van het stelsel en daarom uniform dienen te worden vastgesteld (bijv. onderlinge autorisatieprocollen);
2. Maatregelen voor risico's die kunnen leiden tot stelselrisico's (een gebeurtenis bij een deelnemer die schade toebrengt aan andere deelnemers of Stichting MedMij). Deze zijn gespecificeerd in het stelsel om eenduidige interpretatie af te dwingen (bijv. toegang tot persoonlijke gezondheidsgegevens);
3. Maatregelen die vanuit efficiëntieoogpunt zijn opgenomen in het stelsel zodat niet iedere partij deze afzonderlijk hoeft te definiëren.

De geformuleerde maatregelen kunnen op verschillende manieren worden opgenomen in het afsprakenstelsel. Er kunnen technische specificaties worden geformuleerd voor deelnemers, Beleid en Operationele processen worden vormgegeven, dan wel normen in het Normenkader informatiebeveiliging worden opgenomen.

Verwerking in de afsprakenset

Uit de overkoepelende risicoanalyse op het afsprakenstelsel die is uitgevoerd op release 1.0, is geconcludeerd dat een NEN 7510-certificering voor deelnemers en beheerorganisatie in samenhang met de overige onderdelen van het toetredingsproces, zoals kwalificatie en acceptatie, de belangrijkste informatiebeveiligingsrisico's voor het stelsel afdekt. Op een aantal onderwerpen zijn maatregelen uit de NEN 7510-norm meer specifiek ingevuld voor MedMij of zijn er aanvullende maatregelen voorgesteld. Het betreft onderwerpen waarbij is geconcludeerd dat een ingeschat risico het beste afgedekt kan worden door voor alle partijen een uniforme maatregel te treffen, in plaats van zelfstandig maatregelen te kiezen op basis van een eigen risico inschatting. Of het gaat om onderwerpen waarbij de individuele inschatting gevolgen kan hebben voor andere partijen in het netwerk. Deze maatregelen zijn opgenomen in het Normenkader informatiebeveiliging. Daarnaast zijn maatregelen uit de risicoanalyse op stelselniveau opgenomen in de architectuur en technische specificaties of het beleid en operationele processen. De uitvoering van deze maatregelen wordt getoetst via onder andere het toetredingsproces.

NEN 7510-certificering is gangbaar en wettelijk verplicht bij de gegevensuitwisseling in het aanbiedersdomein. Om voor de uitwisseling met dienstverleners in het persoonsdomein zoveel mogelijk aan te sluiten bij de bestaande gebruiken en certificeringen, is gekozen de NEN 7510 ook verplicht te stellen voor de Dienstverlener persoon. De NEN 7510 kent het vertrouwen van partijen in het aanbiedersdomein en draagt zo bij aan de acceptatie van het stelsel. Het bezitten van een ISO 27001-certificering, de internationale standaard waarop de NEN 7510 is gebaseerd, is voor deelname aan het MedMij Afsprakenstelsel onvoldoende.

Herijking risicoanalyse

De risicoanalyse is een product dat jaarlijks dient te worden herijkt, maar ook wanneer er bepaalde wijzingen plaatsvinden. De risicoanalyse dient te worden herijkt op het moment dat:

- wijzigingen in het afsprakenstelsel worden gemaakt die van invloed kunnen zijn op de risicoanalyse;
- wanneer zich incidenten met aanzienlijke impact hebben voorgedaan;
- er bekende wijzigingen zijn in het dreigingslandschap voor MedMij;
- er significante technische wijzigingen zijn in de werking van het stelsel;
- er wijziging is van wetgeving waar MedMij aan moet voldoen;
- een van de uitgangspunten (zie hieronder) wordt gewijzigd.

Samenwerkings- en escalatiebeleid

Deelnemers vormen met elkaar het MedMij-netwerk. Om een optimale beschikbaarheid van dit netwerk te kunnen waarborgen, zijn deelnemers van elkaar afhankelijk. Van deelnemers wordt daarom verwacht dat zij onderling samenwerken.

Om deze samenwerking te faciliteren, vullen deelnemers en Stichting MedMij (voor de dienst MedMij Registratie) de volgende rollen in:

- Een servicemanager als eindverantwoordelijke voor de dienstverlening voor MedMij;
- Een servicedesk bestaande uit minimaal één persoon als dagelijks aanspreekpunt voor de beheerorganisatie en andere deelnemers.

Om daarnaast te voorkomen dat vragen van gebruikers onnodig bij andere deelnemers, Stichting MedMij of aanbieders terecht komen, dienen deelnemers ook de volgende rol in te vullen:

- Een gebruikers-helpdesk bestaande uit minimaal één persoon als dagelijks aanspreekpunt voor gebruikers.

Deelnemers maken bij Stichting MedMij kenbaar hoe de servicedesk, de servicemanager en de gebruikers-helpdesk te bereiken zijn. Deelnemers en Stichting MedMij registreren en publiceren deze contactgegevens, voor de eerste maal tijdens het toetredingsproces, in een online samenwerkingsplatform.

Servicedeskmedewerkers van de verschillende deelnemers mogen in de dagelijkse operatie een beroep op elkaar doen. Korte lijnen moeten ervoor zorgen dat verstoringen en/of problemen bij de dienstverlening van een deelnemer of bij de dienst MedMij Registratie zo snel mogelijk bij de servicedesk van de betreffende partij bekend zijn en de dienstverlening zo spoedig mogelijk kan worden hersteld.

Mochten er problemen ontstaan in de onderlinge samenwerking, dan kunnen servicedesksmedewerkers escaleren naar hun eigen servicemanager. Deze servicemanager bemiddelt vervolgens met de overige betrokken servicemanagers. Samen beslissen zij hoe de escalatie opgeheven wordt en de normale procesgang wordt hervat.

Indien de servicemanagers er onderling niet uitkomen, dan biedt Stichting MedMij het escalatiekanaal. Namens en samen met de escalerende partijen zal zij bemiddelen om een oplossing te vinden en tijdelijk toezien op de procesgang (totdat het normale proces kan worden hervat). Mocht ook deze bemiddeling niet slagen, dan beschrijft het Klachten- en geschillenbeleid de escalatieroutes buiten het stelsel.

Testbeleid

Om de interoperabiliteit en het vertrouwen in het stelsel te borgen, dienen deelnemers aan te tonen de Architectuur en technische specificaties en de *Gegevensdiensten* die zij ontsluiten op de juiste manier te ondersteunen. De deelnemer doorloopt bij toetreding en tijdens deelname testen. De testen bepalen of de deelnemer voldoende geëquipeerd is om de afspraken uit de architectuur en technische specificaties waar te maken en de gegevensdiensten op de juiste manier te gebruiken. Stichting MedMij toetst niet de volledige implementatie, maar richt zich op risico's, interoperabiliteit tussen deelnemers en cruciale maatregelen voor het vertrouwen in MedMij.

De testresultaten hebben een beperkte geldigheidsduur van 365 dagen vanaf het positief doorlopen van de test. Uitzondering daarop zijn de testresultaten met betrekking tot de ondersteuning van *Systeemrollen,* deze hebben een onbeperkte geldigheid.

Toelichting

Gedurende de geldigheid van een *Gegevensdienst* is een *Deelnemer* ervoor verantwoordelijk de *Systeemrollen* correct te ondersteunen conform de daarbij behorende specificaties (conform verantwoordelijkheid 2 op de Applicatielaag). Sommige *Kwalificatieloketten* bieden een externe toets op de correcte implementatie van de *Systeemrollen* indien een deelnemer dit wenst:

- na een wijziging in zijn applicatie (voor *Dienstverleners Persoon* of *Dienstverleners Zorgaanbieder*),
- in een achterliggend bronsysteem (voor *Dienstverleners Zorgaanbieder*),
- en/of combinatie van applicatie met achterliggend bronsysteem (voor *Dienstverleners Zorgaanbieder*).

Bij het aanvragen en inplannen van de hernieuwde test stelt de *Deelnemer* in overleg met de beheerorganisatie vast tegen welke actieve versie van het MedMij Afsprakenstelsel de test zal worden uitgevoerd (zie Change- en releasebeleid).

Wanneer moet er getest worden? We onderscheiden de volgende situaties:

1. De *Deelnemer* wil erkend worden als ontsluiter van een *Gegevensdienst*;
2. Hertest op initiatief van de *Deelnemer*, omdat de geldigheidsduur van diens testresultaten dreigt te verlopen.
3. Twijfel over de naleving van de afspraken;
4. Hertoetreding als bedoeld in artikel 14.3 van de Deelnemersovereenkomst.

Situatie 1: De deelnemer wil erkend worden als ontsluiter van een gegevensdienst

In situatie 1 moet op grond van het Gegevensdienstenbeleid worden aangetoond dat: (A) de relevante usecases uit de Architectuur en technische specificaties, (B) de algemene verantwoordelijkheden uit de Architectuur en technische specificaties en (C) de systeemrollen uit de *Gegevensdienst* goed worden ondersteund.

Voor (A) geldt het volgende schema:

Scope van de test (relevante usecases)

Usecase(s) behorende bij de *Gegevensdienst*	*Dienstverlener persoon*	*Dienstverlener aanbieder*
Verzamelen	Verzamelen Opvragen Aanbiederslijst Opvragen Gegevensdienstnamenlijst	Verzamelen Opvragen OAuth Client List Opvragen Gegevensdienstnamenlijst
Delen	Delen Opvragen Aanbiederslijst Opvragen Gegevensdienstnamenlijst	Delen Opvragen OAuth Client List Opvragen Gegevensdienstnamenlijst
Abonneren	Abonneren Notificeren	Abonneren Notificeren

De functies moeten worden beschouwd inclusief de bijbehorende verantwoordelijkheden en de formele regels in de relevante Informatiemodellen.

Onder (B) wordt verstaan: de verantwoordelijkheden, inclusief de functie Opvragen Whitelist.

Voor (C) geldt dat in de Catalogus te vinden is waar de ondersteuning van de *Systeemrollen* behorend bij een *Gegevensdienst* kan worden aangetoond. De test op de *Systeemrollen* vindt plaats in een opstelling die afwijkt van de productiesituatie. Het streven is om de toets in deze opstelling met zo min mogelijk aanvullende inspanningen van de deelnemer te kunnen doen. Aanvullende technische inspanning blijft echter nodig. Deelnemers committeren zich via hun deelname aan het afsprakenstelsel aan deze inspanningen. Informatie over kwalificatie kan worden gevonden bij de beheerder van de betreffende informatiestandaard.

De deelnemer kan zich voorbereiden op testen (A) en (B) in een testomgeving aangeboden door Stichting MedMij. Voor test (C) kan de deelnemer zich voorbereiden in de testomgeving van de partij die deze toets verzorgt. Voor (A) en (B) geldt verder dat eerdere positieve testen voor een functie of de algemene verantwoordelijkheden niet opnieuw behoeven te worden uitgevoerd als de deelnemer erkend wil worden als ontsluiter van een nieuwe gegevensdienst.

Situatie 2

De beperking van de geldigheidsduur van de testresultaten wordt begrepen als onderdeel van het Nalevingsbeleid. Wanneer de geldigheid van de testresultaten verloopt, dreigt opschorting van de Deelnemersovereenkomst, in het kader van artikel 7, lid 3. Het verlopen van de testresultaten wordt gezien als één van de wijzen waarop niet-naleving geconstateerd wordt.

Deelnemers zijn zelf verantwoordelijk voor het laten plannen van de testen voor het herbevestigen van de geldigheid van hun implementatie, voordat de geldigheid van bestaande testresultaten verloopt. Daarbij stelt stelt de *Deelnemer* in overleg met de beheerorganisatie vast tegen welke actieve versie van het MedMij Afsprakenstelsel de test zal worden uitgevoerd (zie Change- en releasebeleid).

Bij het succesvol doorlopen van de hertest zijn de nieuwe testresultaten opnieuw 365 dagen geldig.

Situatie 2

Het testbeleid wil eraan bijdragen dat *Deelnemers* een voorspelbare ontwikkelkalender voor hun implementatie kunnen hanteren, afgestemd op de regelmatige releasemomenten van het MedMij Afsprakenstelsel (zie Change- en releasebeleid) en de hertesten.

Her-acceptatie voor (A) en (B)

In Situatie 2 geldt voor het vaststellen van (A) de relevante usecases uit de Architectuur en technische specificaties en voor het vaststellen van (B) de algemene verantwoordelijkheden uit de Architectuur en technische specificaties, dat de her-acceptatietest is te beschouwen als een ‘apk’ voor MedMij *deelnemers*. Doel is om vast te stellen of de implementatie van de *deelnemer* voldoet aan de eisen van één van de actieve versies van het Afsprakenstelsel, de (her-)bevestiging van een implementatie op (A) en (B). (Zie Change- en releasebeleid voor uitleg over de versies van het Afsprakenstelsel.)

In overleg tussen *deelnemer* en de *beheerorganisatie* wordt bepaald of de test tegen de geldige laatst gepubliceerde of de verplichte versie van het Afsprakenstelsel wordt uitgevoerd. Doordat de her-acceptatie testen is los gekoppeld van toetreding en van de uitrol van releases van het Afsprakenstelsel, kunnen *deelnemer* zelf hun ontwikkeltempo en moment van uitrol van een koppelvlak versie bepalen.

Situaties 3 en 4

In situaties 3 en 4 wordt per geval bekeken wat er opnieuw getest moet worden. De geldigheid van eerdere positieve testresultaten kunnen in deze situaties vervallen.

Aanbiedersnamenbeleid

Aanbieders kunnen hun deelname en de manier waarop ze via MedMij te bereiken zijn aan *Personen* kenbaar maken via een *Aanbiedersnaam* (`aanbiedersnaam@medmij`). Het aanbiedersnamenbeleid beschrijft hoe een *Aanbieder* een voor de *Persoon* herkenbare naam kan kiezen, zonder in de toekomst de mogelijkheden van andere *Aanbieders* om een herkenbare naam te kiezen te veel te beperken.

Het is de *Aanbieder* die zijn *Aanbiedersnaam* kiest, maar de *Dienstverlener aanbieder* die de *aanbiedersnaam* aanreikt aan de MedMij Beheerorganisatie voor gebruik in de *Aanbiederslijst*. Daarbij moet de *Dienstverlener aanbieder* een verklaring van de *Aanbieder* kunnen overleggen. Deze verklaring is opgenomen onder het Registratieproces *Aanbiederslijst* op de pagina Operationele processen.

Rollen inzake de *Aanbiedersnaam*

De *Aanbiedersnaam*:

- wordt gekozen door de *Aanbieder*, als verwerkingsverantwoordelijke, voor het specifieke doel om *Gegevensdiensten* aan te bieden over het MedMij-netwerk;
- wordt vastgesteld door de Stichting MedMij, die daartoe onderstaande kwaliteitseisen verifieert;
- wordt door MedMij niet gebonden aan enige *Gegevensdienst*, maar het is betreffende *Aanbieder* gegeven dat wel te doen;
- is niet gebonden aan de *Dienstverlener aanbieder*. De *Dienstverlener aanbieder* informeert *Aanbieders* wel over de context, het doel en het beleid inzake *Aanbiedersnamen* in MedMij;
- wordt door een *Dienstverlener aanbieder* verwerkt en, in het bijzonder, gehanteerd wanneer hij in opdracht van een *Aanbieder* een *Gegevensdienst* wil laten opnemen op, of afvoeren van, de *Aanbiederslijst*;
- wordt op het MedMij-netwerk niet verbonden aan enig ander kenmerk, adres of identificatie van de *Aanbieder*. De verantwoordelijkheid voor zijn portfolio aan adressen (voor verschillende communicatiekanalen) en identificaties (voor verschillende doelen) ligt bij de *Aanbieder* zelf.

Eisen aan de *Aanbiedersnaam*

1. De naam moet gekoppeld zijn aan de naam die de Aanbieder in andere communicatie gebruikt (niet: `stichtingtersamenwerkinghuisartsenoegstgeest@medmij`, wel: `huisartsensamenwerkingoegstgeest@medmij`);
2. De naam mag niet al voorkomen of sterk lijken op een naam die al geregistreerd is;
3. De naam mag niet ambigu zijn en op veel verschillende aanbieders kunnen slaan (niet: `huisartshaarlem@medmij`, wel: `huisartswestergrachthaarlem@medmij`);
4. De naam mag niet de naam van een deelnemer bevatten of anderszins aan een specifieke deelnemer gekoppeld zijn;
5. De naam eindigt altijd op `@medmij`;
6. De naam is minimaal drie en maximaal 280 karakters lang (exclusief `@medmij`);
7. De naam wordt geregistreerd (ook in de *Aanbiederslijst*) in het volgende formaat:
    a. een reeks van één of meer segmenten, gescheiden door
        i. hetzij één koppelteken,
        ii. hetzij één ampersand,
        iii. hetzij één punt;
    b. gevolgd door `@medmij`, waarin
    c. elk segment een reeks van één of meer fragmenten is, zodanig dat
    d. elk fragment bestaat uit een reeks, met een minimale lengte van één karakter, van
        i. kleine letters uit het Nederlandse alfabet (bestaande uit de zesentwintig letters `a..z`) en /of
        ii. Arabische cijfers (`0..9`).

8. Van de naam mogen, buiten de registratie, varianten voorkomen waarin een kleine letter is vervangen door de corresponderende hoofdletter en/of diakritische varianten van letters voorkomen. Deze lettervarianten worden echter als identiek gezien aan de kleine basisletter. De naam is dus niet hoofdletter-gevoelig en evenmin diacriet-gevoelig.
9. De naam mag niet te herleiden zijn tot een persoon;
10. De naam mag in het verleden niet door een andere zorgaanbieder gebruikt zijn;
11. De naam mag het merk MedMij niet negatief beïnvloeden.

Het formaat van de Zorgaanbiedernaam

Het formaat van de *Aanbiedersnaam* benadert dat van de handelsnaam uit het Handels-register. Dat is nastrevenswaardig omdat doel en aard van de *Aan-bie-dersnaam* lijken op die van de handelsnaam.

Met betrekking tot de diakritische tekens is niet zozeer het voorkomen ervan een probleem, maar wel het onderscheidend vermogen tussen verschillende accenten op, aan of onder dezelfde basisletter. Het is geautomatiseerde systemen weliswaar gegeven om `woltgens` van `wöltgens` te onderscheiden, `mondhygiënist` van `mondhygienist` en `hélene` van `helène`, maar dat geldt niet voor (vooral PGO-)gebruikers die *Aanbiedersnamen* handmatig zullen willen intypen. Dat laatste moet mogelijk zijn, omdat een arts bijvoorbeeld op een kaartje of een kladje zijn *Aanbiedersnaam* aan een patiënt zou kunnen meege-ven. In die zin lijkt een *Aanbiedersnaam* op een e-mailadres. Een snel gemaakte fout met een diakritisch teken moet niet even snel tot de adressering van een onbedoelde *Aanbieder* leiden.

Met betrekking tot cijfers is het om vergelijkbare redenen zaak te voorkomen dat te lange reek-sen (volg)nummers ontstaan. Daarom mogen er maximaal vier achtereenvolgende cijfers voorkomen.

Het koppelteken, de ampersand en de punt kunnen een belangrijke functie vervullen in de herken-baar-heid van de *Aanbiedersnaam*, maar een reeks van dergelijke tekens achter elkaar amper.

Aanbiedersnamen worden dus in kleine letters en zonder diakritische tekens geregistreerd en in de *Aanbiederslijst* opgenomen, maar mogen in wíLlëKrîgE diakri-tische en hoofdlettervarianten worden aangegeven.

Zie voor de reguliere expressie van de basisklasse *Aanbiedersnaam* de pagina over de XML-schema's.

Operationele processen

Doel

Naast de usecases, zijn ook een aantal operationele processen in het afsprakenstelsel opgenomen. Deze processen spelen niet direct een rol in de gegevensuitwisseling, maar zijn wel nodig voor een goede operationele werking van het stelsel. Operationele processen geeft op hoofdlijnen een overzicht van de belangrijkste beheerprocessen waarbij deelnemers een rol spelen. Het overzicht is niet uitputtend. Detailuitwerkingen van deze processen zijn beschikbaar voor (potentiële) deelnemers.

Incidenten- en calamiteitenproces

- **Doel:** Het incidenten- en calamiteitenproces heeft als doel MedMij-gerelateerde incidenten en calamiteiten op gestructureerde wijze af te handelen. Daarbij dient de dienstverlening zo min mogelijk te worden verstoord.
- **Initiatie:** Deelnemer en/of Stichting MedMij constateert een incident/calamiteit.
- **Afspraken over het proces:**
  - In de nadere uitwerking van het proces wordt gedefinieerd wat een incident en calamiteit is in het kader van MedMij. De procesafspraken hebben hier betrekking op.
  - Deelnemers en Stichting MedMij zijn verplicht elkaar te informeren over alle incidenten en calamiteiten die de operationele werking van het netwerk beïnvloeden (Deelnemersovereenkomsten, artikel 5: privacy en (informatie)beveiliging).
  - Deelnemers en Stichting MedMij dienen zo spoedig mogelijk de benodigde acties uit te zetten om een incident of calamiteit op te lossen.
  - Stichting MedMij kan bij calamiteiten besluiten een operationeel team samen te stellen en de deelnemer vragen onderdeel te worden van dit team. Deelnemers dienen hieraan mee te werken.
  - Deelnemers en Stichting MedMij hebben allen één persoon binnen de eigen organisatie aangewezen als eindverantwoordelijke en centraal contactpersoon voor informatiebeveiligingsincidenten en -calamiteiten (zie A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging).
  - Communicatie van de deelnemer over incidenten en calamiteiten in het kader van MedMij worden afgestemd met Stichting MedMij (waar dit niet de wettelijke verplichting betreft).
- **Resultaat:** Incident en/of calamiteit is opgelost door de betrokkenen.
- **Uitzonderingen:** -

Proces beheren technische kwetsbaarheden

- **Doel:** Het proces beheren technische kwetsbaarheden heeft als doel om kwetsbaarheden in het stelsel tijdig te identificeren en op te lossen.
- **Initiatie:** *Deelnemer* en/of Stichting MedMij constateert een kwetsbaarheid.
- **Afspraken over het proces:**
  - *Deelnemers* en Stichting MedMij zijn verplicht elkaar te informeren over voor MedMij relevante kwetsbaarheden.
  - Stichting MedMij draagt zorg voor een centraal proces voor het signaleren en delen van kwetsbaarheden. In het proces zijn termijnen verbonden aan het oplossen van de kwetsbaarheden.
  - Uitwisseling van informatie over kwetsbaarheden vindt plaats met extra bescherming (zie Informatieclassificatiebeleid).
  - *Deelnemers* dienen in staat te zijn tijdig te reageren op meldingen van kwetsbaarheden in het MedMij Afsprakenstelsel (A.12.6.1 Beheer van technische kwetsbaarheden).

- **Resultaat:** Kwetsbaarheid is onderzocht en, waar nodig, verholpen door de betrokkenen.
- **Uitzonderingen:** -

Proces erkenning van *Deelnemer* als ontsluiter van *Gegevensdienst*

- **Doel:** Het proces erkenning van *Deelnemer* als ontsluiter van *Gegevensdienst* heeft als doel te toetsen of de *Deelnemer* een *Gegevensdienst* op de juiste wijze ondersteunt.
- **Initiatie:** *Deelnemer* wil een *Gegevensdienst* ontsluiten.
- **Afspraken over het proces:**
  - *Deelnemer* levert bewijs aan voor het succesvol doorlopen van toetsing op de relevante *Systeemrollen* uit de bij de *Gegevensdienst* horende *Informatiestandaard* (zie Testbeleid en Catalogus).
  - Stichting MedMij bepaalt of aanvullende toetsing op functionaliteit uit de Architectuur en technische specificaties benodigd is. Indien het geval, dan dient de *Deelnemer* de ondersteuning van de aanvullende functionaliteit middels een toets te laten zien (zie Testbeleid).
  - Stichting MedMij bepaalt of *Deelnemer* eerst erkend moet worden als ontsluiter van andere *Gegevensdiensten,* omdat de *Gegevensdienst* dit vereist (zie Gegevensdienstenbeleid). Indien het geval, dan dient eerst de erkenning als ontsluiter van de vereiste *Gegevensdienst* behaald te worden.
- **Resultaat:** *Deelnemer* is erkend als ontsluiter van een *Gegevensdienst.* Stichting MedMij initieert het Registratieproces ontsluiting *Gegevensdiensten* door deelnemer.
- **Uitzonderingen:** *Deelnemer* voldoet niet aan de vereisten voor de *Gegevensdienst* en wordt niet erkend als ontsluiter.

Proces vernieuwing erkenning van *Deelnemer*

- **Doel:** Het proces vernieuwing erkenning van *Deelnemer* heeft als doel om periodiek te herbevestigen dat de implementatie van een *Deelnemer* nog steeds aan het MedMij Afsprakenstelsel voldoet.
- **Initiatie:**
  - De geldigheidsduur van de testresultaten van een *Deelnemer* dreigt te verlopen.
  - *Deelnemer* draagt een entry aan voor opname op de *OAuthClientList* of *Aanbiederslijst* in relatie waarmee *Deelnemer* nog niet (geheel) erkend is.
- **Afspraken over het proces:**
  - Stichting MedMij bepaalt, in overleg met *Deelnemer*, op welke onderdelen van het MedMij Afsprakenstelsel *Deelnemer* een hernieuwde test moet ondergaan. Het doel daarbij is om *Deelnemer* ten minste te laten voldoen daan de verplichte (zie Change- en releasebeleid) release van het MedMij Afsprakenstelsel.
  - Wanneer *Deelnemer* de hertest met goed gevolg doorstaat, zijn de testresultaten opnieuw 365 dagen geldig.
  - Wanneer *Deelnemer* de hertest niet doorstaat, bepaalt Stichting MedMij of daarom ontbinding of opschorting van de *Deelnemersovereenkomst* aan de orde is.
  - Stichting MedMij is verantwoordelijk voor het doorvoeren van de benodigde mutaties in het deelnemersregister, naar aanleiding van de resultaten van de hertest.
- **Afspraken over het proces:** Voorzover *Deelnemer* voldoet aan het MedMij Afsprakenstelsel, is diens deelname voor de komende 365 dagen bestendigd.
- **Uitzonderingen:** -

Registratieproces ontsluiting *Gegevensdiensten* door *Deelnemer*

- **Doel:** Het registratieproces ontsluiting *Gegevensdiensten* door *Deelnemer* heeft als doel de juiste informatie vast te leggen over de ontsluiting van *Gegevensdiensten* door de *Deelnemer.*
- **Initiatie:**
  - *Deelnemer* is erkend voor een *Gegevensdienst* en mag deze aanbieden.

- *Deelnemer* wil een *Gegevensdienst* niet meer ontsluiten.
- *Deelnemer* mag een *Gegevensdienst* niet meer ontsluiten op grond van falende herkwalificatie of -acceptatie.

- **Afspraken over het proces:**
  - Stichting MedMij is verantwoordelijk voor het doorvoeren van de benodigde mutaties in het deelnemersregister.
  - Mutaties zijn gebonden aan de verantwoordelijkheden en regels zoals gespecificeerd in de Architectuur en technische specificaties.
- **Resultaat:** Stichting MedMij heeft het deelnemersregister en de overige relevante lijsten aangepast. De *Deelnemer* wordt geïnformeerd over de doorgevoerde wijziging.
- **Uitzonderingen:** -

Registratieprocessen *Aanbiederslijst*, *Whitelist* en *OAuthclientlist*

- **Doel:** De registratieprocessen voor de *Aanbiederslijst*, *Whitelist* en *OAuthclientlist* hebben als doel de juiste informatie te verzamelen benodigd voor een goede operationele werking van het stelsel.
- **Initiatie:**
  - Deelnemer dient een verzoek in bij Stichting MedMij om een entry in de Aanbiederslijst, Whitelist of OAuthclientlist aan te maken, te wijzigen of te verwijderen.
  - Triggers voor wijzigingen zijn per lijst verschillend:
    - *Whitelist*:
      - *Deelnemer* wil een node op het MedMij-netwerk gebruiken.
      - *Deelnemer* wil een van haar eigen nodes niet meer op het MedMij-netwerk gebruiken.
    - *Aanbiederslijst en Aanbiederskoppellijst*:
      - *Dienstverlener aanbieder* wil in het MedMij-netwerk kenbaar maken een *Gegevensdienst* namens een *Aanbieder* te ontsluiten.
      - *Dienstverlener aanbieder* wil in het MedMij-netwerk kenbaar maken een *Gegevensdienst* namens een *Aanbieder* niet meer te ontsluiten.
    - *Alleen Aanbiederslijst*:
      - *Dienstverlener aanbieder* wil een of meerdere endpoints bij een *AanbiederGegevensdienst* wijzigen.
    - *OAuthclientlist*:
      - *Dienstverlener persoon* wil een *OAuthclient* toevoegen.
      - *Dienstverlener persoon* wil een *OAuthclient* verwijderen.
- **Afspraken over het proces:**
  - *Deelnemer* is verantwoordelijk voor het aanleveren van mutaties voor de *Aanbiederslijst*, *WhiteList* en *OAuthclientlist*.
  - Bij het kenbaar maken van het ontsluiten van een *Gegevensdienst* voor een *Aanbieder* overlegt de *Dienstverlener aanbieder* de volgende verklaring van de *Aanbieder*:
    "Ik, [*Aanbieder*], verklaar onder de *Aanbiedersnaam* [*Aanbiedersnaam*] één of meerdere *Gegevensdiensten* aan te willen bieden op het MedMij-netwerk, vanaf [*ingangsdatum*] en deze te laten ontsluiten door [*Dienstverlener aanbieder*]. Tevens geef ik stichting MedMij toestemming de Gegevensdiensten die op enig moment onder *Aanbiedersnaam* [*Aanbiedersnaam*] worden aangeboden openbaar te publiceren."
  - Mutaties zijn gebonden aan de verantwoordelijkheden en regels zoals gespecificeerd in de Architectuur en technische specificaties, het Aanbiedersnamenbeleid en OAuthclient-namenbeleid.
  - Stichting MedMij neemt het verzoek in behandeling en is verantwoordelijk voor een check op integriteit.
  - Valide mutaties worden in 95 procent van de gevallen door Stichting MedMij binnen 2 werkdagen verwerkt. Urgente mutaties krijgen daarbij voorrang. De mutatietijd voor urgente mutaties wordt in overleg met Stichting MedMij bepaald. Bij verwachte overschrijding van de (overeengekomen) verwerkingstijd, informeert Stichting MedMij de deelnemer hierover.

- **Resultaat:** Stichting MedMij heeft het betreffende register aangepast. De deelnemer wordt geïnformeerd over de doorgevoerde wijziging.
- **Uitzonderingen:** Een van de verantwoordelijkheden en regels in de Architectuur en technische specificaties wordt overtreden. Stichting MedMij vraagt de deelnemer om het verzoek aan te passen.

Actualiseren van *Aanbiederslijst, Aanbiederkoppellijst* en de *OauthClientList* bij publicatie nieuwe release

- **Doel:** Borgen dat in de *Aanbiederslijst, de Aanbiederkoppellijst* en de *OAuthclientlist* alleen *Interfaceversies* voorkomen van actieve releases van het MedMij Afsprakenstelsel.
- **Initiatie:**
  - Er komt een nieuwe release uit van het MedMij Afsprakenstelsel. Dat wil zeggen dat de tot dan toe verplichte release de status *verouderd* krijg.
- **Afspraken over het proces:**
  - *MedMij Beheer* is verantwoordelijk voor het verwijderen van alle entries in de *Aanbiederslijst, Aanbiederkoppellijst* en de *OAuthClientList* die horen bij een (zojuist) verouderde *Interfaceversie*.
- **Resultaat:** Stichting MedMij heeft de betreffende lijsten aangepast.
- **Uitzonderingen:** Geen.

Managementinformatieproces

- **Doel:** Het managementinformatieproces heeft als doel de verschillende stakeholders van informatie te voorzien over het gebruik van MedMij.
- **Initiatie:** Proces wordt geïnitieerd door de klok.
- **Afspraken over het proces:**
  - *Deelnemers* zijn verantwoordelijk voor het aanleveren van Managementinformatie.
  - Stichting MedMij zorgt voor de verwerking van de gegevens tot een geaggregeerde rapportage. Concurrentiegevoelige informatie wordt hierbij zoveel mogelijk verborgen.
- **Resultaat:** Een geaggregeerde rapportage voor de betrokkenen.
- **Uitzonderingen:** *Deelnemer* levert de benodigde managementinformatie niet aan. Stichting MedMij verzoekt de *Deelnemer* alsnog de benodigde informatie aan te leveren. Mocht een *Deelnemer* (herhaaldelijk) in gebreke blijven, dan treedt het Nalevingsbeleid in werking.

Uittredingsproces

- **Doel:** Het uittredingsproces heeft als doel een deelnemer op gestructureerde wijze en met oog voor de belangen van de verschillende stakeholders uit te laten treden.
- **Initiatie:**
  - Deelnemer wil uittreden uit het afsprakenstelsel.
  - *Deelnemer* dient uit te treden uit het afsprakenstelsel.
- **Afspraken over het proces:**
  - De belangrijkste verwachtingen van *Deelnemers* bij uittreding staan beschreven in de Deelnemersovereenkomsten (Artikel 7: Opschorting en beëindiging).
  - Stichting MedMij voert de benodigde mutaties door in het deelnemersregister en de relevante lijsten.
- **Resultaat:** *Deelnemer* is uitgetreden uit het afsprakenstelsel.
- **Uitzonderingen:** -

Processen inzake gecontroleerde livegang

Start van een gecontroleerde livegang

- **Doel:** Het in de gelegenheid stellen van een groep *Deelnemers* tot het uitvoeren van een gecontroleerde livegang conform Beleid inzake gecontroleerde livegang.
- **Initiatie:** Minstens één *Aanbieder*, minstens één *Dienstverlener aanbieder* en minstens één *Dienstverlener persoon* willen samen een gecontroleerde livegang uitvoeren voor één *Gegevensdienst* . De bedoelde *Dienstverleners* moeten gekwalificeerd zijn voor die *Gegevensdienst*.
- **Afspraken over het proces:**
  - Gecontroleerde livegangen mogen alleen worden uitgevoerd op de dan verplichte release en bijbehorende *Interfaceversie*. Dit kan de looptijd van de gecontroleerde livegang beperken tot het eerstvolgende releasemoment van het MedMij Afsprakenstelsel.
  - De MedMij Beheerorganisatie creëert een kopie-*Gegevensdienst* van de beoogde *Gegevensdienst* en voegt deze toe aan de *Catalogus* met een geldigheidstermijn zoals gewenst door de betrokkenen, maar voldoend aan het Beleid inzake gecontroleerde livegang.
  - De MedMij Beheerorganisatie voegt de kopie-*Gegevensdienst* toe aan de *Gegevensdienstnamenlijst*, onder dezelfde *Weergavenaam* als de origineel-*Gegevensdienst*.
  - Voor elk van de betrokken *Aanbieders* en *Dienstverleners persoon* wordt het proces 'Toetreding tot een gecontroleerde livegang' uitgevoerd.
- **Resultaat:** De gecontroleerde livegang is operationeel, tenzij gedurende de uitvoering van het proces en zijn deelprocessen niet aan eisen blijkt te zijn voldaan.
- **Uitzonderingen:** -

Toetreding tot een gecontroleerde livegang

- **Doel:** Het in de gelegenheid stellen van een *Aanbieder* (desgewenst met diens *Dienstverlener aanbieder*) of *Dienstverlener persoon* toe te treden tot een bestaande gecontroleerde livegang conform Beleid inzake gecontroleerde livegang.
- **Initiatie:** Een *Aanbieder* (desgewenst met diens *Dienstverlener aanbieder*) of *Dienstverlener persoon* wenst toe te treden tot een gecontroleerde livegang. De betreffende *Dienstverlener* moet gekwalificeerd zijn voor de origineel-*Gegevensdienst* van de gecontroleerde livegang. De *Aanbieder* mag in de afgelopen drie maanden niet al betrokken zijn geweest bij een gecontroleerde livegang op deze origineel-*Gegevensdienst*.
- **Afspraken over het proces:**
  - De MedMij Beheerorganisatie erkent de betreffende *Dienstverlener* op de kopie-*Gegevensdienst*, indien deze is gekwalificeerd op de origineel-*Gegevensdienst*.
  - Betrokken *Dienstverlener* laat zich inzake de kopie-*Gegevensdienst* op gebruikelijke wijze registreren in de *Aanbiederslijst*, de *OAuth Client List* en de *Whitelist*.
- **Resultaat:** De betreffende partij is operationeel in de gecontroleerde livegang, tenzij niet aan de toepasselijke eisen is voldaan.
- **Uitzonderingen:** -

Uittreding uit een gecontroleerde livegang

- **Doel:** Het in de gelegenheid stellen van een *Aanbieder* (desgewenst met diens *Dienstverlener aanbieder*) of *Dienstverlener persoon* uit te treden uit een bestaande gecontroleerde livegang conform Beleid inzake gecontroleerde livegang.
- **Initiatie:** Een *Aanbieder* (desgewenst met diens *Dienstverlener aanbieder*) of *Dienstverlener persoon* wenst uit te treden uit een gecontroleerde livegang. Bij een Aanbieder kan dat gepaard gaan met een wens tot promotie tot het gewone live MedMij-netwerk.
- **Afspraken over het proces:**
  - De MedMij Beheerorganisatie beëindigt de erkenning van betreffende *Dienstverlener* op de kopie-*Gegevensdienst*.
  - De MedMij Beheerorganisatie verwijdert de op de betreffende partij betrekking hebbende elementen uit de *Aanbiederslijst*, de *OAuth Client List* en de *Whitelist*.
  - Indien het een *Aanbieder* betreft die wens te promoveren, start de MedMij Beheerorganisatie het proces 'Promotie uit een gecontroleerde livegang'.

- Mocht de uitreder de laatste *Aanbieder*, *Dienstverlener aanbieder* of *Dienstverlener persoon* zijn in de gecontroleerde livegang, start hij het proces 'Beëindiging van een gecontroleerde livegang'.
- **Resultaat:** De betreffende partij is niet meer operationeel in de gecontroleerde livegang.
- **Uitzonderingen:** -

Promotie uit een gecontroleerde livegang

- **Doel:** Het live gaan van een *Aanbieder*, met diens *Dienstverlener aanbieder*, in het MedMij-netwerk, vanuit een gecontroleerde livegang, conform Beleid inzake gecontroleerde livegang.
- **Initiatie:** Een *Aanbieder* (met diens *Dienstverlener aanbieder*) geven bij uitreding uit de gecontroleerde livegang aan te willen promoveren.
- **Afspraken over het proces:**
  - De MedMij Beheerorganisatie vervangt in de *Aanbiederslijst* die elementen die betrekking hebben op de betreffende *Aanbieder*-kopie-*Gegevensdienst*-combinaties de kopie-*Gegevensdienst* door de origineel-*Gegevensdienst*.
- **Resultaat:** De betreffende *Aanbieder* is live met de betreffende *Gegevensdienst*.
- **Uitzonderingen:** -

Beëindiging van een gecontroleerde livegang

- **Doel:** Het beëindigen van de gelegenheid van een groep *Deelnemers* tot het uitvoeren van een gecontroleerde livegang conform Beleid inzake gecontroleerde livegang.
- **Initiatie:** Wanneer één van de volgende gebeurtenissen zich voordoet:
  - de looptijd van de kopie-*Gegevensdienst* verstrijkt, al dan niet na een eenmalige verlenging;
  - de laatste *Aanbieder*, *Dienstverlener aanbieder* of *Dienstverlener persoon* treedt uit uit de gecontroleerde livegang;
  - Stichting MedMij oordeelt dat enige bij de gecontroleerde livegang betrokken partij voordelen ontleent of beoogt te ontlenen aan de gecontroleerde livegang die niet in overeenstemming zijn met de bedoeling van gecontroleerde livegangen.
- **Afspraken over het proces:**
  - De MedMij Beheerorganisatie beëindigt de geldigheid van de kopie-*Gegevensdienst*.
  - De MedMij Beheerorganisatie verwijdert de kopie-*Gegevensdienst* uit de *Gegevensdienstnamenlijst*. De kopie-*Gegevensdienst* wordt nooit meer opnieuw gebruikt.
  - De MedMij Beheerorganisatie verwijdert de erkenning van betrokken *Dienstverleners* op de kopie-*Gegevensdienst*.
  - De MedMij Beheerorganisatie verwijdert op betrokken kopie-*Gegevensdienst* betrekking hebbende elementen uit de *Aanbiederslijst* en de *OAuth Client List*.
  - Betrokken partijen verwijderen eventuele op hen betrekking hebbende elementen uit de *Whitelist,* voor zover zij die niet ook gebruiken buiten deze gecontroleerde livegang.
- **Resultaat:** De gecontroleerde livegang is niet meer operationeel.
- **Uitzonderingen:** -

Communicatie

Communicatie beschrijft de afspraken over het Merkgebruik en het hanteren van de verplichte Gebruikersvoorlichting, Toestemmingsverklaring en Bevestigingsverklaring.

Merkgebruik

Persoonlijke gezondheidsomgevingen en zorginformatiesystemen kennen vele vormen. De afsprakenset houdt rekening met deze diversiteit en maakt het mogelijk om met een relatief beperkte afsprakenset uitwisseling tussen deze systemen vorm te geven. MedMij heeft niet als doel om met de afsprakenset uniformiteit van deze systemen te realiseren. Integendeel zelfs, MedMij omarmt de diversiteit en gelooft dat alleen zo de verschillende gebruikers goed kunnen worden bediend.

Dit uitgangspunt heeft consequenties voor de betekenis van het merk. MedMij staat vooral symbool voor de veilige en betrouwbare gegevensuitwisseling van gezondheidsgegevens tussen deelnemers aan het stelsel. Het merk is geen keurmerk voor de volledige functionaliteit of dienstverlening van een PGO of aan een Aanbieder. Gebruikers in de verschillende domeinen weten door de toepassing van het merk dat ze de gegevensuitwisseling tussen deelnemers kunnen vertrouwen en dat gegevens op een plek terecht komen waar de privacy en informatiebeveiliging voldoende is gewaarborgd.

Het gebruik van het merk kent in praktijk drie doelen, namelijk:

1. Herkenbaarheid voor de persoon;
2. Profilering van de deelnemer (waaronder herkenbaarheid voor de Aanbieder);
3. Herkenbaarheid communicatie vanuit MedMij.

Het gebruik van het merk bij deze doelen wordt hieronder nader uitgewerkt.

Doel 1: Herkenbaarheid voor de persoon

Het merk MedMij speelt voor de persoon een belangrijke rol bij het herkennen van partijen waarmee gezondheidsgegevens op een veilige en betrouwbare wijze kunnen worden uitgewisseld. De persoon moet bijvoorbeeld een Dienstverlener persoon kunnen uitzoeken die aan de MedMij-afspraken voldoet en ook zijn /haar Aanbieder moet kunnen laten weten uitwisseling via MedMij te ondersteunen. Het merk MedMij mag dan ook voor dit doeleinde worden gebruikt door de Dienstverlener persoon en door Aanbieders (waarvoor Dienstverleners aanbieder AanbiederGegevensdiensten ontsluiten).

De Dienstverlener persoon mag zowel in de persoonlijke gezondheidsomgeving zelf als in de communicatie daaromheen het merk gebruiken. In het systeem moet in ieder geval voor de persoon zichtbaar zijn wanneer sprake is van gegevens(uitwisseling) via MedMij. Het merk moet daarom aan de eindgebruiker gepresenteerd worden bij:

- Het tonen van de mogelijkheid om gegevens uit te wisselen via MedMij;
- Het tonen van de gezondheidsgegevens verkregen via MedMij.

Het recht om als aangesloten Aanbieder het merk te mogen voeren, volgt niet uit de rechtsrelaties in het stelsel. Dit wordt daarom geregeld met een licentietekst op de MedMij-website.

Doel 2: Profilering van de deelnemer

Deelnemers mogen het merk hanteren om naar anderen te laten zien te voldoen aan de afspraken. Zo kan de Dienstverlener aanbieder bijvoorbeeld met het merk aan de Aanbieder kenbaar maken gegevensuitwisseling via MedMij aan te bieden.

Doel 3: Herkenbaarheid communicatie vanuit MedMij

De beheerorganisatie gebruikt het merk voor de herkenbaarheid van de eigen communicatie. Ook gebruikt zij het merk bij communicatieproducten waarvan zij uitgever is, zoals bij de gebruikersvoorlichting.

Uitingsvormen van het merk

Een consistente toepassing van het merk draagt bij aan de waarde hiervan. Deelnemers en Aanbieders mogen het merk uiten met het MedMij-label of met een tekstuele verwijzing naar MedMij. Er zijn twee versies van het MedMij-label:

In principe maken Deelnemers en Aanbieders gebruik van het MedMij-label met payoff. Mocht de payoff onleesbaar worden door het design, dan mag gebruik worden gemaakt van het MedMij-label zonder payoff.

Voor de herkenbaarheid van de communicatie vanuit MedMij, is verdergaand gebruik van de huisstijl in principe voorbehouden aan de beheerorganisatie. Dit geldt ook voor het MedMij-logo, zoals gebruikt door Stichting MedMij en de uitvoeringsorganisatie. Mocht een deelnemer communicatie nader willen laten aansluiten bij deze MedMij-huisstijl, dan vindt hierover altijd afstemming plaats met de beheerorganisatie. Geeft de beheerorganisatie toestemming voor verdergaand gebruik, dan is er een huisstijlhandleiding beschikbaar met daarin onder meer afspraken over kleurgebruik en opmaak.

Voor de waarde van het merk MedMij is het verder belangrijk dat partijen op een zelfde wijze communiceren over de boodschap van dit merk. Hiervoor zijn basistekstelementen beschikbaar bij de beheerorganisatie. Deze dienen ter inspiratie en mogen worden gebruikt in de eigen communicatie.

Gebruikersvoorlichting

De Gebruikersvoorlichting bevat antwoorden op een aantal veelgestelde vragen die belangrijk zijn voor het vertrouwen in MedMij. De gebruikersvoorlichting heeft als doel het vertrouwen van zowel personen als Aanbieders in de digitale gegevensuitwisseling via MedMij te vergroten. Richting de Persoon wordt de Gebruikersvoorlichting persoonsdomein en richting de Aanbieder de Gebruikersvoorlichting Aanbiedersdomein gehanteerd. Deelnemers aan het MedMij Afsprakenstelsel zijn middels de Deelnemersovereenkomsten verplicht om de MedMij-gebruikersvoorlichting aan hun gebruikers voor te leggen. Ook dienen zij bij nieuwe versies de gebruikersvoorlichting opnieuw aan hun gebruikers voor te leggen.

De gebruikersvoorlichting is vormgegeven in de MedMij-huisstijl en dient door deelnemers in deze vorm aan de gebruiker te worden voorgelegd. Het is toegestaan de gebruikersvoorlichting zowel in papieren als digitale vorm met de gebruiker te delen. De gebruikersvoorlichting moet tevens via de website van de deelnemer te vinden zijn door een link op te nemen naar de gebruikersvoorlichting op de MedMij-website. De bestanden met de gebruikersvoorlichting worden bij toetreding tot het stelsel en bij wijziging van de voorlichting met de deelnemer gedeeld.

Toestemmingsverklaring

> Toestemmingsverklaring is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moet deze pagina herzien worden. Er moet dan een generieke tekst geschreven worden, of per domein wordt een tekst opgesteld.

De toestemmingsverklaring en de toelichting daarop zijn verplichte teksten die de *Dienstverlener aanbieder* dient voor te leggen aan de *Persoon* bij het ophalen van gezondheidsgegevens bij de *Aanbieder*. Deze toestemmingsverklaring heeft betrekking op die gegevensuitwisseling. De verplichte toestemmingsverklaring volgt uit de Wet geneeskundige behandelingsovereenkomst (WGBO). De *Aanbieder* is verplicht ervoor te zorgen dat ‘anderen’ dan de patiënt geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van het medisch dossier, tenzij hiervoor toestemming is verleend. Binnen de MedMij afspraken verstrekt de *Zorgaanbieder* via de *Dienstverlener zorgaanbieder* gegevens aan de *Dienstverlener persoon*. Aangezien dit een 'andere' is dan de *Persoon* zelf, moet de *Zorgaanbieder* weten dat de persoon hiervoor toestemming heeft verleend. Bij de functies Verzamelen en de Abonneren staat beschreven hoe het proces rondom het geven van toestemming eruit ziet. De *Dienstverlener zorgaanbieder* implementeert de toestemmingsverklaring en toont deze aan de *Persoon*.

Toestemmingsverklaring

Ik wil persoons- en gezondheidsgegevens opnemen in mijn persoonlijke gezondheidsomgeving (PGO). Persoonsgegevens zijn bijvoorbeeld je naam en geboortedatum. Gezondheidsgegevens zijn de gegevens die een zorgaanbieder van je heeft opgeslagen. Bijvoorbeeld de medicijnen die je slikt, en bloeduitslagen.

Hierbij geef ik `NaamZorgaanbieder` toestemming om de gegevens die ik opvraag aan `NaamLeverancierPGO` te sturen.

De volgende gegevens wil ik opvragen en in mijn PGO opnemen:
- `NaamGegevensdienst`
- `NaamGegevensdienst`

Uitleg over de toestemmingsverklaring

Met een persoonlijke gezondheidsomgeving (PGO) kun je gegevens over je gezondheid verzamelen. Voor het uitwisselen van deze gegevens van jouw zorgaanbieder – zoals je huisartsenpraktijk – naar jouw PGO is een veilige verbinding nodig. In PGO’s met een MedMij-label kunnen deze gegevens veilig worden uitgewisseld. Hierover zijn afspraken gemaakt en vastgelegd in het MedMij Afsprakenstelsel. Het uitwisselen van gegevens tussen de zorgaanbieder en jouw PGO verloopt via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Wet geneeskundige behandelingsovereenkomst is de zorgaanbieder verplicht ervoor te zorgen dat ‘anderen’ (lees: jouw PGO) dan de patiënt (lees: jij) geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van jouw medische dossier, tenzij je hiervoor toestemming hebt gegeven.

Wil je bij jouw zorgaanbieder gegevens opvragen om in jouw PGO te zetten? Dan moet je de zorgaanbieder hier toestemming voor geven. Je geeft dan toestemming voor de specifieke gegevens die hij of zij mag uitwisselen. Niet voor andere gegevens.

De toestemmingsverklaring en de toelichting zijn onderdeel van onderstaand verplichte toestemmingsscherm. De *Dienstverlener zorgaanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid 1a op de pagina User interface (Autorisatieserver).

De *Dienstverlener zorgaanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de pagina.

Bijgesloten HTML- en CSS-bestanden zijn toegevoegd aan deze pagina als hulpmiddel bij de implementatie. Deze bestanden beschrijven de tekst en vormgeving van het scherm. Het is niet verplicht deze toe te passen.

Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de mogelijkheid om hier opnieuw in te loggen.

Optioneel:
Logo ZA

MedMij
veilig online uitwisselen van gezondheidsgegevens

Ik wil persoons- en gezondheidsgegevens opnemen in mijn persoonlijke gezondheidsomgeving (PGO). Persoonsgegevens zijn bijvoorbeeld je naam en geboortedatum. Gezondheidsgegevens zijn de gegevens die een zorgaanbieder van je heeft opgeslagen. Bijvoorbeeld de medicijnen die je slikt, en bloeduitslagen.

Hierbij geef ik **NaamZorgaanbieder** toestemming om de gegevens die ik opvraag aan **NaamLeverancierPGO** te sturen.

De volgende gegevens wil ik opvragen en in mijn PGO opnemen:

- **NaamGegevensdienst**
- **NaamGegevensdienst**

✓ Ja, ik geef toestemming

Nee, ik geef geen toestemming

Wanneer je een keuze hebt gemaakt of deze pagina sluit, dan word je uitgelogd bij **NaamZorgaanbieder**.

☐ Toon toelichting

MedMij
Grip op je eigen gezondheidsgegevens

Optioneel:
Logo ZA

MedMij
veilig online uitwisselen van gezondheidsgegevens

Ik wil persoons- en gezondheidsgegevens opnemen in mijn persoonlijke gezondheidsomgeving (PGO). Persoonsgegevens zijn bijvoorbeeld je naam en geboortedatum. Gezondheidsgegevens zijn de gegevens die een zorgaanbieder van je heeft opgeslagen. Bijvoorbeeld de medicijnen die je slikt, en bloeduitslagen.

Hierbij geef ik **NaamZorgaanbieder** toestemming om de gegevens die ik opvraag aan **NaamLeverancierPGO** te sturen.

De volgende gegevens wil ik opvragen en in mijn PGO opnemen:

- **NaamGegevensdienst**
- **NaamGegevensdienst**

✓ Ja, ik geef toestemming

Nee, ik geef geen toestemming

Wanneer je een keuze hebt gemaakt of deze pagina sluit, dan word je uitgelogd bij **NaamZorgaanbieder**.

☑ Toon toelichting

Met een persoonlijke gezondheidsomgeving (PGO) kun je gegevens over je gezondheid verzamelen. Voor het uitwisselen van deze gegevens van jouw zorgaanbieder - zoals je huisartsenpraktijk - naar jouw PGO is een veilige verbinding nodig. In PGO's met een MedMij-label kunnen deze gegevens veilig worden uitgewisseld. Hierover zijn afspraken gemaakt en vastgelegd in het MedMij Afsprakenstelsel. Het uitwisselen van gegevens tussen de zorgaanbieder en jouw PGO verloopt via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Wet geneeskundige behandelingsovereenkomst is de zorgaanbieder verplicht ervoor te zorgen

dat 'anderen' (lees: jouw PGO) dan de patiënt (lees: jij) geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van jouw medische dossier, tenzij je hiervoor toestemming hebt gegeven.

Wil je bij jouw zorgaanbieder gegevens opvragen om in jouw PGO te zetten? Dan moet je de zorgaanbieder hier toestemming voor geven. Je geeft dan toestemming voor de specifieke gegevens die hij of zij mag uitwisselen. Niet voor andere gegevens.

Toestemmingsverklaring Abonneren

> Toestemmingsverklaring Abonneren is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moet deze pagina herzien worden. Er moet dan een generieke tekst geschreven worden, of per domein wordt een tekst opgesteld.

Deze toestemmingsverklaring en de toelichting daarop zijn verplichte teksten die de *Dienstverlener zorgaanbieder* dient voor te leggen aan de *Persoon* bij het tot stand brengen van een *Abonnement* op gezondheidsgegevens (*Notificaties*) bij de *Zorgaanbieder*. Deze toestemmingsverklaring heeft betrekking op die gegevensuitwisseling. De verplichte toestemmingsverklaring volgt uit de Wet geneeskundige behandelingsovereenkomst (WGBO). De *Zorgaanbieder* is verplicht ervoor te zorgen dat ‘anderen’ dan de patiënt geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van het medisch dossier, tenzij hiervoor toestemming is verleend. Binnen het MedMij Afsprakenstelsel verstrekt de *Zorgaanbieder* door middel van de *Dienstverlener zorgaanbieder* gegevens aan de *Dienstverlener persoon*. Aangezien dit een 'andere' is dan de *Persoon* zelf, moet de *Zorgaanbieder* weten dat de persoon hiervoor toestemming heeft verleend. Bij de functie Abonneren staat beschreven hoe het proces rondom het geven van toestemming eruit ziet. De *Dienstverlener zorgaanbieder* implementeert de toestemmingsverklaring en toont deze aan de *Persoon*.

Toestemmingsverklaring

U geeft hierbij `NaamZorgaanbieder` toestemming om, gedurende ten hoogste `Duur` dagen, meldingen over `NaamGegevensdienst` te doen bij `NaamLeverancierPGO` voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.

De looptijd is mogelijk beperkt door `NaamZorgaanbieder`.

Toelichting op de toestemmingsverklaring

Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen de zorgaanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Wet geneeskundige behandelingsovereenkomst (WGBO) is de zorgaanbieder verplicht ervoor te zorgen dat ‘anderen’ dan de patiënt (lees: u) geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw medisch dossier, *tenzij u hiervoor toestemming heeft verleend*.

Aangezien uw PGO (en eventuele achterliggende partij die werkt volgens de MedMij-afspraken) een zogenaamde ‘andere’ is (in de zin van de WGBO) dient u de zorgaanbieder voor deze gegevensuitwisseling toestemming te verlenen. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door de zorgaanbieder - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

Op basis van uw toestemming moet uw PGO een verzoek doen bij de Zorgaanbieder voor het doen van meldingen over de betreffende gegevensdienst voor de gevraagde duur; de Zorgaanbieder mag dit verzoek afwijzen of het honoreren met de gevraagde of een afwijkende kortere duur.

Verplicht toestemmingsscherm

De toestemmingsverklaring en de toelichting zijn onderdeel van onderstaand verplichte toestemmingsscherm. De *Dienstverlener zorgaanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid 1a op de pagina User interface (Autorisatieserver). De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina (). Deze bestanden beschrijven enkel de tekst en vormgeving van het scherm. De *Dienstverlener zorgaanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina. Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de toestemming.

MedMij
Grip op je eigen gezondheidsgegevens

Optioneel:
Logo ZA

MedMij
veilig online uitwisselen van gezondheidsgegevens

U geeft hierbij NaamZorgaanbieder toestemming om (voortaan) niet langer dan Duur dagen, meldingen over NaamGegevensdienst te doen bij NaamLeverancierPGO voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.

✔ Ja, ik geef toestemming

Nee, ik geef geen toestemming

Als u uw keuze heeft gemaakt of deze pagina sluit, wordt u uitgelogd bij NaamZorgaanbieder.

☑ Toon toelichting

Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen de zorgaanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Wet geneeskundige behandelingsovereenkomst (WGBO) is de zorgaanbieder verplicht ervoor te zorgen dat 'anderen' dan de patiënt (lees: u) geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw medisch dossier, tenzij u hiervoor toestemming heeft verleend.

Aangezien uw PGO (en eventuele achterliggende partij die werkt volgens de MedMij-afspraken) een zogenaamde 'andere' is (in de zin van de WGBO) dient u de zorgaanbieder voor deze gegevensuitwisseling toestemming te verlenen. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door de zorgaanbieder - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

Op basis van uw toestemming moet uw PGO een verzoek doen bij de Zorgaanbieder voor het doen van

meldingen over de betreffende gegevensdienst voor de gevraagde duur; de Zorgaanbieder mag dit verzoek afwijzen of het honoreren met de gevraagde of een afwijkende kortere duur.

Bevestigingsverklaring

> Bevestigingsverklaring is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moet deze pagina herzien worden. Er moet dan een generieke tekst geschreven worden, of per domein wordt een tekst opgesteld.

De bevestigingsverklaring en de toelichting daarop zijn verplichte teksten die de *Dienstverlener zorgaanbieder* dient voor te leggen aan de *Persoon* bij het delen van gezondheidsgegevens met de *Zorgaanbieder*. Deze bevestigingsverklaring heeft betrekking op die gegevensuitwisseling. De verklaring is erop gericht om de *Persoon* te informeren over de voorgenomen uitwisseling van gegevens, en vast te stellen dat deze in overeenstemming met de wil van de *Persoon* plaatsvindt. Daarmee controleert de *Persoon* het verzoek dat de *Dienstverlener persoon* namens hem heeft gedaan voor het delen van een bepaald type gegevens (binnen een *Gegevensdienst*) met een specifieke *Zorgaanbieder*, voordat de *Dienstverlener zorgaanbieder* overgaat tot het autoriseren van de *Dienstverlener persoon* voor deze gegevensuitwisseling.

Bij de functie Delen staat beschreven hoe het proces rondom de bevestiging eruit ziet. De *Dienstverlener zorgaanbieder* implementeert de bevestigingsverklaring en toont deze aan de *Persoon*.

Bevestigingsverklaring

U bevestigt hierbij dat `NaamLeverancierPGO` `NaamGegevensdienst` mag delen met `NaamZorgaanbieder`. De zorgaanbieder beoordeelt of hij deze informatie opneemt in uw medisch dossier en/of gebruikt voor uw behandeling.

Toelichting op de bevestigingsverklaring

U heeft aangegeven uw persoonsgegevens en/of informatie over uw gezondheid met uw zorgaanbieder `NaamZorgaanbieder` te willen uitwisselen.

`NaamZorgaanbieder` verzoekt u te bevestigen dat u uw persoonsgegevens en/of gezondheidsinformatie van het type `NaamGegevensdienst` met hem wenst te delen. Na uw bevestiging stuurt uw zorgaanbieder een bericht naar de leverancier van uw persoonlijke gezondheidsomgeving (`NaamLeverancierPGO`). Hij zorgt er dan voor dat de informatie die u wenst te delen vanuit uw persoonlijke gezondheidsomgeving via MedMij aan uw zorgaanbieder wordt toegezonden. Het is aan `NaamZorgaanbieder` om te beoordelen of hij de informatie die u met hem deelt ook opneemt in uw medisch dossier.

De bevestigingsverklaring en de toelichting zijn onderdeel van een verplicht bevestigingsscherm. De *Dienstverlener zorgaanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid 1b op de pagina User interface (Autorisatieserver).

De *Dienstverlener zorgaanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina.

Bijgesloten HTML en CSS bestanden zijn toegevoegd aan deze pagina als hulpmiddel bij de implementatie. Deze bestanden beschrijven de tekst en vormgeving van het scherm. Het is niet verplicht deze toe te passen.

Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de mogelijkheid om hier opnieuw in te loggen.

Optioneel:
Logo ZA

MedMij
veilig online uitwisselen van gezondheidsgegevens

U bevestigt hierbij dat NaamLeverancierPGO NaamGegevensdienst mag delen met NaamZorgaanbieder. De zorgaanbieder beoordeelt of hij deze informatie opneemt in uw medisch dossier en/of gebruikt voor uw behandeling.

✔Ja, ik bevestig

Nee, ik bevestig niet

Als u uw keuze heeft gemaakt of deze pagina sluit, wordt u uitgelogd bij NaamZorgaanbieder.

☐ Toon toelichting

MedMij
Grip op je eigen gezondheidsgegevens

Optioneel:
Logo ZA

MedMij
veilig online uitwisselen van gezondheidsgegevens

U bevestigt hierbij dat NaamLeverancierPGO NaamGegevensdienst mag delen met NaamZorgaanbieder. De zorgaanbieder beoordeelt of hij deze informatie opneemt in uw medisch dossier en/of gebruikt voor uw behandeling.

✔Ja, ik bevestig

Nee, ik bevestig niet

Als u uw keuze heeft gemaakt of deze pagina sluit, wordt u uitgelogd bij NaamZorgaanbieder.

☑ Toon toelichting

U heeft aangegeven uw persoonsgegevens en/of informatie over uw gezondheid met uw zorgaanbieder NaamZorgaanbieder te willen uitwisselen.

NaamZorgaanbieder verzoekt u te bevestigen dat u uw persoonsgegevens en/of gezondheidsinformatie van het type NaamGegevensdienst met hem wenst te delen. Na uw bevestiging stuurt uw zorgaanbieder een bericht naar de leverancier van uw persoonlijke gezondheidsomgeving (NaamLeverancierPGO). Hij zorgt er dan voor dat de informatie die u wenst te delen vanuit uw persoonlijke gezondheidsomgeving via MedMij aan uw zorgaanbieder wordt toegezonden. Het is aan NaamZorgaanbieder om te beoordelen of hij de informatie die u met hem deelt ook opneemt in uw medisch dossier.

Notificatie van Persoon

Deze pagina bevat teksten die de *Dienstverlener persoon* dient voor te leggen aan de *Persoon* wanneer zij *Persoon* tekstueel op de hoogte stelt van de ontvangst van een *Notificatie* van de *Dienstverlener aanbieder,* in het kader van de functie Notificeren.

Deze release van het afsprakenstelsel kent twee typen *Notificatie*:

1. inhoudelijke *Notificaties*, waarmee wordt aangegeven dat er nieuwe (gezondheids)informatie beschikbaar is gekomen bij een *Aanbieder*. Deze *Notificaties* horen bij de hoofdfunctie *Uitwisseling*;
2. abonnements-*Notificaties*, waarmee een bestaand *Abonnement* namens de *Aanbieder* wordt beëindigd. Deze Notificaties horen bij de hoofdfunctie *Regie*.

Verplichte tekst voor inhoudelijke *Notificaties* — uitgebreide versie

Vanwege uw abonnement bij `NaamAanbieder` op `NaamGegevensdienst`, zijn nieuwe gegevens voor u beschikbaar bij `NaamLeverancierPGO`.

Verplichte tekst voor abonnements-*Notificaties* — uitgebreide versie

`NaamAanbieder` heeft uw abonnement op `NaamGegevensdienst` via `NaamLeverancierPGO` beëindigd.

Wanneer de *Persoon* tekstueel wordt ingelicht over de *Notificatie*, wordt daarbij per default deze uitgebreide versies gebruikt, tenzij de kanalen via welke de *Notificatie* de *Persoon* bereikt onvoldoende veilig zijn om `NaamAanbieder` en `NaamGegevensdienst` over te communiceren. Indien en alleen indien die veiligheid onvoldoende gewaarborgd is, worden de volgende korte versies gebruikt.

Verplichte tekst voor inhoudelijke *Notificaties* — korte versie

Er zijn nieuwe gegevens voor u beschikbaar bij `NaamLeverancierPGO`.

Verplichte tekst voor abonnements-*Notificaties* — korte versie

Eén van uw abonnementen via `NaamLeverancierPGO` is beëindigd.

Beëindigingsverklaring Abonnement

Beëindigingsverklaring Abonnement is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moet deze pagina herzien worden. Er moet dan een generieke tekst geschreven worden, of per domein wordt een tekst opgesteld.

Deze beëindigingsverklaring en de toelichting daarop zijn verplichte teksten die de *Dienstverlener zorgaanbieder* dient voor te leggen aan de *Persoon* bij het beëindigen van een *Abonnement* op gezondheidsgegevens (*Notificaties*) bij de *Zorgaanbieder*. Deze beëindigingsverklaring heeft betrekking op die gegevensuitwisseling. De verplichte beëindigingsverklaring volgt uit de Wet geneeskundige behandelingsovereenkomst (WGBO). De *Zorgaanbieder* is verplicht ervoor te zorgen dat ‘anderen’ dan de patiënt geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van het medisch dossier, tenzij hiervoor toestemming is verleend. Binnen het MedMij Afsprakenstelsel verstrekt de *Zorgaanbieder* door middel van de *Dienstverlener zorgaanbieder* gegevens aan de *Dienstverlener persoon*. Aangezien dit een 'andere' is dan de *Persoon* zelf, moet de *Zorgaanbieder* weten dat de persoon hiervoor de toestemming heeft ingetrokken. Bij de UC Abonneren staat beschreven hoe het proces rondom het intrekken van de toestemming eruit ziet. De *Dienstverlener zorgaanbieder* implementeert de beëindigingsverklaring en toont deze aan de *Persoon*.

Beëindigingsverklaring

U trekt hierbij de toestemming eerder verleend aan `NaamZorgaanbieder` in, om meldingen over `NaamGegevensdienst` te doen bij `NaamLeverancierPGO` voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.

Toelichting op de beëindigingsverklaring

Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen de zorgaanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Wet geneeskundige behandelingsovereenkomst (WGBO) is de zorgaanbieder verplicht ervoor te zorgen dat ‘anderen’ dan de patiënt (lees: u) geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw medisch dossier, *tenzij u hiervoor toestemming heeft verleend*.

Aangezien uw PGO (en eventuele achterliggende partij die werkt volgens de MedMij-afspraken) een zogenaamde ‘andere’ is (in de zin van de WGBO) dient u de zorgaanbieder voor deze gegevensuitwisseling toestemming te verlenen. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door de zorgaanbieder - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

Verplicht beëindigingsscherm

De beëindigingsverklaring en de toelichting zijn onderdeel van onderstaand verplichte toestemmingsscherm. De *Dienstverlener zorgaanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid 1a op de pagina User interface (Autorisatieserver). De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina (). Deze bestanden beschrijven enkel de tekst en vormgeving van het scherm. De *Dienstverlener zorgaanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina. Het is toegestaan zinnen of elementen toe te voegen aan het

scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de toestemming.

MedMij
Grip op je eigen gezondheidsgegevens

Optioneel:
Logo ZA

MedMij
veilig online uitwisselen van gezondheidsgegevens

U trekt hierbij de eerder verleende toestemming aan NaamZorgaanbieder in, om meldingen over NaamGegevensdienst te doen bij NaamLeverancierPGO voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.

✔Ja, ik bevestig

Nee, ik bevestig niet

Als u uw keuze heeft gemaakt of deze pagina sluit, wordt u uitgelogd bij NaamZorgaanbieder.

☑ Toon toelichting

Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen de zorgaanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Wet geneeskundige behandelingsovereenkomst (WGBO) is de zorgaanbieder verplicht ervoor te zorgen dat 'anderen' dan de patiënt (lees: u) geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw medisch dossier, tenzij u hiervoor toestemming heeft verleend.

Aangezien uw PGO (en eventuele achterliggende partij die werkt volgens de MedMij-afspraken) een zogenaamde 'andere' is (in de zin van de WGBO) dient u de zorgaanbieder voor deze gegevensuitwisseling toestemming te verlenen. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door de zorgaanbieder - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

Landingspagina

De landingspagina met de mogelijkheid om in te loggen en de toelichting daarop zijn verplichte teksten die de *Dienstverlener aanbieder* dient voor te leggen aan de *Persoon* bij het ophalen van gezondheidsgegevens bij de *Aanbieder*. Deze landingspagina heeft betrekking op die gegevensuitwisseling. De bijbehorende verplichte toestemmingsverklaring is verder toegelicht in Toestemmingsverklaring

De knop om in te loggen en de toelichting zijn onderdeel van onderstaande verplichte landingspagina. De *Dienstverlener Aanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid core.usrint.100.

Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de mogelijkheid om hier in te loggen.

Bijgesloten HTML en CSS bestanden zijn toegevoegd aan deze pagina als hulpmiddel bij de implementatie. Deze bestanden beschrijven de tekst en vormgeving van het scherm. Het is niet verplicht deze toe te passen.

De *Dienstverlener aanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de pagina.

MedMij
Grip op je eigen gezondheidsgegevens

Optioneel:
Logo ZA

MedMij
veilig online uitwisselen van gezondheidsgegevens

Welkom bij **NaamZorgaanbieder**. Voordat u toestemming kunt geven voor het verzamelen of delen van informatie, moet u inloggen.

Inloggen

Annuleren

☐ Toon toelichting

MedMij
Grip op je eigen gezondheidsgegevens

Optioneel:
Logo ZA

MedMij
veilig online uitwisselen van gezondheidsgegevens

Welkom bij **NaamZorgaanbieder**. Voordat u toestemming kunt geven voor het verzamelen of delen van informatie, moet u inloggen.

Inloggen

Annuleren

☑ Toon toelichting

Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen de zorgaanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Wet geneeskundige behandelingsovereenkomst (WGBO) is de zorgaanbieder verplicht ervoor te zorgen dat 'anderen' dan de patiënt (lees: u) geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw medisch dossier, tenzij u hiervoor toestemming heeft verleend.

Aangezien uw PGO (en eventuele achterliggende partij die werkt volgens de MedMij-afspraken) een zogenaamde 'andere' is (in de zin van de WGBO) dient u de zorgaanbieder voor deze gegevensuitwisseling toestemming te verlenen. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door de zorgaanbieder - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

Annuleringspagina

De annuleringspagina met de mogelijkheid om opnieuw in te loggen en de toelichting daarop zijn verplichte teksten die de *Dienstverlener aanbieder* dient voor te leggen aan de *Persoon* bij het ophalen van gezondheidsgegevens bij de *Aanbieder*. Deze annuleringspagina heeft betrekking op die gegevensuitwisseling. De bijbehorende verplichte toestemmingsverklaring is verder toegelicht in Toestemmingsverklaring.

De knop om (opnieuw) in te loggen en de toelichting zijn onderdeel van onderstaande verplichte annuleringspagina. De *Dienstverlener aanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid core.usrint.101. De *Dienstverlener aanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de pagina.

Bijgesloten HTML en CSS bestanden zijn toegevoegd aan deze pagina als hulpmiddel bij de implementatie. Deze bestanden beschrijven de tekst en vormgeving van het scherm. Het is niet verplicht deze toe te passen.

Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de mogelijkheid om hier opnieuw in te loggen.

MedMij
Grip op je eigen gezondheidsgegevens

Optioneel:
Logo ZA

MedMij
veilig online uitwisselen van gezondheidsgegevens

Uw inlog bij **NaamZorgaanbieder** is afgebroken. Voordat u toestemming kunt geven voor het verzamelen of delen van informatie, moet u alsnog inloggen. Als u wilt stoppen, kunt u dit scherm sluiten.

Inloggen

Annuleren

☐ Toon toelichting

MedMij
Grip op je eigen gezondheidsgegevens

Optioneel:
Logo ZA

MedMij
veilig online uitwisselen van gezondheidsgegevens

Uw inlog bij **NaamZorgaanbieder** is afgebroken. Voordat u toestemming kunt geven voor het verzamelen of delen van informatie, moet u alsnog inloggen. Als u wilt stoppen, kunt u dit scherm sluiten.

Inloggen

Annuleren

☑ Toon toelichting

Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen de zorgaanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Wet geneeskundige behandelingsovereenkomst (WGBO) is de zorgaanbieder verplicht ervoor te zorgen dat 'anderen' dan de patiënt (lees: u) geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw medisch dossier, tenzij u hiervoor toestemming heeft verleend.

Aangezien uw PGO (en eventuele achterliggende partij die werkt volgens de MedMij-afspraken) een zogenaamde 'andere' is (in de zin van de WGBO) dient u de zorgaanbieder voor deze gegevensuitwisseling toestemming te verlenen. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door de zorgaanbieder - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

Managementinformatie

Om het gebruik van MedMij inzichtelijk te maken, leveren de *Dienstverleners persoon* en *Dienstverleners aanbieder* maandelijks een *Beheerrapport* op aan bij Stichting MedMij. De informatie uit deze rapporten wordt geaggregeerd tot een managementrapportage voor de Stichting MedMij en de *Deelnemers*. Concurrentiegevoelige informatie wordt hierbij zoveel mogelijk weggehaald.

Aan de met de *Beheerrapporten* ontvangen informatie voegt Stichting MedMij informatie toe over het gebruik door *Aanbieders*. Deze informatie wordt betrokken uit MedMij Registratie.

De betreffende informatie in opgenomen in het metamodel en een logisch model en wordt door de *Dienstverlener persoon* en *Dienstverlener aanbieder* aangeleverd als XML-document conform het XML-schema zoals gespecificeerd op de pagina XML-schema's. Het betreft de volgende informatie.

	naam in het logische model	definitie voor de *Dienstverlener persoon*	definitie voor de *Dienstverlener zorgaanbieder*
algemeen	`MedMijRapport.Deelnemer`	de identificatie van de *Dienstverlener persoon*	de identificatie van de *Dienstverlener zorgaaanbieder*
	`MedMijRapport.Vanaf`	begindatum en -tijdstip van de periode die de rapportage beslaat: altijd `00h00m00s` van de eerste van een kalendermaand	begindatum en -tijdstip van de periode die de rapportage beslaat: altijd `00h00m00s` van de eerste van een kalendermaand
	`MedMijRapport.Tot`	einddatum en -tijdstip van de periode die de rapportage beslaat: altijd `00h00m00s` van de eerste van de kalendermaand die volgt op `MedMijRapport.Vanaf`	einddatum en -tijdstip van de periode die de rapportage beslaat: altijd `00h00m00s` van de eerste van de kalendermaand die volgt op `MedMijRapport.Vanaf`
	`MedMijRapport.Tijdstempel`	datum en tijdstip van het moment waarop het rapport is aangemaakt	datum en tijdstip van het moment waarop het rapport is aangemaakt
`personen`	`MedMijRapport.Beheerrapport.Personen.Aantal`	het aantal unieke gebruikers (accounts) van de PGO van die *Dienstverlener*	Dit element dient **niet** te worden aangeleverd.

		persoon, gedurende de rapportageperiode	
	`MedMijRapport.Beheerrapport.Personen.AantalActiefSuccesvol`	Aantal unieke gebruikers (Accounts) die in deze periode minimaal één request op een resource interface hebben verstuurd waarop een succesvolle resource respons werd ontvangen	Dit element dient **niet** te worden aangeleverd.
	`MedMijRapport.Beheerrapport.Personen.AantalActiefOnsuccesvol`	Aantal unieke gebruikers (Accounts) die in deze periode minimaal één request op een resource interface hebben verstuurd waarop een niet-succesvolle resource respons werd ontvangen	Dit element dient **niet** te worden aangeleverd.
	MedMijRapport.Beheerrapport.Personen.AantalActiefSuccesvolNieuw	Aantal unieke gebruikers (Accounts) die in deze periode minimaal één request op een resource interface hebben verstuurd waarop een succesvolle resource respons werd ontvangen **EN** die die in voorafgaande periodes binnen dit kalenderjaar NIET voor deze indicator zijn geregistreerd (zie toelichting onder tabel).	Dit element dient **niet** te worden aangeleverd.
per *Gegevensdienst*:	`AuthorizationRequestNumbers.AantalSuccesvol`	het aantal keren dat de *DVP Server* voor deze *Gegevensdienst* een authorization	het aantal keren dat de *Authorization Server* voor deze *Gegevensdienst*

		code heeft ontvangen (UCI verzamelen stap 10 en 11, UCI Delen stap 13 en 14)	een authorization request heeft ontvangen waarop een succesvolle authorization response is uitgegaan
	`AuthorizationRequestNumbers.AantalOnsuccesvol`	Dit element dient **niet** te worden aangeleverd.	het aantal keren dat de *Authorization Server* voor deze *Gegevensdienst* een authorization request heeft ontvangen waarop geen succesvolle authorization response is uitgegaan
	`TokenRequestNumbers.AantalSuccesvol`	het aantal keren dat de *DVP Server* voor deze *Gegevensdienst* een token request heeft gedaan waarop een succesvolle authorization response is ontvangen	het aantal keren dat de *Authorization Server* voor deze *Gegevensdienst* een token request heeft ontvangen waarop een succesvolle authorization response is uitgegaan
	`TokenRequestNumbers.AantalOnsuccesvol`	het aantal keren dat de *DVP Server* voor deze *Gegevensdienst* een token request heeft gedaan waarop geen succesvolle token response is ontvangen	het aantal keren dat de *Authorization Server* voor deze *Gegevensdienst* een token request heeft ontvangen waarop geen succesvolle token response is uitgegaan
	`ResourceRequestNumbers.AantalSuccesvol`	het aantal keren dat de *DVP Server* voor deze *Gegevensdienst* een resource request heeft gedaan waarop een	het aantal keren dat de *Resource Server* voor deze *Gegevensdienst* een resource request heeft ontvangen waarop een

	succesvolle resource response is ontvangen	succesvolle resource response is uitgegaan
`ResourceRequestNumbers.AantalOnsuccesvol`	het aantal keren dat de *DVP Server* voor deze *Gegevensdienst* een resource request heeft gedaan waarop geen succesvolle resource response is ontvangen	het aantal keren dat de *Resource Server* voor deze *Gegevensdienst* een resource request heeft ontvangen waarop geen succesvolle resource response is uitgegaan
`SubscriptionRequestNumbers.AantalSuccesvol`	het aantal keren dat de *DVP Server* voor deze *Gegevensdienst* een subscription request heeft gedaan waarop een succesvolle subscription response is ontvangen	het aantal keren dat de *Subscription Server* voor deze *Gegevensdienst* een subscription request heeft ontvangen waarop een succesvolle subscription response is uitgegaan
`SubscriptionRequestNumbers.AantalOnsuccesvol`	het aantal keren dat de *DVP Server* voor deze *Gegevensdienst* een subscription request heeft gedaan waarop geen succesvolle subscription response is ontvangen	het aantal keren dat de *Subscription Server* voor deze *Gegevensdienst* een subscription request heeft ontvangen waarop geen succesvolle subscription response is uitgegaan
`SubscriptionNotificationNumbers.AantalSuccesvol`	het aantal keren dat bij de *Notification Server* voor deze *Gegevensdienst* een subscription notification is binnengekomen waarop een succesvolle subscription notification response kon worden gestuurd	het aantal keren dat de *Notification Client* voor deze *Gegevensdienst* een subscription notification heeft gestuurd waarop een succesvolle subscription notification response is ontvangen

	`SubscriptionNotificationNumbers.AantalOnsuccesvol`	het aantal keren dat bij de *Notification Server* voor deze *Gegevensdienst* een subscription notification is binnengekomen waarop geen succesvolle subscription notification response kon worden gestuurd	het aantal keren dat bij de *Notification Client* voor deze *Gegevensdienst* een subscription notification heeft gestuurd waarop geen succesvolle subscription notification response is ontvangen
	`ResourceNotificationNumbers.AantalSuccesvol`	het aantal keren dat bij de *Notification Server* voor deze *Gegevensdienst* een resource notification is binnengekomen waarop een succesvolle resource notification response kon worden gestuurd	het aantal keren dat bij de *Notification Client* voor deze *Gegevensdienst* een resource notification heeft gestuurd waarop een succesvolle resource notification response is ontvangen
	`ResourceNotificationNumbers.AantalOnsuccesvol`	het aantal keren dat bij de *Notification Server* voor deze *Gegevensdienst* een resource notification is binnengekomen waarop geen succesvolle subscription notification response kon worden gestuurd	het aantal keren dat bij de *Notification Client* voor deze *Gegevensdienst* een resource notification heeft gestuurd waarop geen succesvolle subscription notification response is ontvangen

AantalActiefSuccesvolNieuw

De indicator 'AantalActiefSuccesvolNieuw' geeft het aantal nieuwe unieke gebruikers weer dat gedurende de rapportageperiode minstens één keer succesvol gebruik heeft gemaakt van de functies verzamelen of delen en die niet al in eerdere rapportageperioden in dit kalenderjaar zijn gerapporteerd (waarbij voor januari geldt dat de teller dus opnieuw start).

Een DVP moet per uniek account per kalenderjaar de datum bijhouden van het moment waarop dit account voor het eerst in dit kalenderjaar één request op een resource interface verstuurde waarop een succesvolle resource respons werd ontvangen. Op basis van deze datum rapporteert de DVP

per maand hoeveel nieuwe accounts er in de rapportageperiode (maand) zijn bijgekomen (Aantal accounts met een datum die valt binnen de rapportageperiode). Als er geen accounts worden gevonden, krijgt de indicator de waarde 0.

Jaarlijks op `99990101 00:00` moet de DVP de geregistreerde data wissen (Nadat er over de laatste periode in het voorafgaande jaar is gerapporteerd(!)).

Telling bij requests voor meerdere Gegevensdiensten

Wanneer gebruik wordt gemaakt van de mogelijkheid voor het verlenen van toestemming voor meerdere *Gegevensdiensten* van één *Aanbieder* in één actie, dan moet hier ook rekening mee worden gehouden in de Managementinformatie. Dit betekent dat:

- Een authorization request dan meetelt bij de telling voor alle *Gegevensdiensten* die zijn opgenomen in de scope van het request;
- Een token request dan meetelt bij de telling voor alle *Gegevensdiensten* waarvoor de authorization code was uitgegeven.

Dit geldt voor zowel succesvolle als voor onsuccesvolle requests.

Beheerrapporten

Met de algemene informatie over *Personen* in de *Beheerrapporten* verkrijgt de Stichting MedMij informatie over de mate waarin MedMij de doelstelling behaalt om alle Nederlanders in de gelegenheid te stellen met een PGO regie te voeren over hun gezondheid(sgegevens).

Met de informatie per *Gegevensdienst* verkrijgt de Stichting MedMij informatie over het succes van de verschillende *Gegevensdiensten*, zodat zij passend beleid kan voeren op de *Catalogus*. Voor elke *Gegevensdienst* is deze informatie geordend per *Interface*. Op deze wijze kunnen *Dienstverleners persoon* en *Dienstverleners aanbieder* de gevraagde informatie verzamelen op een wijze die past bij hun implementatie. Uit de interface-gewijze informatie kunnen door de Stichting MedMij cijfers worden afgeleid over het gebruik van de functies *Verzamelen*, *Delen*, *Abonneren* en *Notificeren*.

De Stichting MedMij en de *MedMij Beheerorganisatie* gebruiken deze informatie niet:

- voor doelen die niet voortvloeien uit de specifieke missie van MedMij;
- op wijzen die niet stroken met de grondslagen van MedMij, of welk deel van het MedMij Afsprakenstelsel dan ook.

De *Gegevensdienst*-specifieke elementen in het *Beheerrapport* van alle *Dienstverleners persoon* samen zouden iedere maand tot hetzelfde totaal moeten leiden als die van alle *Dienstverleners aanbieder* samen. Zij gelden wederzijds als elkaars checksums voor de Stichting MedMij. Voorts geven deze cijfers inzicht in de verdeling van het gebruik van het MedMij-netwerk over de verschillende *Dienstverleners* in beide domein. Daarmee krijgt de Stichting MedMij een indicatie van de mate waarin de Speelveld-principes goed werken.

Addendum aanbieder zonder behandelrelatie

Begrippenlijst

Begrip	Domein	Definitie	Synoniemen
Aanbieder	Zorgaanbiedersdomein	Dit betreft een rol in dit Addendum welke gespeeld kan worden door organisaties die op persoonsniveau gezondheidsinformatie beschikbaar hebben. Zij hebben een wettelijke basis om het BSN te gebruiken, maar geen behandelrelatie in de zin van de WGBO met de zorggebruiker. Vooralsnog is ervoor gekozen de Aanbieder in het zorgaanbiedersdomein te laten vallen en gelden de eisen en verantwoordelijkheden die voor de Zorgaanbieder in het afsprakenstelsel zijn beschreven uitgezonderd hetgeen in dit Addendum beschreven.	brondossierhouder
Dienstverlener aanbieder	Zorgaanbiedersdomein	Dit betreft een rol in dit Addendum. De Dienstverlener aanbieder levert diensten aan de Aanbieder gerelateerd aan de uitwisseling tussen Persoon en Aanbieder en committeert zich hiervoor aan de naleving van de afspraken van het MedMij Afsprakenstelsel. De afspraken die gelden voor de Dienstverlener zorgaanbieder zijn op de Dienstverlener aanbieder van toepassing uitgezonderd hetgeen in dit Addendum beschreven.	

Inleiding

Het MedMij afsprakenstelsel ondersteunt op het moment enkel uitwisseling tussen zorggebruikers en zorgaanbieders wanneer de zorggebruiker met de betreffende zorgaanbieder een behandelrelatie in de zin van de WGBO heeft (gehad). Er zijn echter ook relevante gezondheidsgegevens over de zorggebruiker beschikbaar in andere domeinen. Een voorbeeld hiervan is het publieke gezondheidsdomein (Wet publieke gezondheid), waar onder meer informatie bekend is over welke vaccinaties zijn gegeven in het kader van het rijksvaccinatieprogramma en Covid-19. Ook bij de uitvoering van de Wet langdurige zorg zijn er relevante gegevens bekend bij bijvoorbeeld het CIZ en bij zorgkantoren. Dit addendum maakt het mogelijk om ook deze gezondheidsgegevens te kunnen uitwisselen met het persoonsdomein door *Aanbieders* zonder behandelrelatie te ondersteunen.

Voorwaarden en toepasselijkheid

Dit addendum is van toepassing op organisaties die op persoonsniveau gezondheidsinformatie beschikbaar hebben en een wettelijke basis hebben het BSN te gebruiken, maar geen behandelrelatie hebben. Tevens is de *Aanbieder* een ‘Afnemer DigiD’ in de zin van artikel 1 Besluit verwerking persoonsgegevens generieke digitale infrastructuur. Hoewel het hier strikt genomen geen zorgaanbieders betreft, zullen deze aanbieders en hun dienstverleners, uitgezonderd hetgeen bepaald in dit addendum, wel zo worden behandeld op het MedMij netwerk. Het toelaten van deze aanbieders op het MedMij netwerk bevindt zich in een experimentele fase. Om in deze fase grip te houden op het aanbod van aanbieders mogen zij enkel op het MedMij netwerk

diensten aanbieden na uitdrukkelijke toestemming van stichting MedMij. MedMij behoudt zich het recht voor, toestemming te weigeren of in te trekken. De verwachting is dat in de toekomst de inhoud van dit addendum integraal onderdeel wordt van het afsprakenstelsel en dat daarmee deze voorwaardelijkheid komt te vervallen.

Enkel deelnemers die zijn toegelaten in de rol van *Dienstverlener zorgaanbieder* mogen de rol van *Dienstverlener aanbieder* vervullen. Acceptatie voor de rol *Dienstverlener zorgaanbieder* is tegelijkertijd een acceptatie voor de rol van *Dienstverlener aanbieder*.

Juridische context

Op de *Aanbieder* is sectorspecifieke wetgeving van toepassing (de WGBO is bijvoorbeeld niet van toepassing). Een implicatie is dat er geen controle op behandelrelatie kan en hoeft plaats te vinden en dat de uitwisseling met DVP's als derdenverstrekking dient te worden gezien in het kader van de AVG. Het is aan *Aanbieder* en *Dienstverlener aanbieder* om te bepalen welke additionele wetgeving van toepassing is.

De *Aanbieder* als Gebruiker van Diensten van de *Dienstverlener aanbieder* van het MedMij Afsprakenstelsel ‘verwerkingsverantwoordelijke’ voor de verwerking van persoonsgegevens in de zin van de AVG. In het geval de *Aanbieder* als ‘verwerkingsverantwoordelijke’ de *Dienstverlener aanbieder* inschakelt om in opdracht van hem (bijzondere) persoonsgegevens met de Persoon (via het MedMij- netwerk) te verwerken, is de *Aanbieder* voor deze verwerking van persoonsgegevens verplicht een verwerkersovereenkomst met de *Dienstverlener aanbieder* af te sluiten. MedMij stelt hiervoor een modelverwerksovereenkomst beschikbaar.

Processen en informatie; beschikbaarheids- en ontvankelijkheidstoets

Aangezien er geen behandelrelatie bestaat tussen *Aanbieder* en *Persoon* vervalt de voorwaarde op een controle op de behandelrelatie.

Applicatie; Interfaces; User interface (Autorisatieserver)

De userinterface die aan de Zorggebruiker wordt getoond is aangepast op het niet van toepassing zijn van de WGBO. In de toelichtingen zijn de verwijzing naar WGBO verwijdert en is een verwijzing naar AVG opgenomen. Tevens is in de bevestigingsverklaring opgenomen dat het niet gaat om een medisch dossier.

De volgende verplichte schermen dienen, wanneer van toepassing, getoond te worden:

Annuleringspagina addendum

Beëindigingsverklaring Abonnement addendum

Bevestigingsverklaring addendum

Landingspagina addendum

Toestemmingsverklaring Abonneren addendum

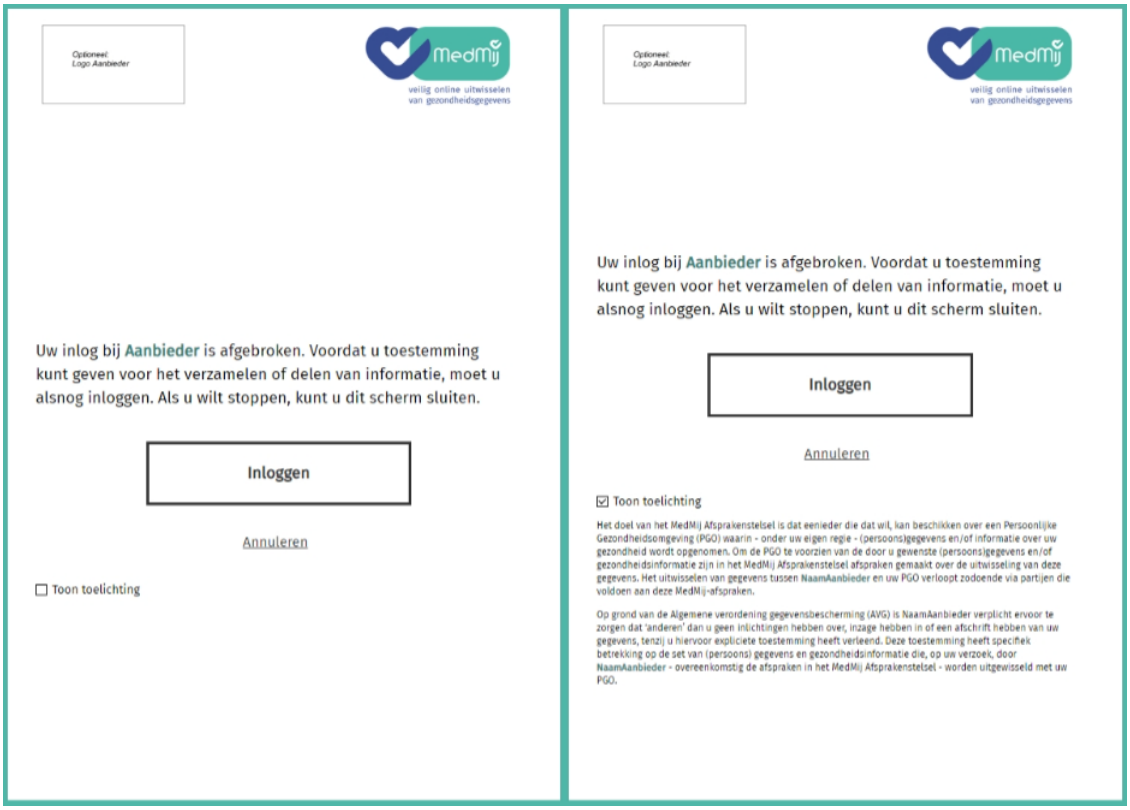
Annuleringspagina addendum

De annuleringspagina met de mogelijkheid om opnieuw in te loggen en de toelichting daarop zijn verplichte teksten die de *Dienstverlener aanbieder* dient voor te leggen aan de *Persoon* bij het ophalen van gezondheidsgegevens bij de *Aanbieder*. Deze annuleringspagina heeft betrekking op die gegevensuitwisseling. De bijbehorende verplichte toestemmingsverklaring is verder toegelicht in Toestemmingsverklaring.

Verplichte annuleringspagina

De knop om (opnieuw) in te loggen en de toelichting zijn onderdeel van onderstaande verplichte annuleringspagina. De *Dienstverlener aanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid core.usrint.100. De HTML- en CSS-bestanden zijn als bijlage toegevoegd aan deze pagina (verplichte schermen). Deze bestanden beschrijven enkel de tekst en vormgeving van het scherm. De *Dienstverlener aanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina. Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de mogelijkheid om hier opnieuw in te loggen.

Verplichte Annuleringspagina



Beëindigingsverklaring Abonnement addendum

Deze beëindigingsverklaring en de toelichting daarop zijn verplichte teksten die de *Dienstverlener aanbieder* dient voor te leggen aan de *Persoon* bij het beëindigen van een *Abonnement* op gezondheidsgegevens (*Notificaties*) bij de *Aanbieder*. Deze beëindigingsverklaring heeft betrekking op die gegevensuitwisseling. De verplichte toestemmingsverklaring volgt uit de Algemene verordening gegevensbescherming (AVG). De *Aanbieder* is verantwoordelijk voor een rechtmatige verstrekking van persoonsgegevens aan derden en mag dit niet zonder expliciete toestemming. Binnen de MedMij afspraken verstrekt de *Aanbieder* via de *Dienstverlener Aanbieder* gegevens aan de *Dienstverlener persoon*. Aangezien dit een 'derde' is in de zin van de AVG, moet de *Aanbieder* weten dat de *Persoon* hiervoor de toestemming heeft ingetrokken. Bij de functie Abonneren staat beschreven hoe het proces rondom het intrekken van de toestemming eruit ziet. De *Dienstverlener Aanbieder* implementeert de beëindigingsverklaring en toont deze aan de *Persoon*.

Beëindigingsverklaring

U trekt hierbij de toestemming eerder verleend aan `NaamAanbieder` in, om meldingen over `NaamGegevensdienst` te doen bij `NaamLeverancierPGO` voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.

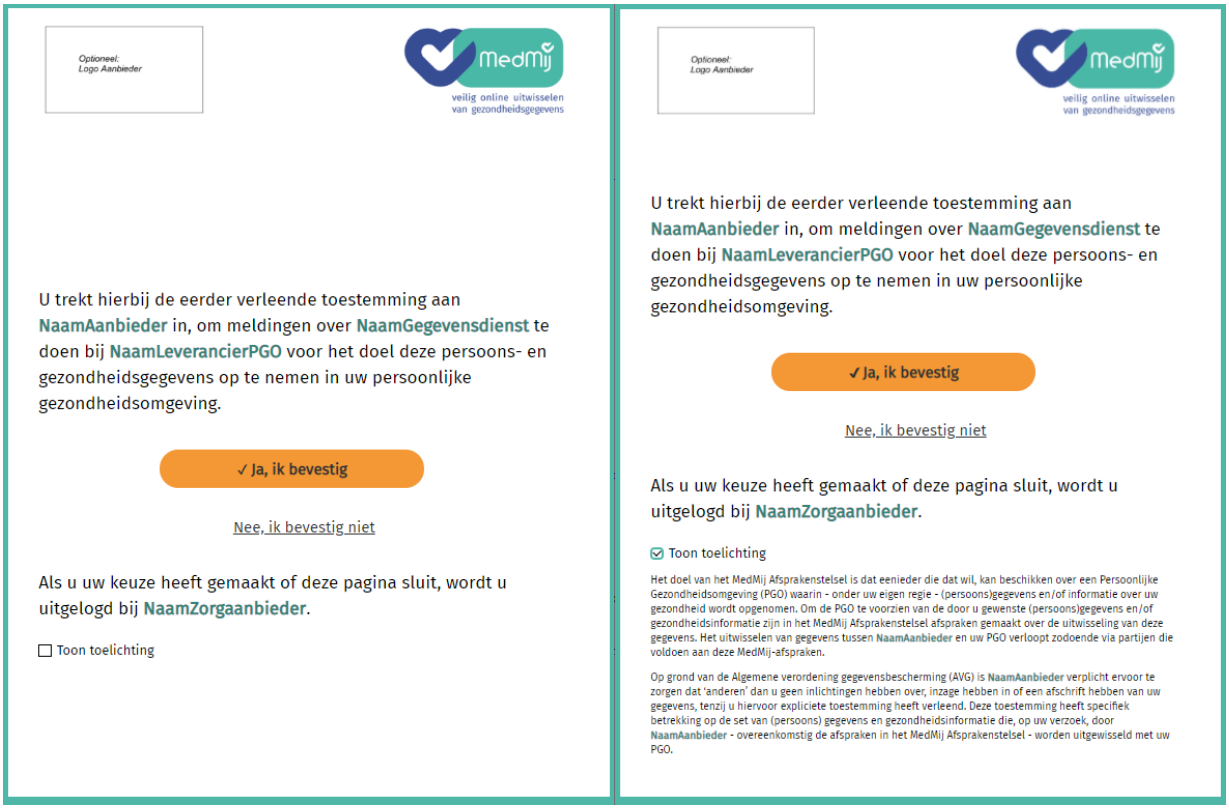
Toelichting op de beëindigingsverklaring

Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen `NaamAanbieder` en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Algemene verordening gegevensbescherming (AVG) is `NaamAanbieder` verplicht ervoor te zorgen dat ‘anderen’ dan u geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw gegevens, *tenzij u hiervoor expliciete toestemming heeft verleend*. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door `NaamAanbieder` - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

Verplicht beëindigingsscherm

De beëindigingsverklaring en de toelichting zijn onderdeel van onderstaand verplichte toestemmingsscherm. De *Dienstverlener Aanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid core.usrint.100. De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina (verplichte schermen). Deze bestanden beschrijven enkel de tekst en vormgeving van het scherm. De *Dienstverlener aanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina. Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de toestemming.


Optioneel:
Logo Aanbieder
MedMij
veilig online uitwisselen
van gezondheidsgegevens
U trekt hierbij de eerder verleende toestemming aan NaamAanbieder in, om meldingen over NaamGegevensdienst te doen bij NaamLeverancierPGO voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.
✓ Ja, ik bevestig
Nee, ik bevestig niet
Als u uw keuze heeft gemaakt of deze pagina sluit, wordt u uitgelogd bij NaamZorgaanbieder.
Toon toelichting
Optioneel:
Logo Aanbieder
MedMij
veilig online uitwisselen
van gezondheidsgegevens
U trekt hierbij de eerder verleende toestemming aan NaamAanbieder in, om meldingen over NaamGegevensdienst te doen bij NaamLeverancierPGO voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.
✓ Ja, ik bevestig
Nee, ik bevestig niet
Als u uw keuze heeft gemaakt of deze pagina sluit, wordt u uitgelogd bij NaamZorgaanbieder.
Toon toelichting
Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen NaamAanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.
Op grond van de Algemene verordening gegevensbescherming (AVG) is NaamAanbieder verplicht ervoor te zorgen dat 'anderen' dan u geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw gegevens, tenzij u hiervoor expliciete toestemming heeft verleend. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door NaamAanbieder - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

Bevestigingsverklaring addendum

De bevestigingsverklaring en de toelichting daarop zijn verplichte teksten die de *Dienstverlener aanbieder* dient voor te leggen aan de *Persoon* bij het delen van gezondheidsgegevens met de *Aanbieder*. Deze bevestigingsverklaring heeft betrekking op die gegevensuitwisseling. De verklaring is erop gericht om de *Persoon* te informeren over de voorgenomen uitwisseling van gegevens, en vast te stellen dat deze in overeenstemming met de wil van de *Persoon* plaatsvindt. Daarmee controleert de *Persoon* het verzoek dat de *Dienstverlener persoon* namens hem heeft gedaan voor het delen van een bepaald type gegevens (binnen een *Gegevensdienst*) met een specifieke *Aanbieder*, voordat de *Dienstverlener aanbieder* overgaat tot het autoriseren van de *Dienstverlener persoon* voor deze gegevensuitwisseling.

Bij de functie Delen staat beschreven hoe het proces rondom de bevestiging eruit ziet. De *Dienstverlener aanbieder* implementeert de bevestigingsverklaring en toont deze aan de *Persoon*.

Bevestigingsverklaring

U bevestigt hierbij dat `NaamLeverancierPGO` `NaamGegevensdienst` mag delen met `NaamAanbieder`. `NaamAanbieder` beoordeelt of hij deze informatie opneemt in uw dossier.

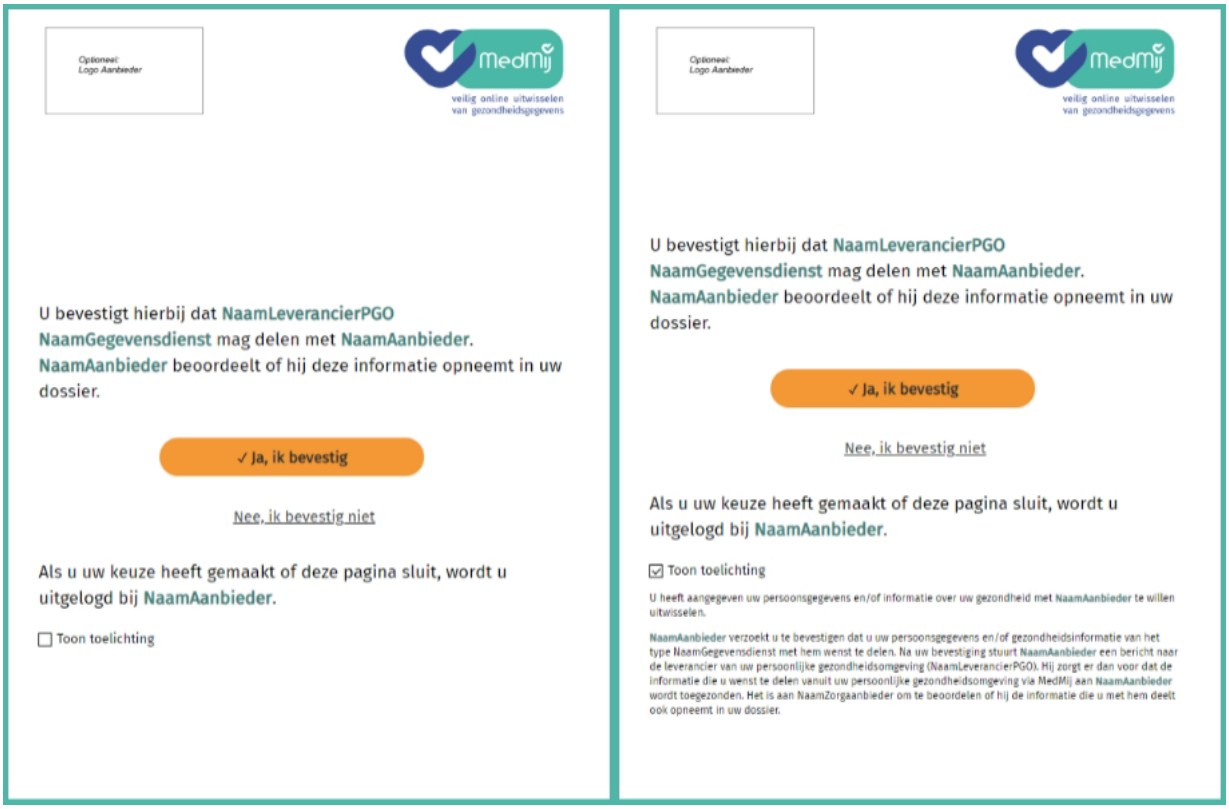
Toelichting op de bevestigingsverklaring

U heeft aangegeven uw persoonsgegevens en/of informatie over uw gezondheid met `NaamAanbieder` te willen uitwisselen.

`NaamAanbieder` verzoekt u te bevestigen dat u uw persoonsgegevens en/of gezondheidsinformatie van het type `NaamGegevensdienst` met hem wenst te delen. Na uw bevestiging stuurt `NaamAanbieder` een bericht naar de leverancier van uw persoonlijke gezondheidsomgeving (`NaamLeverancierPGO`). Hij zorgt er dan voor dat de informatie die u wenst te delen vanuit uw persoonlijke gezondheidsomgeving via MedMij aan `NaamAanbieder` wordt toegezonden. Het is aan `NaamAanbieder` om te beoordelen of hij de informatie die u met hem deelt ook opneemt in uw dossier.

Verplicht bevestigingsscherm

De bevestigingsverklaring en de toelichting zijn onderdeel van een verplicht bevestigingsscherm. De *Dienstverlener aanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid 1b op de pagina User interface (Autorisatieserver). De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina (verplichte schermen). Deze bestanden beschrijven enkel de tekst en vormgeving van het scherm. De *Dienstverlener aanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina. Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de bevestiging.


Optioneel:
Logo Aanbieder
MedMij
veilig online uitwisselen van gezondheidsgegevens
U bevestigt hierbij dat NaamLeverancierPGO NaamGegevensdienst mag delen met NaamAanbieder. NaamAanbieder beoordeelt of hij deze informatie opneemt in uw dossier.
✓ Ja, ik bevestig
Nee, ik bevestig niet
Als u uw keuze heeft gemaakt of deze pagina sluit, wordt u uitgelogd bij NaamAanbieder.
Toon toelichting
Optioneel:
Logo Aanbieder
MedMij
veilig online uitwisselen van gezondheidsgegevens
U bevestigt hierbij dat NaamLeverancierPGO NaamGegevensdienst mag delen met NaamAanbieder. NaamAanbieder beoordeelt of hij deze informatie opneemt in uw dossier.
✓ Ja, ik bevestig
Nee, ik bevestig niet
Als u uw keuze heeft gemaakt of deze pagina sluit, wordt u uitgelogd bij NaamAanbieder.
Toon toelichting
U heeft aangegeven uw persoonsgegevens en/of informatie over uw gezondheid met NaamAanbieder te willen uitwisselen.
NaamAanbieder verzoekt u te bevestigen dat u uw persoonsgegevens en/of gezondheidsinformatie van het type NaamGegevensdienst met hem wenst te delen. Na uw bevestiging stuurt NaamAanbieder een bericht naar de leverancier van uw persoonlijke gezondheidsomgeving (NaamLeverancierPGO). Hij zorgt er dan voor dat de informatie die u wenst te delen vanuit uw persoonlijke gezondheidsomgeving via MedMij aan NaamAanbieder wordt toegezonden. Het is aan NaamZorgaanbieder om te beoordelen of hij de informatie die u met hem deelt ook opneemt in uw dossier.

Landingspagina addendum

De landingspagina met de mogelijkheid om in te loggen en de toelichting daarop zijn verplichte teksten die de *Dienstverlener aanbieder* dient voor te leggen aan de *Persoon* bij het ophalen van gezondheidsgegevens bij de *Aanbieder*. Deze landingspagina heeft betrekking op die gegevensuitwisseling. De bijbehorende verplichte toestemmingsverklaring is verder toegelicht in Toestemmingsverklaring

Verplichte landingspagina

De knop om in te loggen en de toelichting zijn onderdeel van onderstaande verplichte landingspagina. De *Dienstverlener aanbieder*User interface (Autorisatieserver). De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina (verplichte schermen). Deze bestanden beschrijven enkel de tekst en vormgeving van het scherm. De *Dienstverlener aanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina. Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de mogelijkheid om hier in te loggen.

Verplichte Landingspagina

Modelverwerkersovereenkomst addendum

Modelverwerkersovereenkomst Aanbieder - Dienstverlener aanbieder

Doel

De Aanbieder is als verwerkingsverantwoordelijke verantwoordelijk om verwerkingsovereenkomsten af te sluiten in het geval persoonsgegevens in opdracht van hem door een derde (lees: verwerker) worden verwerkt. Binnen het MedMij Afsprakenstelsel opereert de Dienstverlener aanbieder onder verantwoordelijkheid van de Aanbieder. Daarmee dient er altijd een verwerkingsovereenkomst tussen Aanbieder en Dienstverlener zorgaanbieder getekend te worden.

Deze verwerkersovereenkomst is een modelovereenkomst die door de Aanbieder kan worden gebruikt voor MedMij specifieke onderdelen, zoals het verwerken van BSN ten behoeven van authenticatie, het verkrijgen van toestemming van de Persoon voor gegevensuitwisseling met zijn Dienstverlener persoon en het verwerken van persoonsgegevens ten behoeve van de gegevensuitwisseling zelf zoals logging en de verwerking van de betreffende persoonsgegevens door de Dienstverlener aanbieder overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

De ondergetekenden:

1. << naam Aanbieder >> , gevestigd te << plaatsnaam + adres >>, te dezen rechtsgeldig vertegenwoordigd door << naam + functie >>

hierna te noemen: '*Opdrachtgever*',

en

2. << naam Dienstverlener aanbieder >>, (statutair) gevestigd te << plaatsnaam + adres >>, te dezen rechtsgeldig vertegenwoordigd door << functie + naam >>.

hierna te noemen: '*Opdrachtnemer*',

hierna gezamenlijk te noemen: '*Partijen*';

Overwegende dat:

I. Partijen in overeenstemming met de Algemene Verordening gegevensbescherming (AVG) in deze Verwerkersovereenkomst hun afspraken opnemen over het verwerken van persoonsgegevens ten behoeve van de gegevensuitwisseling tussen persoonlijke gezondheidsomgevingen MedMij en de informatiesystemen van de Opdrachtgever.

II. In het kader van de uitvoering van deze Verwerkersovereenkomst de Persoonsgegevens in de zin van artikel 4 sub 1 AVG worden verwerkt binnen de scope van de afspraken zoals opgesteld in het MedMij Afsprakenstelsel.

III. De Opdrachtgever verantwoordelijk is voor het verlenen van toegang tot de persoonsgegevens aan de Persoon en het vaststellen van de identiteit van de Persoon aan de hand van een BSN. De Opdrachtnemer

voert dit proces uit, conform de afspraken in het MedMij Afsprakenstelsel, in opdracht van de Opdrachtgever. De wettelijke basis voor de verwerking van het BSN door Opdrachtgever ten behoeve van authenticatie van de Persoon, met als doel de gegevensuitwisseling tussen Persoon en Opdrachtgever, overeenkomstig het bepaalde in het MedMij Afsprakenstelsel, volgt uit << opnemen wettelijke basis Opdrachtgever >> .

IV. Opdrachtnemer een zogenaamde 'Dienstverlener Zorgaanbieder' binnen het MedMij Afsprakenstelsel is en daarvoor de Deelnemersovereenkomst Dienstverlener zorgaanbieder met de Stichting MedMij heeft afgesloten.

V. Krachtens artikel 4 sub 7 AVG de Opdrachtgever "Verwerkingsverantwoordelijke" is voor de Persoonsgegevens en krachtens artikel 4 sub 8 AVG de Opdrachtnemer "Verwerker" is in het kader van de uitvoering van deze Verwerkersovereenkomst.

VI. Deze overeenkomst is aan te merken als een 'Verwerkersovereenkomst' in de zin van artikel 28 lid 3 AVG.

Verklaren te zijn overeengekomen als volgt

Artikel 1. Begrippen

De hierna en hiervoor in deze Verwerkersovereenkomst vermelde, met een hoofdletter

geschreven begrippen, hebben de volgende betekenis:

1.1 Deelnemersovereenkomst: *'Deelnemersovereenkomst Dienstverlener zorgaanbieder'* die is gesloten tussen Stichting *MedMij en* Opdrachtnemer en op basis waarvan Opdrachtnemer is toegetreden tot het MedMij Afsprakenstelsel.

1.2 Bijlage: aanhangsels bij deze Verwerkersovereenkomst of onder deze Verwerkersovereenkomst aangegane nadere overeenkomst die onlosmakelijk zijn verbonden met deze Verwerkersovereenkomst.

1.3 BSN; het nummer, bedoeld in artikel 1, onder b, van de Wet algemene bepalingen Burgerservicenummer.

1.4 Functionaris voor de gegevensbescherming: de door Opdrachtgever benoemde functionaris als bedoeld in artikel 37 AVG.

1.5 Gegevensdienst: een gestandaardiseerde dienst voor gegevensuitwisseling met waarde voor de gebruiker die door een Dienstverlener persoon of Dienstverlener aanbieder wordt aangeboden over het MedMij-netwerk. De Het MedMij Afsprakenstelsel definieert welke Gegevensdiensten over het MedMij-netwerk aangeboden mogen worden en biedt een faciliteit om het aanbod van de Dienstverlener persoon en Dienstverlener zorgaanbieder inzichtelijk te maken. Opdrachtnemer levert Gegevensdiensten in opdracht van en volgens schriftelijke instructie van de Opdrachtgever via het MedMij-netwerk en heeft voor de verwerking van persoonsgegevens in relatie tot deze Gegevensdiensten de Verwerkersovereenkomst met Opdrachtgever afgesloten.

1.6 MedMij Afsprakenstelsel: de door de Stichting MedMij vastgestelde laatst geldende release van het MedMij Afsprakenstelsel.

1.7 Persoon: degene op wie een Persoonsgegeven betrekking heeft,16 jaar of ouder is, en zich bij Opdrachtnemer authentiseert met een authenticatiemiddel.

1.8 Persoonsgegeven: persoonsgegeven in de zin van artikel 4 sub 1 en sub 15 Algemene Verordening Gegevensbescherming.

1.9 Verwerking: verwerking in de zin van artikel 4 sub 2 Algemene Verordening Gegevensbescherming.

1.10 Verwerkersovereenkomst: deze overeenkomst inclusief Overwegingen en bijbehorende Bijlage(n).

Artikel 2. Totstandkoming, duur van de Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst geldt vanaf de datum van ondertekening en wordt aangegaan voor de duur van de Deelnemersovereenkomst.

2.2 De Verwerkersovereenkomst eindigt van rechtswege wanneer de Deelnemersovereenkomst eindigt.

Artikel 3. Voorwerp van de Verwerkersovereenkomst

3.1 Opdrachtnemer verwerkt het BSN ten behoeven van authenticatie en verwerkt Persoonsgegevens voor:

- het verkrijgen van toestemming van de Persoon voor het verstrekken van Persoonsgegevens aan een derde partij namelijk de Dienstverlener persoon;
- de inhoud van de gegevensuitwisseling;
- handelingen ten behoeve van de gegevensuitwisseling;

overeenkomstig het bepaalde in het MedMij Afsprakenstelsel voor Opdrachtgever op basis van de G egevensdiensten van het MedMij Afsprakenstelsel zoals opgenomen in Bijlage I. De verwerking van Persoonsgegevens vindt uitsluitend plaats in opdracht en volgens schriftelijke instructie van de Opdrachtgever en zoals in Bijlage I aangegeven, behoudens afwijkende wettelijke verplichtingen.

3.2 Opdrachtnemer zal de Persoonsgegevens aantoonbaar op behoorlijke en zorgvuldige wijze en in overeenstemming met de op hem als Verwerker op grond van de privacy- en andere toepasselijke wet- en regelgeving betreffende de verwerking van Persoonsgegevens verwerken.

3.3 Opdrachtnemer verwerkt de Persoonsgegevens niet voor eigen doeleinden. Voor zover niet anders is bepaald in deze Verwerkersovereenkomst, neemt Opdrachtnemer geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over het doel en de middelen voor de Verwerking van de Persoonsgegevens berust nimmer bij Opdrachtnemer.

3.4 Opdrachtnemer schakelt geen derden in zonder voorafgaande specifieke of algemene schriftelijke toestemming van Opdrachtgever. Opdrachtgever kan aan de toestemming om derden in te schakelen voorwaarden verbinden.

3.5 Indien Opdrachtnemer op grond van een wettelijke verplichting gegevens dient te verstrekken, verifieert Opdrachtnemer de grondslag van het verzoek en de identiteit van de verzoeker en informeert hij onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, Opdrachtgever ter zake.

3.6 Opdrachtnemer verleent Opdrachtgever volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de privacy- en andere toepasselijke wet- en regelgeving betreffende de verwerking van Persoonsgegevens, meer in het bijzonder met betrekking tot de rechten van betrokkenen, zoals, maar niet beperkt tot, een verzoek om inzage, verbetering, aanvulling, verwijdering, afscherming of de overdraagbarheid van Persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet. Tevens verleent Opdrachtnemer volledige medewerking aan het adequaat informeren van de betrokkenen in het kader van de meldplicht datalekken. De eventuele kosten die voortvloeien uit het niet of niet tijdig voldoen aan de meldplicht met betrekking tot datalekken komen voor rekening van Opdrachtnemer.

3.7 Indien Opdrachtnemer (pogingen tot) onrechtmatige of anderszins ongeautoriseerde verwerkingen of inbreuken op de beveiligingsmaatregelen van de Persoonsgegevens signaleert, zal hij Opdrachtgever hierover onmiddellijk inlichten en op eigen kosten alle redelijkerwijs benodigde maatregelen treffen om een (dreigende) schending van de privacy- en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens te voorkomen of te beperken; één en ander onverminderd de verplichting van Opdrachtnemer om de eventueel door Opdrachtgever daardoor geleden schade te vergoeden.

3.8 Opdrachtgever en Opdrachtnemer betrekken de Functionaris voor de gegevensbescherming tijdig en naar behoren bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

3.9 Overeenkomstig het bepaalde in Hoofdstuk V van de Algemene Verordening Gegevensbescherming verwerkt Opdrachtnemer geen Persoonsgegevens buiten een land van de Europese Unie/Europese Economische ruimte zonder een passend beschermingsniveau.

Artikel 4. Beveiliging

4.1 Opdrachtnemer zal overeenkomstig de voor Opdrachtgever geldende wet- en regelgeving voor beveiliging de benodigde maatregelen implementeren die het vertrouwen en de continuïteit van de Verwerking borgen. De maatregelen, die zijn opgenomen in het Normenkader informatiebeveiliging van het MedMij Afsprakenstelsel, dienen met inachtneming van de stand der techniek een passend beschermingsniveau te verzekeren voor de Verwerking in relatie tot het MedMij Afsprakenstelsel, zulks met inachtneming van de risico’s die de Verwerking met zich meebrengen.

4.2 Opdrachtnemer rapporteert aan Opdrachtgever over de door hem genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin. De rapportage dient betrekking te hebben op de in het eerste lid bedoelde beveiligingsmaatregelen. Daarnaast toont Opdrachtnemer aan dat hij voldoet aan de voor hem geldende normen op het gebied van informatiebeveiliging. Opdrachtnemer kan aan de hand van geldige certificering of een gelijkwaardig bewijsmiddel aantonen dat hij hieraan voldoet.

Artikel 5. Geheimhouding

5.1 Opdrachtnemer is gehouden tot geheimhouding van alle Persoonsgegevens en informatie die zij als uitvloeisel van deze Verwerkersovereenkomst verwerkt, behoudens in zoverre die gegevens of informatie klaarblijkelijk geen geheim of vertrouwelijk karakter hebben, dan wel reeds algemeen bekend zijn.

5.2 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer ten aanzien van de daarbij aangeduide gegevens of informatie bijzondere maatregelen treffen met het oog op de geheimhouding daarvan, welke maatregelen onder meer kunnen inhouden de vernietiging van betrokken gegevens of informatie zodra de noodzaak voor Opdrachtnemer om daarvan nog langer kennis te nemen, is komen te vervallen.

5.3 Opdrachtnemer zal in haar overeenkomsten met het personeel van Opdrachtnemer bedingen dat door die personen op overeenkomstige wijze als in artikel 5.1 en 5.2 bepaald geheimhouding zal worden betracht ten aanzien van alle gegevens en informatie die zij in het kader van hun werkzaamheden voor Opdrachtnemer verwerken. Opdrachtnemer staat er jegens Opdrachtgever voor in dat de bedoelde bedingen door de betrokken personen zullen worden nageleefd.

Artikel 6. Gebruik onderaannemers (subverwerkers)

6.1 Opdrachtnemer zal aan de door hem ingeschakelde derde dezelfde of strengere verplichtingen opleggen als voor hemzelf gelden op basis van deze Verwerkersovereenkomst en uit de wet- en regelgeving voortvloeien en ziet toe op de naleving daarvan door de derde. De betreffende afspraken met de derde worden schriftelijk vastgelegd. Opdrachtnemer zal Opdrachtgever op eerste verzoek een afschrift verstrekken van deze overeenkomsten(en).

6.2 Niettegenstaande de toestemming van de Opdrachtgever voor het inschakelen van een derde partij blijft Opdrachtnemer volledig aansprakelijk jegens Opdrachtgever voor de gevolgen van het uitbesteden van werkzaamheden aan een derde. De toestemming van Opdrachtgever voor het uitbesteden van werkzaamheden aan een derde partij laat onverlet dat voor de inzet van subverwerkers artikel 3.10 van overeenkomstige toepassing is.

Artikel 7. Controle

7.1 Opdrachtgever kan de Verwerking en de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen van Opdrachtnemer, dan wel die van door Opdrachtnemer ingeschakelde derden, op elk door hem gewenst moment controleren of doen controleren. In verband daarmee verstrekt Opdrachtnemer op eerste verzoek van Opdrachtgever een (zelf)verklaring waarin een oordeel wordt gegeven over de genoemde naleving.

7.2 Opdrachtnemer zal alle redelijkerwijs benodigde medewerking verlenen aan de controle en er voor zorg dragen ook de door hem ingeschakelde derden hiertoe de redelijkerwijs benodigde medewerking zullen verlenen.

7.3 Het uitvoeren van een controle zal niet tot een vertraging van de door Opdrachtnemer in het kader van deze Verwerkersovereenkomst te verrichten werkzaamheden mogen leiden. Indien niettemin vertraging optreedt, zullen Partijen in overleg treden teneinde daarvoor zo snel mogelijk een oplossing te vinden.

7.4 De met de controle gemoeide kosten zijn voor rekening van Opdrachtgever, tenzij uit de controle blijkt dat Opdrachtnemer is tekortgeschoten in de nakoming van zijn verplichting(en) uit deze Verwerkersovereenkomst.

7.5 Opdrachtnemer voert de door Opdrachtgever aangegeven aanbevelingen ter verbetering uit binnen de daartoe door Opdrachtgever te bepalen termijn.

Artikel 8. Opschorting en beëindiging

8.1 Partijen kunnen deze Verwerkersovereenkomst tussentijds opzeggen met inachtneming van een opzegtermijn van één kalendermaand.

8.2 Deze Verwerkersovereenkomst kan door Opdrachtgever met onmiddellijke ingang worden beëindigd indien Opdrachtgever heeft vastgesteld dat Opdrachtnemer niet of onvoldoende voldoet aan de in artikel 4 van deze Verwerkersovereenkomst voorgeschreven technische en organisatorische beveiligingseisen dan wel anderszins de in deze Verwerkersovereenkomst opgenomen voorschriften, verplichtingen of procedures niet nakomt of volgt.

8.3 Verplichtingen welke naar hun aard bestemd zijn ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst gelden. Tot deze bepalingen behorend onder meer de bepalingen betreffende geheimhouding, aansprakelijkheid en toepasselijk recht.

8.4 Partijen zijn gerechtigd, onverminderd hetgeen daartoe bepaalde in de Deelnemersovereenkomst Dienstverlener zorgaanbieder, de uitvoering van de Verwerkersovereenkomst en de daarmee samenhangende Deelenemersovereenkomst op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang te ontbinden, indien:

a) de ander partij wordt ontbonden of anderszins ophoudt te bestaan;

b) de andere partij aantoonbaar tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die ernstige toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling;

c) een partij in staat van faillissement wordt verklaard of surseance van betaling.

8.5 Opdrachtgever is gerechtigd deze Verwerkersovereenkomst per direct te ontbinden indien de Opdrachtnemer te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of rechtspraak aan de verwerking van persoonsgegevens worden gesteld.

Artikel 9. Bewaartermijn, teruggave en vernietiging van Persoongegevens

9.1 Opdrachtnemer bewaart de Persoonsgegevens niet langer dan strikt noodzakelijk voor het doel zoals opgenomen in Bijlage I en conform de bepalingen in het MedMij Afsprakenstelsel.

9.2 Bij beëindiging van de Verwerkersovereenkomst of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijke verzoek van Opdrachtgever zal Opdrachtnemer, kosteloos, naar keuze van Opdrachtgever, de Persoonsgegevens vernietigen of teruggeven aan Opdrachtgever. Op eerste verzoek van Opdrachtgever verstrekt Opdrachtnemer bewijs van het feit dat de Persoonsgegevens vernietigd of verwijderd zijn.

Artikel 10. Aansprakelijkheid

10.1 Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen. Gebruikers kunnen zich jegens Partijen onmiddellijk en direct op deze aansprakelijkheid beroepen.

10.2 Partijen zijn jegens elkaar aansprakelijk indien zij de verplichtingen uit de Verwerkersovereenkomst en /of de privacy- en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens schenden door deze niet of niet naar behoren na te komen. Indien en voor zover deze schending toerekenbaar is, heeft deze schadeplichtigheid tot gevolg.

10.3 Opdrachtnemer vrijwaart Opdrachtgever en stelt Opdrachtgever schadeloos voor alle claims, acties, aanspraken van derden voor verliezen, schade of kosten, waaronder boetes van de Autoriteit Persoonsgegevens die Opdrachtgever maakt of lijdt en die rechtstreeks of indirect voortvloeien uit of tot stand komen in verband met een tekortkoming door de Opdrachtnemer en/of diens onderaannemers in de nakoming van zijn verplichtingen onder deze Verwerkersovereenkomst.

Artikel 11. Slotbepalingen

11.1 Afwijkingen van deze Verwerkersovereenkomst zijn slechts bindend voor zover zij uitdrukkelijk tussen Partijen schriftelijk zijn overeengekomen.

11.2 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing

11.3 Geschillen over en die voortvloeien uit deze overeenkomst worden voorgelegd aan de bevoegde rechter in Den Haag.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

<< naam Aanbieder >>

namens deze,

Naam:

Functie:

Datum

Plaats

<< Naam Dienstverlener aanbieder >>

namens deze,

Naam:

Functie:

Datum:

Plaats:

Bijlage 1. Overzicht Persoonsgegevens en Procedure

Het doel van de Verwerking voor MedMij specifieke onderdelen, overeenkomstig het bepaalde in het MedMij Afsprakenstelsel is op verzoek van de Persoon door de Opdrachtnemer het verwerken van het BSN ten behoeven van authenticatie, het verkrijgen van toestemming van de Persoon voor gegevensuitwisseling, het verwerken van persoonsgegevens ten behoeve van de gegevensuitwisseling, zoals logging, de verwerking van de betreffende persoonsgegevens zelf namens de Opdrachtgever van deze Persoon.

Hiervoor worden uitsluitend de volgende Persoonsgegevens door Opdrachtnemer verwerkt:

- BSN;
- Toestemmingsverklaring van de Persoon voor het verstrekken van gegevens aan een derde partij namelijk de Dienstverlener persoon;
- Bevestigingsverklaring van de Persoon voor het delen van gegevens met de Opdrachtgever;
- De Persoonsgegevens uit de gegevensdiensten die door de Opdrachtgever conform de afspraken uit het MedMij Afsprakenstelsel via het MedMij-netwerk worden verstrekt of verkregen;
- De persoonsgegevens ten behoeve van de gegevensuitwisseling (zoals logging).

De categorie betrokkenen van wie bovenstaande persoonsgegevens worden verwerkt zijn: Personen die willen beschikken over hun gezondheidsinformatie in de PGO en 16 jaar of ouder zijn.

Overeenkomstig artikel 3.1 van deze Verwerkersovereenkomst worden de Persoonsgegevens overeenkomstig de beschreven Processen & Informatie met de bijbehorende use cases door 'Dienstverlener zorgaanbieder' zoals opgenomen in het MedMij Afsprakenstelsel door Opdrachtnemer verwerkt.

Toestemmingsverklaring Abonneren addendum

Deze toestemmingsverklaring en de toelichting daarop zijn verplichte teksten die de *Dienstverlener aanbieder* dient voor te leggen aan de *Persoon* bij het tot stand brengen van een *Abonnement* op gezondheidsgegevens (*Notificaties*) bij de *Aanbieder*. Deze toestemmingsverklaring heeft betrekking op die gegevensuitwisseling. De verplichte toestemmingsverklaring volgt uit de Algemene verordening gegevensbescherming (AVG). De *Aanbieder* is verantwoordelijk voor een rechtmatige verstrekking van persoonsgegevens aan derden en mag dit niet zonder expliciete toestemming. Binnen de MedMij afspraken verstrekt de *Aanbieder* via de *Dienstverlener Aanbieder* gegevens aan de *Dienstverlener persoon*. Aangezien dit een 'derde' is in de zin van de AVG, moet de *Aanbieder* kunnen aantonen dat de *Persoon* hiervoor toestemming heeft verleend. Bij de functie Abonneren staat beschreven hoe het proces rondom het geven van toestemming eruit ziet. De *Dienstverlener aanbieder* implementeert de toestemmingsverklaring en toont deze aan de *Persoon*.

Toestemmingsverklaring

U geeft hierbij `NaamAanbieder` toestemming om, gedurende ten hoogste `Duur` dagen, meldingen over `NaamGegevensdienst` te doen bij `NaamLeverancierPGO` voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.

De looptijd is mogelijk beperkt door `NaamAanbieder`.

Toelichting op de toestemmingsverklaring

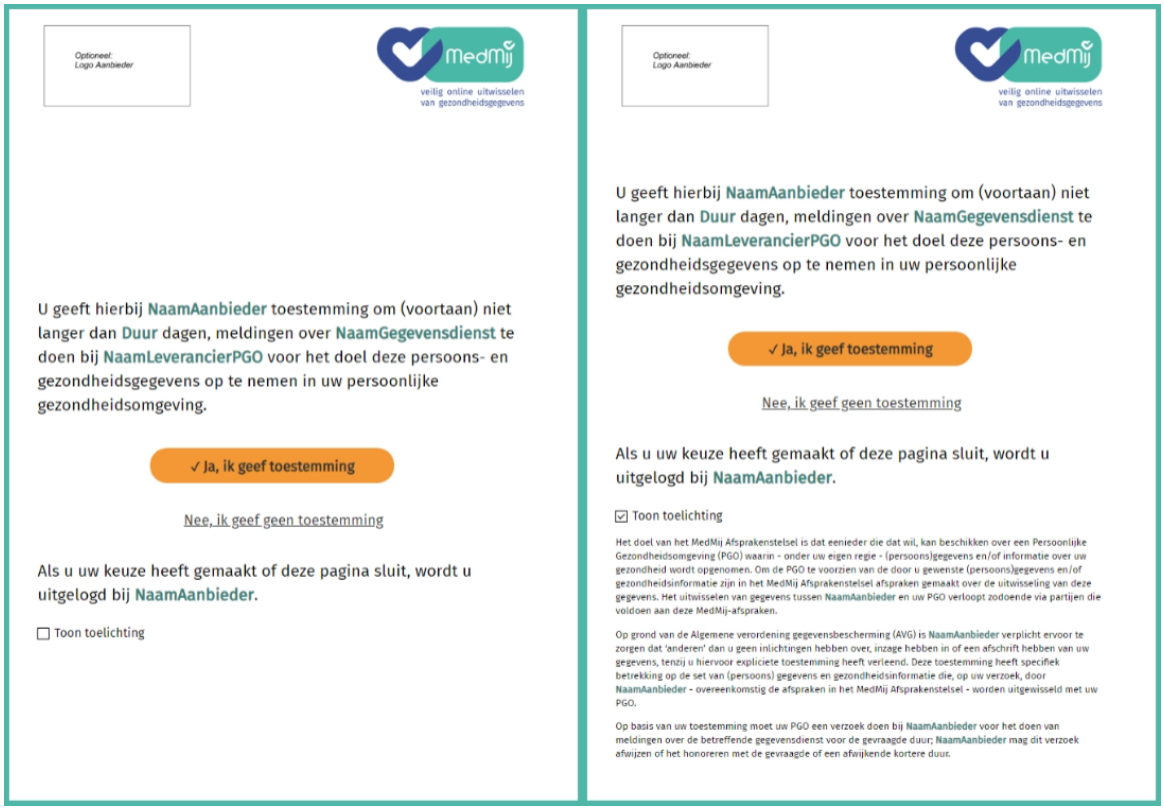
Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen `NaamAanbieder` en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Algemene verordening gegevensbescherming (AVG) is `NaamAanbieder` verplicht ervoor te zorgen dat ‘anderen’ dan u geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw gegevens, *tenzij u hiervoor expliciete toestemming heeft verleend*. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door `NaamAanbieder` - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

Op basis van uw toestemming moet uw PGO een verzoek doen bij `NaamAanbieder` voor het doen van meldingen over de betreffende gegevensdienst voor de gevraagde duur; `NaamAanbieder` mag dit verzoek afwijzen of het honoreren met de gevraagde of een afwijkende kortere duur.

Verplicht toestemmingsscherm

De toestemmingsverklaring en de toelichting zijn onderdeel van onderstaand verplichte toestemmingsscherm. De *Dienstverlener aanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid 1a op de pagina User interface (Autorisatieserver). De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina (verplichte schermen). Deze bestanden beschrijven enkel de tekst en vormgeving van het scherm. De *Dienstverlener aanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina. Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de toestemming.


Optioneel:
Logo Aanbieder
MedMij
veilig online uitwisselen
van gezondheidsgegevens
U geeft hierbij NaamAanbieder toestemming om (voortaan) niet langer dan Duur dagen, meldingen over NaamGegevensdienst te doen bij NaamLeverancierPGO voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.
✓ Ja, ik geef toestemming
Nee, ik geef geen toestemming
Als u uw keuze heeft gemaakt of deze pagina sluit, wordt u uitgelogd bij NaamAanbieder.
Toon toelichting
Optioneel:
Logo Aanbieder
MedMij
veilig online uitwisselen
van gezondheidsgegevens
U geeft hierbij NaamAanbieder toestemming om (voortaan) niet langer dan Duur dagen, meldingen over NaamGegevensdienst te doen bij NaamLeverancierPGO voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.
✓ Ja, ik geef toestemming
Nee, ik geef geen toestemming
Als u uw keuze heeft gemaakt of deze pagina sluit, wordt u uitgelogd bij NaamAanbieder.
Toon toelichting
Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen NaamAanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.
Op grond van de Algemene verordening gegevensbescherming (AVG) is NaamAanbieder verplicht ervoor te zorgen dat 'anderen' dan u geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw gegevens, tenzij u hiervoor expliciete toestemming heeft verleend. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door NaamAanbieder - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.
Op basis van uw toestemming moet uw PGO een verzoek doen bij NaamAanbieder voor het doen van meldingen over de betreffende gegevensdienst voor de gevraagde duur; NaamAanbieder mag dit verzoek afwijzen of het honoreren met de gevraagde of een afwijkende kortere duur.

Toestemmingsverklaring addendum

De toestemmingsverklaring en de toelichting daarop zijn verplichte teksten die de *Dienstverlener aanbieder* dient voor te leggen aan de *Persoon* bij het ophalen van gezondheidsgegevens bij de *Aanbieder*. Deze toestemmingsverklaring heeft betrekking op die gegevensuitwisseling. De verplichte toestemmingsverklaring volgt uit de Algemene verordening gegevensbescherming (AVG). De *Aanbieder* is verantwoordelijk voor een rechtmatige verstrekking van persoonsgegevens aan derden en mag dit niet zonder expliciete toestemming. Binnen de MedMij afspraken verstrekt de *Aanbieder* via de *Dienstverlener Aanbieder* gegevens aan de *Dienstverlener persoon*. Aangezien dit een 'derde' is in de zin van de AVG, moet de *Aanbieder* kunnen aantonen dat de *Persoon* hiervoor toestemming heeft verleend. Bij de UC Verzamelen en de UC Abonneren staat beschreven hoe het proces rondom het geven van toestemming eruit ziet. De *Dienstverlener aanbieder* implementeert de toestemmingsverklaring en toont deze aan de *Persoon*.

Toestemmingsverklaring

U geeft hierbij `NaamAanbieder` toestemming om `NaamGegevensdienst` uit te wisselen met `NaamLeverancierPGO` voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.

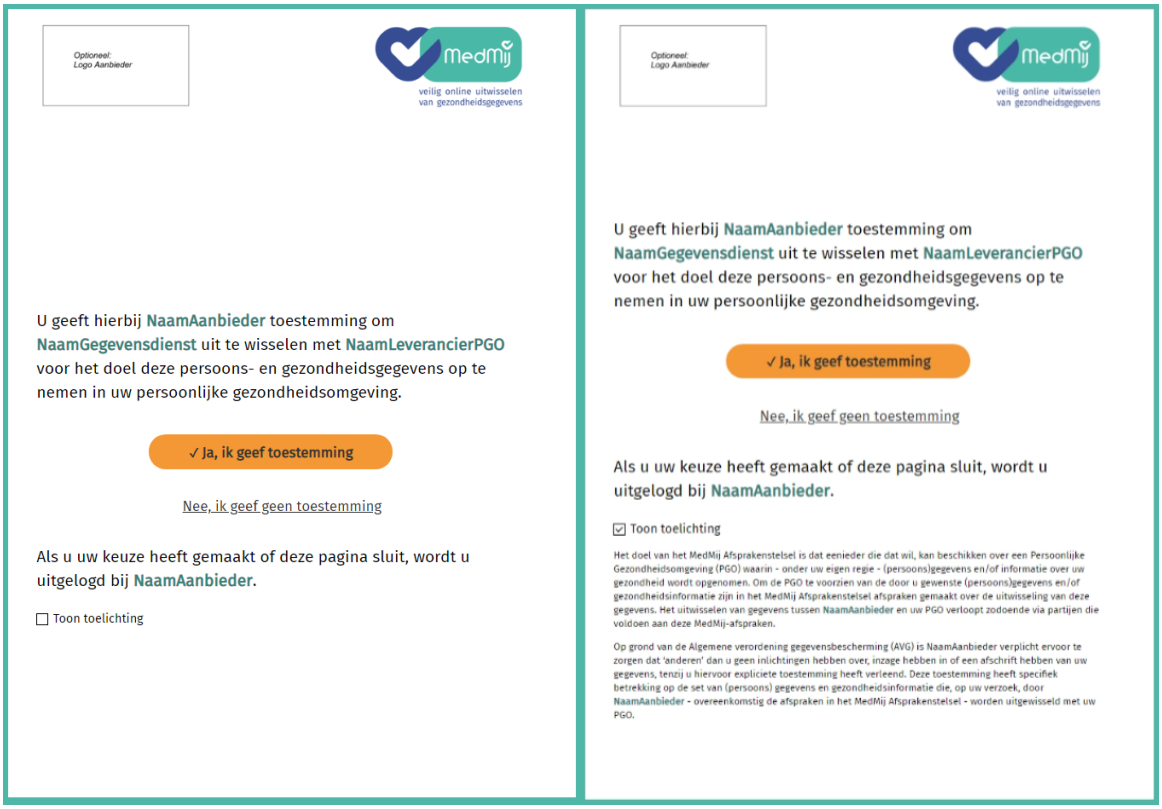
Toelichting op de toestemmingsverklaring

Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen `NaamAanbieder` en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Algemene verordening gegevensbescherming (AVG) is `NaamAanbieder` verplicht ervoor te zorgen dat ‘anderen’ dan u geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw gegevens, *tenzij u hiervoor expliciete toestemming heeft verleend*. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door `NaamAanbieder` - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

Verplicht toestemmingsscherm

De toestemmingsverklaring en de toelichting zijn onderdeel van onderstaand verplichte toestemmingsscherm. De *Dienstverlener aanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid 1a op de pagina User interface (Autorisatieserver). De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina (verplichte schermen). Deze bestanden beschrijven enkel de tekst en vormgeving van het scherm. De *Dienstverlener aanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina. Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de toestemming.


Optioneel:
Logo Aanbieder
MedMij
veilig online uitwisselen van gezondheidsgegevens
U geeft hierbij NaamAanbieder toestemming om NaamGegevensdienst uit te wisselen met NaamLeverancierPGO voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.
✓ Ja, ik geef toestemming
Nee, ik geef geen toestemming
Als u uw keuze heeft gemaakt of deze pagina sluit, wordt u uitgelogd bij NaamAanbieder.
Toon toelichting
Optioneel:
Logo Aanbieder
MedMij
veilig online uitwisselen van gezondheidsgegevens
U geeft hierbij NaamAanbieder toestemming om NaamGegevensdienst uit te wisselen met NaamLeverancierPGO voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.
✓ Ja, ik geef toestemming
Nee, ik geef geen toestemming
Als u uw keuze heeft gemaakt of deze pagina sluit, wordt u uitgelogd bij NaamAanbieder.
Toon toelichting
Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen NaamAanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.
Op grond van de Algemene verordening gegevensbescherming (AVG) is NaamAanbieder verplicht ervoor te zorgen dat 'anderen' dan u geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw gegevens, tenzij u hiervoor expliciete toestemming heeft verleend. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door NaamAanbieder - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

Catalogus

De Catalogus is release-onafhankelijk en kan worden gevonden op MedMij Catalogus.

Deelnemersovereenkomsten

De Deelnemersovereenkomst bevat de basisafspraken tussen Stichting MedMij en een deelnemer aan het afsprakenstelsel. Aangezien er twee typen deelnemers zijn, wordt onderscheid gemaakt tussen een Deelnemersovereenkomst Dienstverlener persoon en een Deelnemersovereenkomst Dienstverlener aanbieder. Deze overeenkomsten zorgen ervoor dat deelnemers gehouden zijn aan de op hen rustende verantwoordelijkheden en verplichtingen. De overeenkomsten binden deelnemers tevens aan de besturings- en nalevingsafspraken die noodzakelijk zijn voor het borgen van het vertrouwen in MedMij. Deelnemers mogen binnen MedMij in hun rol alleen diensten verrichten indien zij een Deelnemersovereenkomst hebben gesloten met Stichting MedMij.

Deelnemersovereenkomst Dienstverlener persoon

Deelnemersovereenkomst Dienstverlener persoon is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moet deze pagina herzien worden. Er moet dan een generieke tekst geschreven worden, of per domein wordt een tekst opgesteld.

Doel

De Deelnemersovereenkomsten bevatten de basisafspraken tussen Stichting MedMij en de Deelnemers van het MedMij Afsprakenstelsel. Er zijn twee typen Deelnemersovereenkomsten, namelijk de Deelnemersovereenkomst Dienstverlener persoon en de Deelnemersovereenkomst Dienstverlener aanbieder.

Partijen

De <Stichting MedMij>, te dezen vertegenwoordigd door <naam>, <functie>

Verder te noemen: Stichting MedMij

en

<Naam partij > gevestigd te <adres>, te dezen vertegenwoordigd door <naam>, <functie>

verder te noemen: Deelnemer,

Hierna gezamenlijk te noemen: Partijen

Overwegende dat

I. het doel van het MedMij Afsprakenstelsel is een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de Persoon met zijn PGO en de Zorgaanbieder met zijn informatiesystemen te waarborgen;

II. de Stichting MedMij verantwoordelijk is voor het beheer van het MedMij Afsprakenstelsel en de controle van de naleving hiervan door de Deelnemer;

III. de Deelnemer wenst toe te treden tot het MedMij Afsprakenstelsel in de rol van Dienstverlener persoon en in deze hoedanigheid wenst te worden toegelaten tot het Netwerk;

IV. de Deelnemer de Toetredingsprocedure voor de rol Dienstverlener persoon met goed gevolg heeft doorlopen;

V. het de Deelnemer wordt toegestaan Diensten aan te bieden. De Deelnemer committeert zich hiervoor aan de laatst geldende release(s) van het MedMij Afsprakenstelsel zoals vastgesteld door de Stichting MedMij en de daarin opgenomen afspraken voor de rol Dienstverlener persoon;

VI. in het MedMij Afsprakenstelsel de verplichtingen zijn vastgelegd waaraan de Deelnemer dient te voldoen;

VII. de Deelnemer desgevraagd te allen tijde zijn medewerking verleent aan de controle op de naleving van de verplichtingen die in het MedMij Afsprakenstelsel voor de rol van Dienstverlener persoon zijn vastgelegd;

VIII. de Deelnemer een actieve bijdrage levert aan de (door)ontwikkeling van het MedMij Afsprakenstelsel.

Verklaren te zijn overeengekomen als volgt

Artikel 1 Definities

De hierna met een hoofdletter aangeduide begrippen hebben in deze Overeenkomst de volgende betekenis:

1.1 Architectuur en technische specificaties: de beschrijving van de technische eisen voor de uitwisseling van (persoons)gegevens en/of gezondheidsinformatie voor de Deelnemer conform het MedMij Afsprakenstelsel.

1.2 AVG: Algemene Verordening Gegevensbescherming.

1.3 Deelnemer: een organisatie die conform de statuten van de Stichting is toegelaten tot de Stichting , toetreedt tot het MedMij Afsprakenstelsel en overeenkomstig hetgeen daarover in het MedMij Afsprakenstelsel is opgenomen de rol van Dienstverlener persoon of Dienstverlener zorgaanbieder vervult.

1.4 Dienstverlener persoon: dit betreft een rol in het MedMij Afsprakenstelsel. De Dienstverlener persoon levert een PGO, een dienst aan de Persoon voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de Zorgaanbieder mogelijk maakt via het Netwerk en conform de afspraken van het MedMij Afsprakenstelsel.

1.5 Dienstverlener zorgaanbieder: dit betreft een rol in het MedMij Afsprakenstelsel. De Dienstverlener zorgaanbieder levert Diensten aan Zorgaanbieders gerelateerd aan de gegevensuitwisseling tussen de Persoon en de Zorgaanbieder via het Netwerk en committeert zich hiervoor aan de naleving van de afspraken van het MedMij Afsprakenstelsel.

1.6 Dienst(en): activiteiten, processen en functionaliteit van de Dienstverlener persoon aan de Persoon teneinde de gegevensuitwisseling tussen Gebruikers te realiseren overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

1.7 Gebruiker: afnemer van de Dienst(en) van de Dienstverlener persoon, zijnde de Persoon, of een afnemer van de Dienst(en) van de Dienstverlener zorgaanbieder, zijnde de Zorgaanbieder.

1.8 Gegevensdienst: een gestandaardiseerde dienst voor gegevensuitwisseling met waarde voor de Gebruiker die door een Dienstverlener persoon of Dienstverlener zorgaanbieder wordt aangeboden over het Netwerk. MedMij definieert welke Gegevensdiensten over het Netwerk aangeboden mogen worden en biedt een faciliteit om het aanbod van de Dienstverlener persoon en Dienstverlener zorgaanbieder inzichtelijk te maken.

1.9 MedMij Afsprakenstelsel: de door de Stichting MedMij vastgestelde laatst geldende release(s) van het MedMij Afsprakenstelsel.

1.10 Merk: (de) woordmerk(en) en/of beeldmerk(en) ten aanzien waarvan Stichting MedMij het merkenrecht uitoefent.

1.11 Netwerk: het MedMij-netwerk zoals gedefinieerd in het MedMij Afsprakenstelsel.

1.12 Overeenkomst: deze Deelnemersovereenkomst.

1.13 Persoon: Persoon die gebruik wenst te maken van een PGO welke gegevens kan uitwisselen met de Zorgaanbieder conform het MedMij Afsprakenstelsel.

1.14 PGO: Een persoonlijke gezondheidsomgeving is een dienst aan de Persoon voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de Zorgaanbieder mogelijk maakt middels het MedMij Afsprakenstelsel.

1.15 Stichting MedMij: beheerder van het MedMij Afsprakenstelsel.

1.16 Toetredingsprocedure: procedure zoals beschreven in de operationele processen van het MedMij Afsprakenstelsel die een organisatie succesvol moet doorlopen om toe te kunnen treden tot en deel te kunnen nemen aan het MedMij Afsprakenstelsel.

1.17 Zorgaanbieder: een zorgverlener of een verband van zorgverleners die behandelingsovereenkomsten kunnen aangaan met patiënten overeenkomstig artikel 7:446 BW, en die via een Dienstverlener zorgaanbieder gegevens kan uitwisselen met de Persoon conform het MedMij Afsprakenstelsel.

Artikel 2 Voorwerp van de Deelnemersovereenkomst

2.1 De Deelnemer heeft het recht voor eigen rekening en risico een PGO en Diensten via het Netwerk aan de Persoon aan te bieden.

2.2 De Deelnemer staat in voor de aantoonbare en controleerbare naleving van de Nederlandse wet- en regelgeving die van toepassing is bij het aanbieden van zijn Diensten en de PGO.

2.3 De Deelnemer is gedurende de looptijd van deze Overeenkomst verplicht op elk en op enig moment ten minste één Gegevensdienst aan de Persoon aan te bieden.

2.4 Partijen zijn gehouden onverkort alle verantwoordlijkheden en verplichtingen op grond van deze Overeenkomst en alle overige bindende regelingen die op enig moment in het MedMij Afsprakenstelsel voor hun rol zijn vastgesteld en in werking zijn getreden, na te komen.

2.5 De Deelnemer conformeert en houdt zich aan de operationele processen en het beleid van het MedMij Afsprakenstelsel, alsmede de voor de Deelnemer relevante architectuur en technische specificaties, het n ormenkader Informatiebeveiliging en de afspraken over managementinformatie en communicatie.

2.6 Partijen erkennen de grondslagen en de juridische context van het MedMij Afsprakenstelsel.

2.7 De Deelnemer levert in samenwerking met Stichting MedMij een actieve bijdrage aan de (door) ontwikkeling van de volgende release van het MedMij Afsprakenstelsel. Partijen houden hiervoor de door de Stichting MedMij vastgestelde strategische releaseplanning aan.

2.8 Het is de Deelnemer niet toegestaan tevens Diensten aan te bieden in de rol van Dienstverlener zorgaanbieder zonder hiervoor de Toetredingsprocedure voor deze rol in het MedMij Afsprakenstelsel te doorlopen.

2.9 De Stichting zorgt ervoor dat de Deelnemer te allen tijde kennis heeft van en/of te allen tijde kennis kan nemen van de operationele processen en samenwerkingsafspraken in relatie tot het beheer, het onderhoud en de (door)ontwikkeling van het MedMij Afsprakenstelsel opdat de Deelnemer (zo nodig) zijn taken en verantwoordelijkheid in of bij de uitvoering van deze operationele processen en samenwerkingsafspraken - dan wel anderszins voor zover van belang voor het vertrouwen in het MedMij Afsprakenstelsel - in zijn rol als Deelnemer kan nemen en/of vervullen.

2.10 Deelnemers brengen elkaar geen onderlinge vergoeding in rekening voor de gegevensuitwisseling tussen Deelnemers ten behoeve van het kunnen leveren van Diensten en Gegevensdiensten via het Netwerk.

Artikel 3 Duur en beëindiging van de Overeenkomst

3.1 Deze Overeenkomst treedt inwerking vanaf de datum van ondertekening en geldt voor onbepaalde tijd.

3.2. De Deelnemer is te allen tijde gerechtigd de Overeenkomst tussentijds door middel van een aangetekend schrijven te beëindigen met inachtneming van een opzegtermijn van vier weken, onverminderd zijn lopende verplichtingen uit deze Overeenkomst zoals, doch niet beperkt tot geheimhouding, privacy en (informatie)beveiliging, als ook nader bepaald in de artikelen 5 en 10 van de Overeenkomst.

3.3 Na beëindiging van de Overeenkomst, om wat voor reden dan ook, zal de Deelnemer direct alle activiteiten en uitingen in het kader van het vervullen van de desbetreffende rol(len) staken, dan wel zo snel mogelijk staken als praktisch haalbaar is. De Deelnemer zal alle medewerking verlenen aan het proces uittreding, zoals opgenomen in het MedMij Afsprakenstelsel. De Deelnemer verleent tevens alle medewerking om zijn Gebruikers te informeren over de stopzetting van de Diensten evenals de verwijzing naar meer informatie voor de mogelijkheden om via een andere Dienstverlener persoon Diensten in het kader van het MedMij Afsprakenstelsel af te nemen.

Artikel 4 Informatieplicht en communicatie

4.1 De Deelnemer draagt, overeenkomstig het bepaalde in het MedMij Afsprakenstelsel en alvorens gebruik wordt gemaakt van zijn Diensten, zorg voor adequate informatieverstrekking en communicatie over zijn Diensten en de PGO aan de Persoon. De Deelnemer hanteert hiervoor de afspraken omtrent communicatie. De informatieverstrekking heeft tenminste betrekking op:

1. deze Overeenkomst;
2. de overeenkomst van de Deelnemer met de Persoon;
3. de verantwoordelijkheid van de Persoon;
4. de Gebruikersvoorlichting zoals ter beschikking gesteld in het MedMij Afsprakenstelsel;
5. de werking van de PGO en bijbehorende Dienst(en);
6. de verwerking van persoonsgegevens overeenkomstig de geldende privacywet-en regelgeving en hoe de Persoon zijn rechten in deze bij de Deelnemer kan uitoefenen.

4.2 De Deelnemer legt communicatie, waaronder persberichten, met betrekking tot de Overeenkomst en het MedMij Afsprakenstelsel ter goedkeuring voor aan de Stichting MedMij alvorens deze wordt gepubliceerd.

4.3 De Deelnemer is te allen tijde aanspreekbaar voor de Persoon op het verlenen van zijn Diensten aan de Persoon en draagt zorg voor een adequate afhandeling hiervan.

4.4 De Deelnemer geeft toestemming voor vermelding van zijn organisatie, zijn rol in het MedMij Afsprakenstelsel en zijn Gegevensdiensten op de MedMij-website.

Artikel 5 Privacy en (Informatie)beveiliging

5.1 Partijen zijn verplicht te voldoen aan de privacy- en beveiligingseisen zoals opgenomen in het normenkader informatiebeveiliging van het MedMij Afsprakenstelsel.

5.2 De Deelnemer is verplicht jegens de Stichting MedMij aan te tonen dat hij voldoet aan de voor hem geldende eisen op het gebied van privacy- en informatiebeveiligingsbeleid evenals het normenkader informatiebeveiliging van het MedMij Afsprakenstelsel.

5.3 Partijen informeren elkaar onverwijld indien sprake is van een storing, aantasting van de betrouwbaarheid van Diensten en/of de PGO of een beveiligingsincident alsmede alle andere aangelegenheden die verband houden met of gevolgen kunnen hebben voor de veiligheid, betrouwbaarheid, beschikbaarheid en continuïteit van de Diensten en/of de PGO overeenkomstig het bepaalde in het MedMij Afsprakenstelsel. De Deelnemer volgt hiervoor het incidenten- en calamiteitenproces, zoals beschreven in het MedMij Afsprakenstelsel.

5.4 De Deelnemer is verantwoordelijk voor de beveiliging en controle van de eigen netwerkverbindingen en -systemen die worden gebruikt voor de koppeling met de netwerkverbindingen en/of - systemen van de Persoon.

5.5 In het kader van deze Overeenkomst is het doel van de verwerking van de persoonsgegevens de waarborging en realisering van een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de Persoon en Zorgaanbieder via de Dienstverlener Persoon en de Dienstverlener Zorgaanbieder overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

5.6 Voor zover de verwerking van persoonsgegevens door de Deelnemer wordt gebaseerd op de rechtmatigheidsgrondslag 'toestemming' in de zin van artikel 6 lid 1 AVG is de verwerking voor een ander doel dan genoemd in artikel 5.5 van deze Overeenkomst toegestaan, mits de beginselen van de AVG op deze verdere verwerking wordt toegepast, de Persoon over deze verdere verwerking wordt geïnformeerd alsmede over de rechten die de Persoon tegen deze verdere verwerking kan uitoefenen. Voor zover de verwerking van de persoonsgegevens wordt gebaseerd op de rechtmatigheidsgrondslag 'noodzakelijk voor de uitvoering van de overeenkomst' in de zin van artikel 6 lid 1 sub c AVG, is verdere verwerking van de persoonsgegevens door de Deelnemer alleen toegestaan indien de evenredigheidstoets van artikel 6 lid 4 AVG succesvol is doorlopen.

5.7 De Deelnemer verstrekt geen persoonsgegevens van de Persoon aan anderen dan degenen waaraan de Deelnemer uit hoofde van de Overeenkomst gegevens mag verstrekken c.q. op grond van een wettelijke verplichting moet verstrekken. Het is de Deelnemer uitdrukkelijk verboden om data betreffende de Persoon te verkopen.

5.8 De Deelnemer en de Stichting hebben aan elkaar kenbaar gemaakt wie binnen de organisatie aanspreekbaar is op het onderwerp privacy en de bepalingen in artikel 5 van de Overeenkomst.

Artikel 6 Aansprakelijkheid

6.1 Partijen aanvaarden door ondertekening van deze Overeenkomst aansprakelijkheid voor het eigen handelen en/of nalaten binnen de rol die zij vervullen. Gebruikers kunnen zich jegens Partijen onmiddellijk en direct op deze aansprakelijkheid beroepen.

6.2 In het kader van aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding.

6.3 De Deelnemer vrijwaart de Stichting MedMij voor vorderingen van derden, uit welke hoofde dan ook, ten gevolge van het gebruik van Diensten en Gegevensdiensten van de Deelnemer.

Artikel 7 Opschorting en ontbinding

7.1 De Stichting is gerechtigd de Overeenkomst door middel van een aangetekend schrijven met onmiddellijke ingang buiten rechte te ontbinden, indien de Deelnemer ook na schriftelijke ingebrekestelling stellende een redelijke termijn in gebreke blijft enige verplichting(en) uit deze Overeenkomst te voldoen.

7.2 Buiten hetgeen elders in deze Overeenkomst is bepaald, is de Stichting MedMij gerechtigd deze Overeenkomst door middel van een aangetekend schrijven met onmiddellijke ingang buiten rechte zonder dat enige ingebrekestelling is vereist te ontbinden indien:

1. De Deelnemer zijn faillissement aanvraagt of failliet is verklaard.
2. De Deelnemer (voorlopige) surceance van betaling aanvraagt of aan hem surseance van betaling is verleend, of onder een schuldsaneringsregeling valt.
3. De onderneming van Deelnemer wordt geliquideerd.
4. De Deelnemer zijn huidige onderneming staakt dan wel op een aanmerkelijk deel van het vermogen van de Deelnemer beslag wordt gelegd.

7. 3 Indien niet-nakoming als bedoeld in artikel 7.1 van de Overeenkomst een gevaar vormt voor de veilige en betrouwbare werking van het Netwerk is de Stichting MedMij gerechtigd passende maatregelen te treffen, waaronder het sommeren van de Deelnemer de levering van Diensten per direct voor een bepaalde tijd op te schorten.

7.4 Indien de Stichting MedMij gebruik maakt van het recht als bedoeld in artikel 7.2 en/of 7.3 van de Overeenkomst meldt hij dit onverwijld aan de Deelnemer.

Artikel 8 Verantwoordelijkheid voor derde partij

8.1 Het is de Deelnemer toegestaan voor zijn Diensten derden in te schakelen.

8.2 Indien de Deelnemer derden inschakelt voor de verwerking van persoonsgegevens, vertaalt de Deelnemer de voor hem geldende afspraken uit het MedMij Afsprakenstelsel in dit kader door naar (sub) verwerkers. De uitvoering van de verwerking van persoonsgegevens door een door de Deelnemer ingeschakelde verwerker wordt geregeld in een (sub)verwerkersovereenkomst.

8.3 De Deelnemer staat er jegens de Stichting MedMij voor in dat de door hem ingeschakelde derde voor zijn Diensten en/of Gegevensdiensten alle verplichtingen uit deze Overeenkomst nakomt en is aansprakelijk voor het handelen op grond van deze Overeenkomst van de door hem ingeschakelde derde.

Artikel 9 Controle naleving

9.1 De Stichting MedMij is bevoegd te (laten) onderzoeken of de Deelnemer de afspraken, eisen en voorwaarden uit het MedMij Afsprakenstelsel en deze Overeenkomst naleeft.

9.2 De Deelnemer verleent zijn medewerking aan een onderzoek tot naleving van het MedMij Afsprakenstelsel en deze Overeenkomst door of namens de Stichting MedMij, dan wel verstrekt de Stichting MedMij in dit kader alle noodzakelijke informatie op eerste verzoek.

Artikel 10 Geheimhouding

10.1 Partijen nemen in relatie tot het MedMij Afsprakenstelsel strikte geheimhouding in acht voor zover het vertrouwelijke informatie betreft of informatie waarvan men het vertrouwelijk karakter redelijkerwijs kan

vermoeden, tenzij een wettelijke plicht of een rechterlijke uitspraak openbaarmaking van deze gegevens gebiedt.

Artikel 11 Intellectueel eigendom

11.1 Alle intellectuele eigendom voor alle soorten zaken die worden ontwikkeld door, voor of namens de Stichting MedMij, zoals bijdragen aan Request For Changes (RFC'S) en/of overige documentatie die bijdragen aan de ontwikkeling van de afspraken binnen het MedMij Afsprakenstelsel en die via het MedMij Afsprakenstelsel openbaar worden gemaakt, komen toe aan Stichting MedMij.

11.2 Alle auteursrechten die door de Deelnemer kunnen worden uitgeoefend voor alle soorten zaken die worden ontwikkeld door, voor of namens de Stichting MedMij, waar en wanneer dan ook, zoals bijdragen aan Request For Changes (RFC'S) en/of overige documentatie die via het MedMij Afsprakenstelsel openbaar worden, berusten bij de Stichting MedMij. Deze intellectuele eigendomsrechten worden op grond van deze Overeenkomst door de Deelnemer om niet aan de Stichting MedMij overgedragen, welke overdracht door Stichting MedMij wordt aanvaard.

11.3 De Deelnemer doet hierbij afstand jegens de Stichting MedMij voor zover van toepassing op bijdragen aan de ontwikkeling van de afspraken binnen het MedMij Afsprakenstelsel zoals bedoeld in artikel 11.1, alsmede van alle eventueel aan hem toekomende persoonlijkheidsrechten als bedoeld in de Auteurswet en voor zover de toepasselijke regelgeving zodanige afstand toelaat. Deelnemer doet dit ook namens eventueel aan zijn zijde betrokken personeelsleden afstand jegens de Stichting MedMij van alle eventueel aan deze personeelsleden toekomende persoonlijkheidsrechten, in de mate waarin de toepasselijke regelgeving zodanige afstand toelaat.

11.4 De Deelnemer heeft het niet-exclusieve en niet-overdraagbare recht om, gedurende de looptijd van deze Overeenkomst, het Merk te gebruiken in verband met het aanbieden van Diensten, in overeenstemming met deze Overeenkomst en de daaruit voortvloeiende voorschriften.

11.5 De Deelnemer zal niets doen dan wel nalaten waardoor de rechten van de Stichting MedMij ten aanzien van het Merk kunnen worden aangetast en/of de ter zake van het Merk opgebouwde goodwill negatief zou kunnen worden beïnvloed en zal op geen enkele wijze, direct dan wel indirect schade toebrengen aan het Merk zoals, maar niet beperkt tot, het niet voldoen aan de privacy- en beveiligingseisen.

Artikel 12 Overdraagbaarheid rechten en verplichtingen overeenkomst

12.1 Partijen zijn niet bevoegd hun rechten en verplichtingen uit de Overeenkomst over te dragen aan een derde, behalve na schriftelijke toestemming van de wederpartij.

12.2 In het geval de Deelnemer zijn rechten en plichten uit de Overeenkomst wil overdragen, dient de overnemende partij eveneens toegelaten te zijn tot het MedMij Afsprakenstelsel in de rol van Dienstverlener p ersoon.

Artikel 13 Geschillen en toepasselijk recht

13.1 Partijen proberen ieder geschil naar aanleiding van deze Overeenkomst eerst in onderling overleg op te lossen. Indien Partijen het geschil ter zake van deze Overeenkomst niet in onderling overleg kunnen beslechten zal het geschil worden voorgelegd aan de ter zake bevoegde rechter te Utrecht, tenzij Partijen zelf alsnog minitrial, bindend advies, arbitrage of andere vormen van alternatieve geschillenbeslechting overeenkomen.

13.2 Op deze Overeenkomst, de uitvoering van deze Overeenkomst en op alle geschillen die daaruit mochten voortvloeien is Nederlands recht van toepassing.

Artikel 14 Overig

14.1 Deze Overeenkomst komt in de plaats van en vervangt alle eerdere overeenkomsten en/of bindende afspraken tussen Partijen in relatie tot het MedMij Afsprakenstelsel.

14.2 De Deelnemer is in de Europese Unie ingeschreven in een door het betreffende lidstaat van vestiging erkend handelsregister.

14.3 In het geval de Deelnemer van juridische status verandert en daarmee mogelijk niet meer aan de toetredingseisen voldoet, dient de Deelnemer deze wijziging schriftelijk te melden aan de Stichting MedMij. Te denken valt aan overname door een onderneming buiten Nederland of de EU, fusie of splitsing en faillissement. In het geval van wijziging van de juridische status behoudt de Stichting MedMij het recht de Overeenkomst te beëindigen en/of de Deelnemer te vragen opnieuw de Toetredingsprocedure te doorlopen.

Aldus overeengekomen in tweevoud,

Namens Stichting MedMij Naam: Functie: Datum: Plaats:	Namens de Deelnemer Naam: Functie: Datum: Plaats:
<Handtekening Stichting MedMij>	<Handtekening deelnemer>

Deelnemersovereenkomst Dienstverlener aanbieder

Deelnemersovereenkomst Dienstverlener aanbieder is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moet deze pagina herzien worden. Er moet dan een generieke tekst geschreven worden, of per domein wordt een tekst opgesteld.

Doel

De Deelnemersovereenkomsten bevatten de basisafspraken tussen Stichting MedMij en de deelnemers van het afsprakenstelsel. Er zijn twee type Deelnemersovereenkomsten, namelijk de Deelnemersovereenkomst Dienstverlener persoon en de Deelnemersovereenkomst Dienstverlener aanbieder.

Partijen

De <Stichting MedMij>, te dezen vertegenwoordigd door <naam>, <functie>,

Verder te noemen: Stichting MedMij

en

<Naam partij> gevestigd te <adres>, te dezen vertegenwoordigd door <naam>, <functie>,

Verder te noemen: Deelnemer,

Hierna gezamenlijk te noemen: Partijen

Overwegende dat

I. het doel van het MedMij Afsprakenstelsel is een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de Persoon met zijn PGO en de Zorgaanbieder met zijn informatiesystemen te waarborgen;

II. de Stichting MedMij verantwoordelijk is voor het beheer van het MedMij Afsprakenstelsel en de controle van de naleving hiervan door de Deelnemer;

III. de Deelnemer wenst toe te treden tot het MedMij Afsprakenstelsel in de rol van Dienstverlener zorgaanbieder en in deze hoedanigheid wenst te worden toegelaten tot het Netwerk;

IV. het de Deelnemer de Toetredingsprocedure voor de rol Dienstverlener zorgaanbieder met goed gevolg heeft doorlopen;

V. de Deelnemer wordt toegestaan Diensten aan te bieden. De Deelnemer committeert zich hiervoor aan de laatst geldende release(s) van het MedMij Afsprakenstelsel zoals vastgestreld door de Stichting MedMij en de daarin opgenomen afspraken voor de rol Dienstverlener zorgaanbieder;

VI. in het MedMij Afsprakenstelsel de verplichtingen zijn opgenomen waaraan de Deelnemer dient te voldoen;

VII. de Deelnemer desgevraagd te allen tijde zijn medewerking verleent aan de controle op de naleving van de verplichtingen die in het MedMij Afsprakenstelsel voor de rol van Dienstverlener zorgaanbieder zijn vastgelegd;

VIII. de Deelnemer een bijdrage wenst te leveren aan de (door)ontwikkeling van het MedMij Afsprakenstelsel.

Verklaren te zijn overeengekomen als volgt

Artikel 1 Definities

De hierna met een hoofdletter aangeduide begrippen hebben in deze Overeenkomst de volgende betekenis:

1.1 Architectuur en technische specificaties: de beschrijving van de technische eisen voor de uitwisseling van (persoons)gegevens en/of gezondheidsinformatie door de Deelnemer conform het MedMij Afsprakenstelsel.

1.2 AVG: Algemene Verordening Gegevensbescherming.

1.3 Deelnemer: een organisatie die conform de statuten van de Stichting is toegelaten tot de Stichting, toetreedt tot het MedMij Afsprakenstelsel en overeenkomstig hetgeen daarover in het MedMij Afsprakenstelsel is opgenomen de rol van Dienstverlener persoon of Dienstverlener zorgaanbieder vervult.

1.4 Dienstverlener persoon: dit betreft een rol in het MedMij Afsprakenstelsel. De Dienstverlener persoon levert een PGO, een dienst aan de Persoon voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de Zorgaanbieder mogelijk maakt via het Netwerk en conform de afspraken van het MedMij Afsprakenstelsel.

1.5 Dienstverlener zorgaanbieder: dit betreft een rol in het MedMij Afsprakenstelsel. De Dienstverlener zorgaanbieder levert Diensten aan Zorgaanbieders gerelateerd aan de gegevensuitwisseling tussen de Persoon en de Zorgaanbieder via het Netwerk en committeert zich hiervoor aan de naleving van de afspraken van het MedMij

1.6 Dienst(en): activiteiten, processen en functionaliteit van de Dienstverlener zorgaanbieder aan de Zorgaanbieder teneinde de gegevensuitwisseling tussen de Zorgaanbieder en de Persoon van 16 jaar of ouder te realiseren overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

1.7 Gebruiker: afnemer van de Dienst(en) van de Dienstverlener zorgaanbieder, zijnde de Zorgaanbieder, of een afnemer van de Dienst(en) van de Dienstverlener persoon, zijnde de Persoon.

1.8 Gegevensdienst: een gestandaardiseerde dienst voor gegevensuitwisseling met waarde voor de Gebruiker die door een Dienstverlener persoon of Dienstverlener zorgaanbieder wordt aangeboden over het Netwerk. MedMij definieert welke Gegevensdiensten over het Netwerk aangeboden mogen worden en biedt een faciliteit om het aanbod van de Dienstverlener persoon en Dienstverlener zorgaanbieder inzichtelijk te maken. De Dienstverlener zorgaanbieder levert Gegevensdiensten in opdracht van en volgens schriftelijke instructie van de Zorgaanbieder via het Netwerk en heeft voor de verwerking van persoonsgegevens in relatie tot deze Gegevensdiensten een verwerkersovereenkomst met de Zorgaanbieder afgesloten.

1.9 MedMij Afsprakenstelsel: de door de Stichting MedMij vastgestelde laatst geldende release van het MedMij Afsprakenstelsel.

1.10 Merk: (de) woordmerk(en) en/of beeldmerk(en) ten aanzien waarvan Stichting MedMij het merkenrecht uitoefent.

1.11 Netwerk: het MedMij-netwerk zoals gedefinieerd in het MedMij Afsprakenstelsel.

1.12 Overeenkomst: deze Deelnemersovereenkomst.

1.13 Persoon: Persoon die gebruik wenst te maken van een PGO welke gegevens kan uitwisselen met de Zorgaanbieder conform het MedMij Afsprakenstelsel.

1.14 PGO: Een persoonlijke gezondheidsomgeving is een dienst aan de Persoon voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de Zorgaanbieder mogelijk maakt middels het MedMij Afsprakenstelsel.

1.15 Stichting MedMij: beheerder van het afsprakenstelsel MedMij.

1.16 Toetredingsprocedure: procedure zoals beschreven in de operationele processen van het MedMij Afsprakenstelsel die een organisatie succesvol moet doorlopen om toe te kunnen treden en deel te kunnen nemen aan het MedMij Afsprakenstelsel.

1.17 Zorgaanbieder: een zorgverlener of een verband van zorgverleners die behandelingsovereenkomsten kunnen aangaan met patiënten overeenkomstig artikel 7:446 BW, en die via een Dienstverlener zorgaanbieder gegevens kan uitwisselen met de Persoon conform het MedMij Afsprakenstelsel.

Artikel 2 Voorwerp van de Deelnemersovereenkomst

2.1 De Deelnemer heeft het recht voor eigen rekening en risico Diensten via het Netwerk aan te bieden aan de Zorgaanbieder.

2.2 De Deelnemer staat in voor de aantoonbare en controleerbare naleving van de Nederlandse wet- en regelgeving die van toepassing is bij het aanbieden van zijn Diensten en de PGO.

2.3 De Deelnemer is gedurende de looptijd van deze Overeenkomst verplicht op elk en op enig moment ten minste één Gegevensdienst aan zijn Gebruikers aan te bieden.

2.4 Partijen zijn gehouden onverkort alle verantwoordlijkheden en verplichtingen op grond van deze Overeenkomst en alle overige bindende regelingen die op enig moment in het MedMij Afsprakenstelsel voor hun rol zijn vastgesteld en in werking zijn getreden, na te komen.

2.5 De Deelnemer conformeert en houdt zich aan de operationele processen en het beleid van het MedMij Afsprakenstelsel, alsmede de voor de Deelnemer relevante architectuur en technische specificaties, het normenkader Informatiebeveiliging en de afspraken over managementinformatie en communicatie.

2.6 Partijen erkennen de grondslagen en de juridische context van het MedMij Afsprakenstelsel.

2.7 De Deelnemer levert in samenwerking met Stichting MedMij een actieve bijdrage aan de (door) ontwikkeling van de volgende release van het MedMij Afsprakenstelsel. Partijen houden hiervoor de door de Stichting MedMij vastgestelde strategische releaseplanning aan.

2.8 Het is de Deelnemer niet toegestaan tevens Diensten aan te bieden in de rol van Dienstverlener persoon zonder hiervoor de Toetredingsprocedure voor deze rol in het MedMij Afsprakenstelsel te doorlopen.

2.9 De Stichting MedMij zorgt ervoor dat de Deelnemer te allen tijde kennis heeft van en/of te allen tijde kennis kan nemen van de operationele processen en samenwerkingsafspraken in relatie tot het beheer, het onderhoud en de (door)ontwikkeling van het MedMij Afsprakenstelsel opdat de Deelnemer (zo nodig) zijn taken en verantwoordelijkheid in of bij de uitvoering van deze operationele processen en

samenwerkingsafspraken - dan wel anderszins voor zover van belang voor het vertrouwen in het MedMij Afsprakenstelsel - in zijn rol als Deelnemer kan nemen en/of vervullen.

2.10 Deelnemers brengen elkaar geen onderlinge vergoeding in rekening voor de gegevensuitwisseling tussen Deelnemers ten behoeve van het kunnen leveren van Diensten en Gegevensdiensten via het Netwerk.

Artikel 3 Duur en beëindiging van Overeenkomst

3.1 Deze Overeenkomst treedt inwerking vanaf de datum van ondertekening en geldt voor onbepaalde tijd.

3.2. De Deelnemer is te allen tijde gerechtigd de Overeenkomst tussentijds door middel van een aangetekend schrijven te beëindigen met inachtneming van een opzegtermijn van vier weken, onverminderd zijn lopende verplichtingen uit deze Overeenkomst zoals, doch niet beperkt tot geheimhouding, privacy en (informatie)beveiliging, als ook nader bepaald in de artikelen 5 en 10 van de Overeenkomst.

3.3 Na beëindiging van de Overeenkomst, om wat voor reden dan ook, zal de Deelnemer direct alle activiteiten en uitingen in het kader van het vervullen van de desbetreffende rol(len) staken, dan wel zo snel mogelijk staken als praktisch haalbaar is. De Deelnemer zal alle medewerking verlenen aan het proces uittreding, zoals opgenomen in het MedMij Afsprakenstelsel. De Deelnemer verleent tevens alle medewerking om zijn Gebruikers te informeren over de stopzetting van de Diensten evenals de verwijzing naar meer informatie voor de mogelijkheden om via een andere Dienstverlener persoon Diensten in het kader van het MedMij Afsprakenstelsel af te nemen.

Artikel 4 Informatieplicht en communicatie

4.1 De Deelnemer draagt, overeenkomstig het bepaalde in het MedMij Afsprakenstelsel en alvorens gebruik wordt gemaakt van zijn Diensten, zorg voor adequate informatieverstrekking en communicatie over zijn Diensten richting de Zorgaanbieder. De Deelnemer hanteert hiervoor de afspraken omtrent communicatie. De informatieverstrekking heeft tenminste betrekking op:

1. deze Overeenkomst;
2. de overeenkomst van de Deelnemer met de Zorgaanbieder;
3. de verantwoordelijkheden van de Zorgaanbieder;
4. de Gebruikersvoorlichting zoals ter beschikking gesteld in het MedMij Afsprakenstelsel;
5. de werking van de Dienst;
6. de verwerking van persoonsgegevens overeenkomstig de geldende privacywet-en regelgeving.

4.2 De Deelnemer legt communicatie, waaronder persberichten, met betrekking tot de Overeenkomst en het MedMij Afsprakenstelsel ter goedkeuring voor aan de Stichting MedMij alvorens deze wordt gepubliceerd.

4.3 De Deelnemer is te allen tijde aanspreekbaar voor de Zorgaanbieder op het verlenen van zijn Diensten conform het MedMij Afsprakenstelsel.

4.4 De Deelnemer geeft toestemming voor vermelding van zijn organisatie, zijn rol in het MedMij Afsprakenstelsel en zijn Gegevensdiensten op de MedMij-website.

Artikel 5 Privacy en (Informatie)beveiliging

5.1 Partijen zijn verplicht te voldoen aan de privacy- en beveiligingseisen zoals opgenomen in het normenkader informatiebeveiliging van het MedMij Afsprakenstelsel.

5.2 De Deelnemer is verplicht jegens de Stichting MedMij aan te tonen dat hij voldoet aan de voor hem geldende eisen op het gebied van privacy- en informatiebeveiligingsbeleid evenals het normenkader informatiebeveiliging van het MedMij Afsprakenstelsel.

5.3 Partijen informeren elkaar onverwijld indien sprake is van een storing, aantasting van de betrouwbaarheid van Diensten en/of de PGO of een beveiligingsincident alsmede alle andere aangelegenheden die verband houden met of gevolgen kunnen hebben voor de veiligheid, betrouwbaarheid, beschikbaarheid en continuïteit van de Diensten en/of de PGO overeenkomstig het bepaalde in het MedMij Afsprakenstelsel. De Deelnemer volgt hiervoor het incidenten- en calamiteitenproces, zoals beschreven in het MedMij Afsprakenstelsel.

5.4 De Deelnemer is verantwoordelijk voor de beveiliging en controle van de eigen netwerkverbindingen en -systemen die worden gebruikt voor de koppeling met de netwerkverbindingen en/of - systemen van de Zorgaanbieder.

5.5 In het kader van deze Overeenkomst is het doel van de verwerking van de persoonsgegevens de waarborging en realisering van een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de Persoon en Zorgaanbieder via de Dienstverlener Persoon en de Dienstverlener Zorgaanbieder overeenkomstig het bepaalde in het MedMij Afsprakenstelsel. De Deelnemer verwerkt de persoonsgegevens in het kader van deze Overeenkomst in opdracht van en namens de Zorgaanbieder.

5.6 De Deelnemer verstrekt de persoonsgegevens van de Persoon, die hij in opdracht van en namens de Zorgaanbieder verwerkt, niet aan anderen dan degenen waaraan de Deelnemer de gegevens mag verstrekken c.q. op grond van een wettelijke verplichting moet verstrekken. Het is de Deelnemer uitdrukkelijk verboden om data betreffende de Persoon te verkopen.

5.7 Voor de Diensten van de Deelnemer die geschieden in opdracht van de Zorgaanbieder en door Deelnemer in het kader van de uitvoering van deze Overeenkomst plaatsvinden en waarbij persoonsgegevens in de zin van de AVG worden verwerkt, kan voor deze verwerking van persoonsgegevens gebruik worden gemaakt van de modelverwerkersovereenkomst.

5.8 De Deelnemer en de Stichting hebben aan elkaar kenbaar gemaakt wie binnen de organisatie aanspreekbaar is op het onderwerp privacy en de bepalingen in artikel 5 van de Overeenkomst.

Artikel 6 Aansprakelijkheid

6.1 Partijen aanvaarden door ondertekening van deze Overeenkomst aansprakelijkheid voor het eigen handelen en/of nalaten binnen de rol die zij vervullen. Gebruikers kunnen zich jegens Partijen onmiddellijk en direct op deze aansprakelijkheid beroepen.

6.2 In het kader van aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding.

6.3 De Deelnemer vrijwaart de Stichting MedMij voor vorderingen van derden, uit welke hoofde dan ook, ten gevolge van het gebruik van Diensten en Gegevensdiensten van de Deelnemer.

Artikel 7 Opschorting en ontbinding

7.1 De Stichting is gerechtigd de Overeenkomst door middel van een aangetekend schrijven met onmiddellijke ingang buiten rechte te ontbinden, indien de Deelnemer ook na schriftelijke ingebrekestelling stellende een redelijke termijn in gebreke blijft enige verplichting(en) uit deze Overeenkomst te voldoen.

7.2 Buiten hetgeen elders in deze Overeenkomst is bepaald, is de Stichting MedMij gerechtigd deze Overeenkomst door middel van een aangetekend schrijven met onmiddellijke ingang buiten rechte zonder dat enige ingebrekestelling is vereist te ontbinden indien:

1. De Deelnemer zijn faillissement aanvraagt of failliet is verklaard.
2. De Deelnemer (voorlopige) surceance van betaling aanvraagt of aan hem surseance van betaling is verleend, of onder een schuldsaneringsregeling valt.
3. De onderneming van Deelnemer wordt geliquideerd.
4. De Deelnemer zijn huidige onderneming staakt dan wel op een aanmerkelijk deel van het vermogen van de Deelnemer beslag wordt gelegd.

7. 3 Indien niet-nakoming als bedoeld in artikel 7.1 van de Overeenkomst een gevaar vormt voor de veilige en betrouwbare werking van het Netwerk is de Stichting MedMij gerechtigd passende maatregelen te treffen, waaronder het sommeren van de Deelnemer de levering van Diensten per direct voor een bepaalde tijd op te schorten.

7.4 Indien de Stichting MedMij gebruik maakt van het recht als bedoeld in artikel 7.2 en/of 7.3 van de Overeenkomst meldt hij dit onverwijld aan de Deelnemer.

Artikel 8 Verantwoordelijkheid voor derde partij

8.1 Het is de Deelnemer toegestaan voor zijn Diensten derden in te schakelen.

8.2 Indien de Deelnemer derden inschakelt voor de verwerking van persoonsgegevens, vertaalt de Deelnemer de voor hem geldende afspraken uit het MedMij Afsprakenstelsel in dit kader door naar (sub) verwerkers. De uitvoering van de verwerking van persoonsgegevens door een door de Deelnemer ingeschakelde verwerker wordt geregeld in een (sub)verwerkersovereenkomst.

8.3 De Deelnemer staat er jegens de Stichting MedMij voor in dat de door hem ingeschakelde derde voor zijn Diensten en/of Gegevensdiensten alle verplichtingen uit deze Overeenkomst nakomt en is aansprakelijk voor het handelen op grond van deze Overeenkomst van de door hem ingeschakelde derde.

Artikel 9 Controle naleving

9.1 De Stichting MedMij is bevoegd te (laten) onderzoeken of de Deelnemer de afspraken, eisen en voorwaarden uit het MedMij Afsprakenstelsel en deze Overeenkomst naleeft.

9.2 De Deelnemer verleent zijn medewerking aan een onderzoek tot naleving van het MedMij Afsprakenstelsel en deze Overeenkomst door of namens de Stichting MedMij, dan wel verstrekt de Stichting MedMij in dit kader alle noodzakelijke informatie op eerste verzoek.

Artikel 10 Geheimhouding

10.1 Partijen nemen in relatie tot het MedMij Afsprakenstelsel strikte geheimhouding in acht voor zover het vertrouwelijke informatie betreft of informatie waarvan men het vertrouwelijk karakter redelijkerwijs kan vermoeden, tenzij een wettelijke plicht of een rechterlijke uitspraak openbaarmaking van deze gegevens gebiedt.

Artikel 11 Intellectueel eigendom

11.1 Alle intellectuele eigendom voor alle soorten zaken die worden ontwikkeld door, voor of namens de Stichting MedMij, zoals bijdragen aan Request For Changes (RFC'S) en/of overige documentatie die bijdragen aan de ontwikkeling van de afspraken binnen het MedMij Afsprakenstelsel en die via het MedMij Afsprakenstelsel openbaar worden gemaakt, komen toe aan Stichting MedMij.

11.2 Alle auteursrechten die door de Deelnemer kunnen worden uitgeoefend voor alle soorten zaken die worden ontwikkeld door, voor of namens de Stichting MedMij, waar en wanneer dan ook, zoals bijdragen aan Request For Changes (RFC'S) en/of overige documentatie die via het MedMij Afsprakenstelsel openbaar worden, berusten bij de Stichting MedMij. Deze intellectuele eigendomsrechten worden op grond van deze Overeenkomst door Deelnemer om niet aan de Stichting MedMij overgedragen, welke overdracht door Stichting MedMij wordt aanvaard.

11.3 De Deelnemer doet hierbij afstand jegens de Stichting MedMij voor zover van toepassing op bijdragen aan de ontwikkeling van de afspraken binnen het MedMij Afsprakenstelsel zoals bedoeld in artikel 11.1, alsmede van alle eventueel aan hem toekomende persoonlijkheidsrechten als bedoeld in de Auteurswet en voor zover de toepasselijke regelgeving zodanige afstand toelaat. Deelnemer doet dit ook namens eventueel aan zijn zijde betrokken personeelsleden afstand jegens de Stichting MedMij van alle eventueel aan deze personeelsleden toekomende persoonlijkheidsrechten, in de mate waarin de toepasselijke regelgeving zodanige afstand toelaat.

11.4 De Deelnemer heeft het niet-exclusieve en niet-overdraagbare recht om, gedurende de looptijd van deze Overeenkomst, het Merk te gebruiken in verband met het aanbieden van Diensten, in overeenstemming met deze Overeenkomst en de daaruit voortvloeiende voorschriften.

11.5 De Deelnemer zal niets doen dan wel nalaten waardoor de rechten van de Stichting MedMij ten aanzien van het Merk kunnen worden aangetast en/of de ter zake van het Merk opgebouwde goodwill negatief zou kunnen worden beïnvloed en zal op geen enkele wijze, direct dan wel indirect schade toebrengen aan het Merk zoals, maar niet beperkt tot, het niet voldoen aan de privacy- en beveiligingseisen.

Artikel 12 Overdraagbaarheid rechten en verplichtingen overeenkomst

12.1 Partijen zijn niet bevoegd hun rechten en verplichtingen uit de Overeenkomst over te dragen aan een derde, behalve na schriftelijke toestemming van de wederpartij.

12.2 In het geval de Deelnemer zijn rechten en plichten uit de Overeenkomst wil overdragen, dient de overnemende partij eveneens toegelaten te zijn tot het MedMij Afsprakenstelsel in de rol van Dienstverlener zorgaanbieder.

Artikel 13 Geschillen en toepasselijk recht

13.1 Partijen proberen ieder geschil naar aanleiding van deze Overeenkomst eerst in onderling overleg op te lossen. Indien Partijen het geschil ter zake van deze Overeenkomst niet in onderling overleg kunnen

oplossen, zal het geschil worden voorgelegd aan de ter zake bevoegde rechter te Utrecht, tenzij Partijen zelf alsnog minitrial, bindend advies, arbitrage of andere vormen van alternatieve geschillenbeslechting overeenkomen.

13.2 Op deze Overeenkomst, de uitvoering van deze Overeenkomst en op alle geschillen die daaruit mochten voortvloeien is Nederlands recht van toepassing.

Artikel 14 Overig

14.1 Deze Overeenkomst komt in de plaats van en vervangt alle eerdere overeenkomsten en/of bindende afspraken tussen Partijen in relatie tot het MedMij Afsprakenstelsel.

14.2 De Deelnemer is in de Europese Unie ingeschreven in een door het betreffende lidstaat van vestiging erkend handelsregister.

14.3 In het geval de Deelnemer van juridische status verandert en daarmee mogelijk niet meer aan de toetredingseisen voldoet, dient de Deelnemer deze wijziging schriftelijk te melden aan de Stichting MedMij. Te denken valt aan overname door een onderneming buiten Nederland of de EU, fusie of splitsing en faillissement. In het geval van wijziging van de juridische status behoudt de Stichting Medmij het recht de Overeenkomst te beëindigen en/of de Deelnemer te vragen opnieuw de Toetredingsprocedure te doorlopen.

Aldus overeengekomen in tweevoud,

Namens MedMij Naam: Functie: Datum: Plaats:	Namens de Deelnemer Naam: Functie: Datum: Plaats:
<Handtekening Stichting MedMij	<Handtekening deelnemer>

Toetreding

Toetreding beschrijft de afspraken rondom toetreding tot het MedMij Afsprakenstelsel. Hierbij beschrijft het Toetredingsbeleid de belangrijkste kaders en het Toetredingsproces de processtappen. De Zelfverklaring integriteit en Intentieverklaringen zijn documenten die in het toetredingsproces worden gebruikt.

Toetredingsbeleid

> Toetredingsbeleid is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moet deze pagina herzien worden. Er moet dan een generieke tekst geschreven worden, of per domein wordt een tekst opgesteld.

> Het toetredingsbeleid beschrijft de belangrijkste kaders waarbinnen de toetreding tot het MedMij Afsprakenstelsel plaatsvindt.

Het bestuur van Stichting MedMij besluit over toetreding van deelnemers. De uitvoeringsorganisatie bereidt, met input van de aanmeldende partij, deze besluitvorming voor conform het Toetredingsproces. De uitvoeringsorganisatie ziet erop toe dat een nieuwe deelnemer, alvorens toe te treden, over juiste en volledige informatie beschikt en dat is vastgesteld of de partij aan de afspraken kan voldoen. Op basis van de verzamelde input formuleert de uitvoeringsorganisatie een advies aan het bestuur. Deelname van een nieuwe partij wordt alleen afgeraden wanneer een partij niet voldoet aan de eisen, dan wel er andere zwaarwegende motivaties zijn om deze partij niet toe te laten treden.

De uitvoeringsorganisatie toetst voorafgaand aan het toetredingsproces op de aanwezigheid van:

- De basale informatie over de potentiële deelnemer, zoals organisatie- en contactgegevens (van wettelijk vertegenwoordiger en contactpersoon voor toetreding);
- Een door de potentiële deelnemer ingevulde en ondertekende Zelfverklaring integriteit;
- Een inschrijving in een handelsregister in de EU;
- Een intentieverklaring Kandidaat-deelnemer voor de betreffende rol waarin de *Deelnemer* toetreedt.

Na een positieve beoordeling van de aangeleverde documentatie is de aanmeldende partij kandidaat-deelnemer. Tijdens het vervolg van het toetredingsproces dient de kandidaat-deelnemer erkend te worden als ontsluiter van minimaal één gegevensdienst (zie Gegevensdienstenbeleid en Testbeleid). Toetreding vindt plaats op basis van de dan verplichte release van het MedMij Afsprakenstelsel (zie Change- en releasebeleid).

Ook dient de kandidaat-deelnemer bewijs van NEN7510-certificering en de aanvullende auditverklaring, conform het Normenkader informatiebeveiliging, aan te leveren. Het toetredingsproces wordt afgerond met de ondertekening van de Deelnemersovereenkomst door de kandidaat-deelnemer en Stichting MedMij.

> In de situatie dat een kandidaat-deelnemer reeds over een geldig NEN 7510-certificaat beschikt, waarbij het MedMij Afsprakenstelsel nog geen onderdeel uitmaakt van de scope, dan kan deze worden gebruikt voor toetreding tot MedMij. Wel dient de vereiste aanvullende auditverklaring met onderbouwende rapportage van een certificerende instelling te worden aangetoond voor het Normenkader MedMij. Op het moment dat hercertificering op NEN 7510 plaatsvindt, moet het MedMij Afsprakenstelsel wel onderdeel uitmaken van de scope.

Na de toetreding levert de *Deelnemer* de informatie aan voor de *Whitelist*, *OAuthClientList* en de *Aanbiederslijst*, conform de registratieprocessen daarvoor (zie Operationele processen).

De implementatie van de afspraken en het aanleveren van de juiste informatie is de verantwoordelijkheid van de *Deelnemer*. Waar nodig en gepast kan de beheerorganisatie ondersteuning bieden door concrete problemen op te lossen, voorlichting te geven over het MedMij Afsprakenstelsel en ondersteuning te bieden in de vorm van aanvullende workshops, ketentesten en POC's.

Bij toetreding worden met de deelnemer aanvullend ook afspraken gemaakt over de rol in de governance. Zo kan een *Deelnemer* plaatsnemen in de Deelnemersraad en bij overleggen over de doorontwikkeling.

Toetredingsproces

Het toetredingsbeleid beschrijft het proces van toetreding tot het MedMij Afsprakenstelsel.

- **Doel:** Het toetredingsproces heeft als doel een gecontroleerde toetreding tot het MedMij Afsprakenstelsel mogelijk te maken.
- **Initiatie:** Deelnemer wil toetreden tot het afsprakenstelsel.
- **Afspraken over het proces:**
  - Potentiële deelnemer toont aan te voldoen aan de afspraken uit de Afsprakenset;
  - Potentiële deelnemer en Stichting MedMij bekrachtigen de toetreding door het ondertekenen van de Deelnemersovereenkomst.
- **Resultaat:** Deelnemer is toegetreden tot het afsprakenstelsel.
- **Uitzonderingen:** Deelnemer is niet toegelaten tot het stelsel, omdat niet aan alle afspraken wordt voldaan.

Zelfverklaring integriteit

Doel

Toelating van een partij waarvan de integriteit in het geding is, kan het merk en de geloofwaardigheid hiervan aantasten. Met de zelfverklaring integriteit heeft het bestuur van Stichting MedMij een instrument om bij toetreding in kaart brengen welke issues bij de potentiële deelnemer spelen op het gebied van integriteit. Met de verklaring wordt getracht integriteitskwesties van (bestuurders van) de potentiële deelnemer vroegtijdig aan het licht te krijgen. Denk bijvoorbeeld aan het niet zijn nagekomen van belangrijke wettelijke verplichtingen op het gebied van privacy en informatiebeveiliging. De aanwezigheid van integriteitskwesties kan reden zijn voor het bestuur om een deelnemer uit te sluiten voor deelname. Mocht een deelnemer bij toetreding de verklaring niet naar waarheid hebben ingevuld, dan kan dit aanleiding geven om alsnog de deelnemersovereenkomst te ontbinden.

Zie Zelfverklaring integriteit MedMij Afsprakenstelsel voor de Word-versie van de zelfverklaring.

Ondergetekende,

Bedrijf:

Naam rechtsgeldig vertegenwoordiger:

Handelsnaam:

KvK nummer:

Contactpersoon

Naam contactpersoon:

Functie:

E-mailadres:

Telefoonnummer:

Verklaart hierbij als potentiële deelnemer voor de rol waarvoor hij wenst toe te treden tot het MedMij Afsprakenstelsel dat:

I. De potentiële deelnemer zelf, of iemand die lid is van het bestuurs-, leidinggevend of toezichthoudend orgaan van de potentiële deelnemer of daarin vertegenwoordigings-, beslissings- of controlebevoegdheid heeft, niet is veroordeeld bij onherroepelijk vonnis, welk vonnis niet langer dan vijf jaar geleden is gewezen voor een veroordeling met betrekking tot:

1. deelneming aan een criminele organisatie in de zin artikel 140 Wetboek van Strafrecht (WvSr);
2. corruptie (328ter WvSr) ;
3. fraude in de zin van diefstal (310 WvSr), verduistering (321WvSr), valsheid in geschriften (225 WvSr), oplichting (326 WvSr) en bedrog bij jaarstukken (336 WvSr).

II. Op de potentiële deelnemer geen van de volgende situaties van toepassing is:

1. hij failliet is, of
2. hij in staat van insolventie of liquidatie verkeert, of
3. hij een regeling met schuldeisers heeft getroffen, of
4. hij in een andere, vergelijkbare toestand ingevolge een soortgelijke procedure uit hoofde van nationale wet- of regelgeving verkeert, bijvoorbeeld doordat de potentiële deelnemer een schuldsaneringsregeling heeft getroffen op basis van de Wet schuldsanering natuurlijke personen, of
5. zijn activa worden beheerd door een curator of door de rechtbank, of f) zijn bedrijfsactiviteiten zijn gestaakt.

III. De potentiële deelnemer zelf, of iemand die lid is van het bestuurs-, leidinggevend of toezichthoudend orgaan van de potentiële deelnemer of daarin vertegenwoordigings-, beslissings- of controlebevoegdheid zich niet schuldig heeft gemaakt aan ernstige beroepsfouten.

IV. Dat de potentiële deelnemer kan bevestigen dat hij aantoonbaar en controleerbaar voldoet aan de beginselen en verplichtingen van de Algemene Verordening Gegevensbescherming (AVG).

V. De potentiële deelnemer kan bevestigen dat:

1. hij zich niet in ernstige mate schuldig heeft gemaakt aan valse verklaringen bij het verstrekken van de informatie aangaande deze zelfverklaring, en
2. hij geen informatie heeft achtergehouden aangaande deze zelfverklaring.

Nadere toelichting door potentiële deelnemer

Indien de potentiële deelnemer één of meerdere van de bovengenoemde punten niet positief kan bevestigen, graag hieronder per onderwerp een toelichting opnemen met daarbij een duidelijke omschrijving van:

1. wat thans precies de concrete situatie is, en
2. welke acties en/of adequate maatregelen binnen welke tijdsperiode zijn en/of worden opgenomen, en
3. de redenen waarom de potentiële deelnemer desondanks een betrouwbare partij is, en
4. waarom Stichting MedMij wel zou moeten besluiten om potentiële deelnemer als deelnemer toe te laten tot toelating tot het MedMij Afsprakenstelsel.

Onderwerp[1]	Toelichting acties en maatregelen
1.	1. ..... 2. ..... 3. ..... 4. .....
2.	

Tot slot

Ondergetekende verklaart desgevraagd en onverwijld de eventuele bewijsstukken - in het kader van bewijsvoering van deze zelfverklaring en de besluitvorming over de toetreding als deelnemer tot het MedMij Afsprakenstelsel - op eerste verzoek van de Stichting MedMij te kunnen overleggen.

Datum: Plaats: Functie Naam:
<Handtekening deelnemer>[2]

Noot

1. Opnemen onderwerp dat niet positief kan worden bevestigd.

2. Ondertekening dient plaats te vinden door een bevoegd vertegenwoordiger van de rechtspersoon. Dat kan zijn de statutair bestuurder van de rechtspersoon of een gevolmachtigde, in dat geval moet een kopie van een volmacht worden bijgevoegd. Indien dit document afgedrukt meerdere pagina's bestrijkt, graag alle voorliggende pagina's paraferen.

Intentieverklaringen

De Intentieverklaringen expliciteert de verwachtingen die de kandidaat-deelnemer en Stichting MedMij van elkaar mogen hebben rondom het toetredingsproces. Er is een Intentieverklaring Dienstverlener persoon en een Intentieverklaring Dienstverlener zorgaanbieder. De inhoud van de verklaring is voor beide rollen hetzelfde, de terminologie is per verklaring toegespitst op de rol.

Intentieverklaring Dienstverlener persoon

Intentieverklaring Dienstverlener persoon is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moet deze pagina herzien worden. Er moet dan een generieke tekst geschreven worden, of per domein wordt een tekst opgesteld.

De Intentieverklaring Dienstverlener persoon expliciteert de verwachtingen die de kandidaat-deelnemer voor de rol van Dienstverlener persoon en Stichting MedMij van elkaar mogen hebben rondom het toetredingsproces. Zie Voorbeeld intentieverklaring Dienstverlener Persoon voor een pdf-versie van de Intentieverklaring Dienstverlener persoon. Dit document dient als voorbeeld. De intentieverklaring wordt bij een volledige aanmelding tot kandidaat-deelnemer opgemaakt door de uitvoeringsorganisatie.

Ondergetekenden,

<< *Naam Bedrijf* >>,gevestigd en kantoorhoudende te << *Plaatsnaam, postcode en adres* >>, ten deze rechtsgeldig vertegenwoordigd door << *naam + functie* >>,

Hierna verder te noemen: ‘kandidaat-deelnemer’

Stichting MedMij, gevestigd en kantoorhoudend te << *Plaatsnaam, postcode en adres* >>, ten deze rechtsgeldig vertegenwoordigd door << *naam + functie* >>,

Hierna verder te noemen ‘Stichting MedMij’

Hierna gezamenlijk te noemen: Partijen

Overwegende dat:

1. Stichting MedMij verantwoordelijk is voor het beheer en de doorontwikkeling van het MedMij Afsprakenstelsel;
2. VZVZ Servicecentrum in opdracht van de Stichting MedMij zorgdraagt voor het beheer, de doorontwikkeling en de toetreding van partijen tot het MedMij Afsprakenstelsel;
3. Nictiz in opdracht van Stichting MedMij zorgdraagt voor de coördinatie van de informatiestandaarden waarnaar bij de gegevensdiensten in het MedMij Afsprakenstelsel wordt verwezen;
4. Stichting MedMij, in gezamenlijkheid met VZVZ Servicecentrum en Nictiz, zich inspannen kandidaat-deelnemer naar beste vermogen te ondersteunen bij het doorlopen van het toetredingsproces voor deelname aan het MedMij Afsprakenstelsel;
5. kandidaat-deelnemer kennis heeft genomen van de meest recente versie van het MedMij Afsprakenstelsel en de informatiestandaarden waarnaar bij de gegevensdiensten in het MedMij Afsprakenstelsel wordt verwezen;
6. kandidaat-deelnemer begrijpt wat deelname aan het MedMij Afsprakenstelsel betekent;
7. kandidaat-deelnemer zelf verantwoordelijk is voor de implementatie van het MedMij Afsprakenstelsel voor de rol waarvoor hij toetreedt;
8. kandidaat-deelnemer begrijpt dat voor de gegevensdiensten die hij via het MedMij-netwerk wenst te leveren, voordat deze in productie mogen worden uitgewisseld - als onderdeel van het toetredingsproces van het MedMij Afsprakenstelsel - eerst met succes een toets moet worden

afgelegd op de inhoud van de informatiestandaard (kwalificatie) en op de uitwisseling van de gegevensdienst (acceptatie);
9. kandidaat-deelnemer begrijpt dat het MedMij Afsprakenstelsel op het moment van ondertekening van deze Intentieverklaring nog in ontwikkeling is en dat de kwalificatie op de inhoud en de acceptatie op de uitwisseling zoals genoemd in Overweging VIII. alleen kan worden ontvangen op basis van de formele release van het MedMij Afsprakenstelsel;
10. kandidaat-deelnemer begrijpt dat de release van het MedMij Afsprakenstelsel zoals gepubliceerd op het moment van ondertekening van deze Intentieverklaring niet de formele release van het MedMij Afsprakenstelsel is, maar juist is bedoeld ter voorbereiding op toetreding tot de formele release van het MedMij Afsprakenstelsel.
11. kandidaat-deelnemer alleen wordt toegestaan een rol in het MedMij-netwerk te vervullen indien zij daartoe een Deelnemersovereenkomst met de Stichting MedMij heeft afgesloten;

Verklaren als volgt:

Artikel 1 Onderwerp

1.1 Kandidaat-deelnemer wenst toe te treden als Deelnemer van het MedMij Afsprakenstelsel in de rol van Dienstverlener persoon.

1.2 Kandidaat-deelnemer gegevensdiensten levert zoals gedefinieerd in het MedMij Afsprakenstelsel.

1.3 De in artikel 1.2 bedoelde gegevensdiensten, als onderdeel van het toetredingsproces van het MedMij Afsprakenstelsel, worden gekwalificeerd op de inhoud van de informatiestandaard en worden geaccepteerd op de uitwisseling overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

1.4 Kandidaat-deelnemer een inspanningsverplichting heeft een kwalificatie op de informatiestandaarden zoals opgenomen in het MedMij Afsprakenstelsel via Nictiz te behalen.

1.5 Kandidaat-deelnemer een inspanningsverplichting heeft een acceptatie op de uitwisseling overeenkomstig het bepaalde in het MedMij Afsprakenstelsel via VZVZ Servicecentrum te behalen.

1.6 Kandidaat-deelnemer in het bezit komt van de benodigde NEN 7510-certificering overeenkomstig het bepaalde in het MedMij Afsprakenstelsel, alsmede van de aanvullende auditverklaringen als bedoeld in het Normenkader informatiebeveiliging van het MedMij Afsprakenstelsel.

1.7 Stichting MedMij zorgdraagt voor de volledigheid van de benodigde documentatie en de toegankelijkheid van de laatst geldende versie van het MedMij Afsprakenstelsel opdat kandidaat -deelnemer opvolging kan geven aan de artikelen 1.2, 1,3, 1.4, 1.5 en 1.6 van deze Intentieverklaring.

1.8 Stichting MedMij zich inspant om kandidaat-deelnemer waar mogelijk in het toetredingsproces te ondersteunen.

1.9 Stichting MedMij zorgdraagt voor duidelijke communicatie over de planning van het toetredingsproces.

1.10 Partijen bereid zijn om aan het eind van het succesvol doorlopen van het toetredingsproces de Deelnemersovereenkomst Dienstverlener persoon te sluiten.

Artikel 2 Contactpersoon en rapportage

2.1 Partijen wijzen een contactpersoon aan die als primair aanspreekpunt fungeert voor de tenuitvoerlegging van deze Intentieverklaring.

2.2 De in artikel 2.1 genoemde contactpersonen hebben tot taak de contacten over de (wijze van) uitvoering van de Intentieverklaring te coördineren en te onderhouden.

2.3 In het geval de voortgang van de werkzaamheden bij één van de Partijen vertraging dreigt te ondervinden, stellen de contactpersonen elkaar hiervan zo spoedig mogelijk op de hoogte, alsmede wat de oorzaak van de vertraging is en wat de consequenties van de vertraging zijn.

Artikel 3 Communicatie

3.1 Partijen zullen persberichten aangaande de toetreding tot het MedMij Afsprakenstelsel met elkaar afstemmen en berichten pas naar buiten brengen nadat beide Partijen met het persbericht hebben ingestemd.

Artikel 4 Geheimhouding

4.1 Partijen zullen zich ervoor inspannen dat informatie welke hen in het kader van deze Intentieverklaring bereikt en waarvan zij weten althans behoren te weten dat deze informatie een vertrouwelijk karakter heeft, niet aan derden bekend wordt, anders dan na schriftelijke toestemming van de wederpartij. Partijen zullen de in dit artikel bedoelde informatie binnen hun organisatie niet in ruimere kring verspreiden dan ten behoeve van deze Intentieverklaring noodzakelijk is en zullen aan eventueel in te schakelen derden een geheimhoudingsverplichting opleggen. Deze bepaling geldt niet voor zover Partijen wettelijk verplicht zijn bedoelde informatie aan een derde ter beschikking te stellen en evenmin voor wat betreft gegevens die aan hen ten tijde van het ter beschikking stellen reeds uit andere hoofde op rechtmatige wijze ter kennis is gekomen.

Artikel 5 Inwerkingtreding en duur

5.1 Deze Intentieverklaring treedt inwerking onmiddellijk na ondertekening en eindigt met de ondertekening van de Deelnemersovereenkomst Dienstverlenerpersoon tussen Partijen.

5.2 De intentieverklaring is niet in rechte afdwingbaar met uitzondering van de in artikel 4 opgenomen geheimhoudingsbepaling.

Aldus verklaard in tweevoud

Namens Stichting MedMij:

Datum:	
Plaats:	
Functie:	
Naam:	
Handtekening:	

Namens de kandidaat-deelnemer:

Datum:	
Plaats:	
Functie:	
Naam:	
Handtekening:	

Intentieverklaring Dienstverlener zorgaanbieder

Intentieverklaring Dienstverlener zorgaanbieder is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moet deze pagina herzien worden. Er moet dan een generieke tekst geschreven worden, of per domein wordt een tekst opgesteld.

De Intentieverklaring Dienstverlener zorgaanbieder expliciteert de verwachtingen die de kandidaat-deelnemer voor de rol van Dienstverlener zorgaanbieder en Stichting MedMij van elkaar mogen hebben rondom het toetredingsproces. Zie Voorbeeld intentieverklaring Dienstverlener zorgaanbieder voor een pdf-versie van de Intentieverklaring Dienstverlener zorgaanbieder. Dit document dient als voorbeeld. De intentieverklaring wordt bij een volledige aanmelding tot kandidaat-deelnemer opgemaakt door de uitvoeringsorganisatie.

Ondergetekenden,

<< *Naam Bedrijf* >>,gevestigd en kantoorhoudende te << *Plaatsnaam, postcode en adres* >>, ten deze rechtsgeldig vertegenwoordigd door << *naam + functie* >>,

Hierna verder te noemen: ‘kandidaat-deelnemer’

Stichting MedMij, gevestigd en kantoorhoudend te << *Plaatsnaam, postcode en adres* >>, ten deze rechtsgeldig vertegenwoordigd door << *naam + functie* >>,

Hierna verder te noemen ‘Stichting MedMij’

Hierna gezamenlijk te noemen: Partijen

Overwegende dat:

1. Stichting MedMij verantwoordelijk is voor het beheer en de doorontwikkeling van het MedMij Afsprakenstelsel;
2. VZVZ Servicecentrum in opdracht van de Stichting MedMij zorgdraagt voor het beheer, de doorontwikkeling en de toetreding van partijen tot het MedMij Afsprakenstelsel;
3. Nictiz in opdracht van Stichting MedMij zorgdraagt voor de coördinatie van de informatiestandaarden waarnaar bij de gegevensdiensten in het MedMij Afsprakenstelsel wordt verwezen;
4. Stichting MedMij, in gezamenlijkheid met VZVZ Servicecentrum en Nictiz, zich inspannen kandidaat-deelnemer naar beste vermogen te ondersteunen bij het doorlopen van het toetredingsproces voor deelname aan het MedMij Afsprakenstelsel;
5. kandidaat-deelnemer kennis heeft genomen van de meest recente versie van het MedMij Afsprakenstelsel en de informatiestandaarden waarnaar bij de gegevensdiensten in het MedMij Afsprakenstelsel wordt verwezen;
6. kandidaat-deelnemer begrijpt wat deelname aan het MedMij Afsprakenstelsel betekent;
7. kandidaat-deelnemer zelf verantwoordelijk is voor de implementatie van het MedMij Afsprakenstelsel voor de rol waarvoor hij toetreedt;
8. kandidaat-deelnemer begrijpt dat voor de gegevensdiensten die hij via het MedMij-netwerk wenst te leveren, voordat deze in productie mogen worden uitgewisseld - als onderdeel van het

toetredingsproces van het MedMij Afsprakenstelsel - eerst met succes een toets moet worden afgelegd op de inhoud van de informatiestandaard (kwalificatie) en op de uitwisseling van de gegevensdienst (acceptatie);

9. kandidaat-deelnemer begrijpt dat het MedMij Afsprakenstelsel op het moment van ondertekening van deze Intentieverklaring nog in ontwikkeling is en dat de kwalificatie op de inhoud en de acceptatie op de uitwisseling zoals genoemd in Overweging VIII. alleen kan worden ontvangen op basis van de formele release van het MedMij Afsprakenstelsel;
10. kandidaat-deelnemer begrijpt dat de release van het MedMij Afsprakenstelsel zoals gepubliceerd op het moment van ondertekening van deze Intentieverklaring niet de formele release van het MedMij Afsprakenstelsel is, maar juist is bedoeld ter voorbereiding op toetreding tot de formele release van het MedMij Afsprakenstelsel.
11. kandidaat-deelnemer alleen wordt toegestaan een rol in het MedMij-netwerk te vervullen indien zij daartoe een Deelnemersovereenkomst met de Stichting MedMij heeft afgesloten;

Verklaren als volgt:

Artikel 1 Onderwerp

1.1 Kandidaat-deelnemer wenst toe te treden als Deelnemer van het MedMij Afsprakenstelsel in de rol van Dienstverlener zorgaanbieder.

1.2 Kandidaat-deelnemer gegevensdiensten levert zoals gedefinieerd in het MedMij Afsprakenstelsel.

1.3 De in artikel 1.2 bedoelde gegevensdiensten, als onderdeel van het toetredingsproces van het MedMij Afsprakenstelsel, worden gekwalificeerd op de inhoud van de informatiestandaard en worden geaccepteerd op de uitwisseling overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

1.4 Kandidaat-deelnemer een inspanningsverplichting heeft een kwalificatie op de informatiestandaarden zoals opgenomen in het MedMij Afsprakenstelsel via Nictiz te behalen.

1.5 Kandidaat-deelnemer een inspanningsverplichting heeft een acceptatie op de uitwisseling overeenkomstig het bepaalde in het MedMij Afsprakenstelsel via VZVZ Servicecentrum te behalen.

1.6 Kandidaat-deelnemer in het bezit komt van de benodigde NEN 7510-certificering overeenkomstig het bepaalde in het MedMij Afsprakenstelsel, alsmede van de aanvullende auditverklaringen als bedoeld in het Normenkader informatiebeveiliging van het MedMij Afsprakenstelsel.

1.7 Stichting MedMij zorgdraagt voor de volledigheid van de benodigde documentatie en de toegankelijkheid van de laatst geldende versie van het MedMij Afsprakenstelsel opdat kandidaat -deelnemer opvolging kan geven aan de artikelen 1.2, 1,3, 1.4, 1.5 en 1.6 van deze Intentieverklaring.

1.8 Stichting MedMij zich inspant om kandidaat-deelnemer waar mogelijk in het toetredingsproces te ondersteunen.

1.9 Stichting MedMij zorgdraagt voor duidelijke communicatie over de planning van het toetredingsproces.

1.10 Partijen bereid zijn om aan het eind van het succesvol doorlopen van het toetredingsproces de Deelnemersovereenkomst Dienstverlener zorgaanbieder te sluiten.

Artikel 2 Contactpersoon en rapportage

2.1 Partijen wijzen een contactpersoon aan die als primair aanspreekpunt fungeert voor de tenuitvoerlegging van deze Intentieverklaring.

2.2 De in artikel 2.1 genoemde contactpersonen hebben tot taak de contacten over de (wijze van) uitvoering van de Intentieverklaring te coördineren en te onderhouden.

2.3 In het geval de voortgang van de werkzaamheden bij één van de Partijen vertraging dreigt te ondervinden, stellen de contactpersonen elkaar hiervan zo spoedig mogelijk op de hoogte, alsmede wat de oorzaak van de vertraging is en wat de consequenties van de vertraging zijn.

Artikel 3 Communicatie

3.1 Partijen zullen persberichten aangaande de toetreding tot het MedMij Afsprakenstelsel met elkaar afstemmen en berichten pas naar buiten brengen nadat beide Partijen met het persbericht hebben ingestemd.

Artikel 4 Geheimhouding

4.1 Partijen zullen zich ervoor inspannen dat informatie welke hen in het kader van deze Intentieverklaring bereikt en waarvan zij weten althans behoren te weten dat deze informatie een vertrouwelijk karakter heeft, niet aan derden bekend wordt, anders dan na schriftelijke toestemming van de wederpartij. Partijen zullen de in dit artikel bedoelde informatie binnen hun organisatie niet in ruimere kring verspreiden dan ten behoeve van deze Intentieverklaring noodzakelijk is en zullen aan eventueel in te schakelen derden een geheimhoudingsverplichting opleggen. Deze bepaling geldt niet voor zover Partijen wettelijk verplicht zijn bedoelde informatie aan een derde ter beschikking te stellen en evenmin voor wat betreft gegevens die aan hen ten tijde van het ter beschikking stellen reeds uit andere hoofde op rechtmatige wijze ter kennis is gekomen.

Artikel 5 Inwerkingtreding en duur

5.1 Deze Intentieverklaring treedt inwerking onmiddellijk na ondertekening en eindigt met de ondertekening van de Deelnemersovereenkomst Dienstverlener zorgaanbieder tussen Partijen.

5.2 De intentieverklaring is niet in rechte afdwingbaar met uitzondering van de in artikel 4 opgenomen geheimhoudingsbepaling.

Aldus verklaard in tweevoud

Namens Stichting MedMij:

Datum:	
Plaats:	
Functie:	
Naam:	

Handtekening:	

Namens de kandidaat-deelnemer:

Datum:	
Plaats:	
Functie:	
Naam:	
Handtekening:	

Governance

Het MedMij Afsprakenstelsel is een ‘levende’ set van afspraken. De zorg en IT zijn en blijven in beweging en de afspraken moeten hierbij blijven aansluiten. Ook zijn de afspraken voor deelnemers aan het stelsel niet vrijblijvend. Er moet daarom toe worden gezien op naleving van de afspraken. Dit vraagt om goed beheer en regie op de afspraken, ofwel de inrichting van governance op het afsprakenstelsel.

Hoewel er vele definities bestaan van governance kan het worden omschreven als (een reeks van) processen (tradities, beleid of regels) die formeel en/of informeel worden toegepast om verantwoordelijkheden tussen actoren van een bepaald systeem te verdelen. Governance gaat daarmee over actoren, relaties en de manier waarop een gezamenlijk doel wordt bereikt. De governance omschrijft op welke wijze de afspraken worden beheerd, welke rollen daarin te onderkennen zijn en door welke partijen die rollen worden vervuld.

Een goede inrichting van de governance draagt bij aan het vertrouwen in het stelsel. Hierbij zijn verschillende aspecten van belang. Een goede governance:

- Ziet toe op en draagt bij aan de realisatie van het hogere maatschappelijk doel, namelijk de persoon meer regie geven over de gezondheid door grip de eigen gezondheidsgegevens;
- Brengt vertegenwoordiging van de betrokken partijen in gesprek met elkaar zodat zij samen sturing kunnen geven aan het afsprakenstelsel;
- Legt taken, bevoegdheden en verantwoordelijkheden duidelijk en transparant vast;
- Legt duidelijk vast wat wel en wat niet onder verantwoordelijkheid van de governance valt;
- Borgt het publiek belang van het stelsel als geheel;
- Is slagvaardig op ieder niveau van besturing door voldoende ruimte voor besluitvorming en initiatief /innovatie;
- Is open en gaat uit van een samenwerkingsmodel. De overlegstructuur is transparant, toekomstvast en schaalbaar en kent een werkbare vorm door afvaardiging met mandaat;
- Is in overeenstemming met de mededingings- en andere wetgeving. Dienstverleners kunnen op grond van objectieve criteria en processen tot het stelsel toetreden;
- Borgt onafhankelijkheid en transparantie bij toetreding, sanctiebeleid en geschillenbeslechting, en heeft controles en toezicht goed en onafhankelijk georganiseerd;
- Is klaar voor het opvangen en oplossen van toekomstige beveiligingsincidenten en andere calamiteiten;
- Zorgt dat afspraken aan blijven sluiten bij de praktijk en nageleefd kunnen worden;
- Zorgt voor duidelijke regie op het stelsel (onder andere bij aansluiting op het stelsel, kwalificaties, toezicht en handhaving, etc.);
- Is begrijpelijk en transparant voor alle stakeholders;
- Regelt waar nodig en waar haalbaar middelen om gemeenschappelijke doelstellingen te behalen.

De keuzes op deze aspecten worden geleid door een viertal criteria:

1. **Vertrouwd.** Het belangrijkste criterium is dat de governance van het Afsprakenstelsel vertrouwen moet opwekken bij alle betrokkenen bij het stelsel. Personen moeten voldoende vertrouwen hebben in de uitwisseling van gegevens om voor elkaar te krijgen dat zij gebruik maken van PGO’s, aanbieders moeten hun gegevens beschikbaar durven stellen via MedMij en IT-leveranciers moeten deel willen nemen aan het stelsel.
2. **Doelgericht en doelmatig.** De besturingsstructuur moet helpen het doel van het Afsprakenstelsel MedMij op een zo efficiënt en effectief mogelijke manier te bereiken. Daarvoor moet de governance doelmatig zijn, ‘lean and mean’ en slagvaardig.
3. **Draagvlak.** De besturingsstructuur moet voldoende draagvlak hebben om legitiem te zijn en zijn taken goed te kunnen uitvoeren. Het is daarom belangrijk dat de governance structuur gedragen wordt door de verschillende stakeholders, en dat de structuur rekening houdt met de verhoudingen zoals ze nu zijn en kan meeveranderen naar behoefte.

4. **Omgevingsbewust.** Er zijn veel aanpalende ontwikkelingen die effect kunnen hebben op het Afsprakenstelsel of waar de verdere ontwikkeling van afhankelijk is. Om deze afhankelijkheden te ondervangen moet in de governance worden stilgestaan bij responsiviteit, de mate waarin kan worden geanticipeerd op ontwikkelingen en innovaties mogelijk kunnen worden gemaakt. Ketenproblemen moeten worden geïdentificeerd en tevens duidelijk en kloppend zijn.

Naast het afsprakenstelsel, levert het programma MedMij ook profielen bij bestaande informatiestandaarden en een financieringsstelsel op. Het beheer van deze producten, plus de activiteiten die ondernomen worden om MedMij van de grond te krijgen, moeten uiteindelijk ook ergens landen. Voor de informatiestandaarden geldt dat het afsprakenstelsel hier alleen naar verwijst en dat het beheer bij andere partijen is belegd (bijvoorbeeld bij Nictiz, Zorginstituut Nederland, etc.). Voor het financieringsstelsel geldt dat zij waarschijnlijk moet landen in de governance van de financierende partij(en). Van de stimulerende activiteiten om MedMij van de grond te krijgen, moet verder nog worden bepaald óf en waar deze moeten worden belegd.

De governance wordt in de documentatie nader uitgewerkt aan de hand van de volgende onderwerpen:

- Rollen: welke rollen zijn te onderkennen binnen de governance en welke partijen vullen deze rollen in?
- Inrichting: hoe ziet met deze rollen de inrichting van de governance eruit en welke verantwoordelijkheden hebben zij hierbinnen?
- Statuten Stichting MedMij: de formele vertaling van de rollen en inrichting in statuten voor de rechtspersoon Stichting MedMij.

Rollen

Rollen beschrijft de rollen die binnen de governance te onderkennen zijn en welke partijen deze rollen invullen.

Binnen de governance worden zes rollen onderscheiden, namelijk:

- **Deelnemer:** een partij die dienstverlening aanbiedt binnen het MedMij Afsprakenstelsel;
- **Gebruiker:** een partij die gebruik maakt van dienstverlening van deelnemers aan het afsprakenstelsel;
- **Eigenaar:** een partij die eindverantwoordelijk is voor het stelsel en de strategische kaders;
- **Financier:** een partij die het beheer van het stelsel financiert;
- **Beheerder:** een partij verantwoordelijk voor het beheer van het afsprakenstelsel;
- **Toezichthouder:** een partij die toeziet op het handelen binnen wet- en regelgeving;

Een groot aantal partijen hebben belang bij het bestaan van het afsprakenstelsel en kunnen in meer of mindere mate deze rollen invullen:

- Individuele personen, met als specifieke doelgroep patiënten
- Vertegenwoordiging van patiënten
- Zorgaanbieders, waaronder huisartsen, ziekenhuizen, verpleeghuizen en andere partijen die omwille van hun professie gegevens over jouw gezondheid bijhouden;
- Rijksoverheid
- Gemeenten
- PGO-leveranciers
- XIS-leveranciers
- Andere ICT-dienstverleners (integrators, infrastructuurpartijen, etc.)
- Zorgverzekeraars
- Standaardisatie-instituten
- Certificerings- en auditbureaus

Hieronder wordt beargumenteerd welke rol MedMij ziet voor deze partijen binnen de governance van het stelsel.

Deelnemer

Een deelnemer biedt diensten aan binnen het MedMij Afsprakenstelsel vanuit de rol van Dienstverlener persoon en/of Dienstverlener aanbieder. Zie Opzet voor meer informatie over de rol van dienstverlener in het stelsel. Partijen die de rol van deelnemer kunnen invullen zijn XIS-, PGO-leveranciers en andere IT-dienstverleners in de zorg. Ook aanbieders, die eigen IT-systemen ontwikkelen en hiermee willen toetreden tot het stelsel, acteren als deelnemer.

Deelnemer MedMij Afsprakenstelsel

XIS-, PGO-leveranciers en andere IT-dienstverleners in de zorg.

Gebruiker

Een gebruiker neemt diensten af van deelnemers aan het MedMij afsprakenstelsel. Onder gebruikers verstaan we patiënten en aanbieders, maar ook PGO- en XIS-leveranciers die bij de ontsluiting van gegevens richting MedMij ontlast worden door deelnemers aan het stelsel. Zie Opzet voor meer informatie over de rol van gebruiker in het stelsel.

Gebruiker MedMij Afsprakenstelsel

Patiënten, aanbieders, PGO- en XIS-leveranciers.

Eigenaar

Een eigenaar is eindverantwoordelijk voor het stelsel en bepaalt de strategische koers. Het gaat dan om verantwoordelijkheid voor het grotere geheel en niet om verantwoordelijkheid voor individuele dienstverlening (deze ligt bij deelnemers zelf). Kijkend naar de lijst van betrokken actoren is er een bijna onuitputtelijke lijst van mogelijke combinaties van eigenaren te benoemen. Echter een groot deel lijkt al bij voorbaat af te vallen, zeker als we kijken naar het doel van MedMij en hoe partijen participeren. De doelstelling van MedMij maakt het bijna vanzelfsprekend dat in ieder geval patiënten en aanbieders optreden als eigenaar. Immers, zij zijn de voornaamste belanghebbenden en zullen vanuit dat belang stevige invloed willen kunnen uitoefenen op het blijvend functioneren van het afsprakenstelsel.

Achter het belang van patiënten en aanbieders gaat een forse marktpotentie schuil voor de deelnemers aan het stelsel. Vanuit die potentie zouden ook zij wellicht eigenaar willen zijn van het stelsel. Zeker ook omdat zij uiteindelijk moeten voldoen aan de afspraken. Een wezenlijke vraag die speelt is of deelnemers ook tegelijkertijd eigenaar zouden mogen zijn. Kijken we naar bestaande afsprakenstelsels zoals iDEAL, GSM en eHerkenning, dan lijkt dat gebruikelijk. Gelet op de doelstelling van MedMij, het belang om de patiënt centraal te stellen, alsook op termijn het afsprakenstelsel te verbreden naar andere sectoren omdat gezondheid geen monopolie is van zorg, alsmede de belangenverstrengeling die dan kan ontstaan tussen het ‘doel’ waar de eigenaren zich hard voor maken en de ‘middelen’ die van de deelnemers komen, is het wenselijk om de rollen waar mogelijk gescheiden te houden. Dit leidt dan tot de afweging dat deelnemers, lees: de ICT-leveranciers in de zorg, geen eigenaarschap inzake MedMij op zich kunnen nemen. Zij krijgen wel, vanwege het grote belang van deze partijen bij de uitvoering, een (andere) rol in de besturing.

De overheid is belanghebbende, maar gelet op haar meer afstandelijke positie met betrekking tot de zorgsector ligt (mede-)eigenaarschap wat minder voor de hand. De zorgverzekeraars hebben wellicht wel een voorkeur om als eigenaar deel te nemen in MedMij, te meer omdat verdergaande digitalisering in de zorg, en dan met name in het primaire zorgproces (eHealth toepassingen) kunnen bijdragen aan de efficiency en kwaliteitsverhoging van de zorg. Burgers en aanbieders zijn echter huiverig voor grote inmenging van overheid en zorgverzekeraars met betrekking tot zorginformatie. We volgen daarom het advies van PBLQ, dat is gegeven na een eerste verkenning van de governance voor het afsprakenstelsel, waarin zij stellen dat deelname van zorgverzekeraars en overheid in de actieve besluitvorming potentieel minder vertrouwenwekkend is voor burgers en politiek.

De andere genoemde instanties zoals standaardisatiebureaus, certificatie- en auditbureaus zijn minder voor de hand liggend als mogelijke eigenaar, al is het wel weer mogelijk dat dergelijke bureaus in opdracht c.q. ten behoeve van MedMij werkzaamheden uitvoeren.

Eigenaar MedMij Afsprakenstelsel

Om het belang van patiënten en aanbieders blijvend te borgen, gericht op vertrouwde uitwisseling van gezondheidsgegevens, en te voorkomen dat die belangen vermengd raken met andere, kunnen alleen zij optreden als eigenaar. Een vertegenwoordiging van deze patiënten en aanbieders geeft georganiseerd sturing aan het beheer van MedMij. De organisatie waarin zij dat doen, treedt formeel op als eigenaar van het stelsel.

Financier

Een financier is verantwoordelijk voor de financiële ondersteuning van het beheer van de afspraken. Een aloude zegswijze ‘Wie betaalt, wie bepaalt’ kan bij de vraag wie optreedt als financier behulpzaam zijn. Als gekeken wordt naar de meest voor-de-hand-liggende eigenaren, patiënten en aanbieders, dan zien we dat

dit geen vermogende groepen zijn die het Afsprakenstelsel financieel kunnen trekken. Immers, patiënten c.q. burgers zijn relatief slecht georganiseerd. In onze vertegenwoordigde democratie is het daarom doorgaans de overheid die voor het belang van de burgers opkomt. Dit roept daarmee de vraag op of een eigenaar ook financier dan wel de financier ook eigenaar zou moeten zijn? Het antwoord daarop is nee. Op dit moment ondersteunt de overheid de rol van de patiënt bijvoorbeeld door de Patiëntenfederatie Nederland te subsidiëren. Dit laatste zou een wijze van financiering vanuit de overheid kunnen zijn zonder dat de overheid hoeft op te treden als (mede-)eigenaar. Op die manier bepaalt de overheid alleen of en onder welke voorwaarde de financiering wordt verstrekt, maar niet wat er op de agenda komt.

Een andere partij die, in een zelfde constructie als bij de overheid, als financier zou kunnen optreden, en ook een zeker belang heeft bij de ontwikkeling van MedMij, zijn de zorgverzekeraars. Zij hebben baat bij afspraken en een toekomstvisie die in lijn ligt met het verder ontwikkelen van PGO's ten dienste van het verbeteren van de zorg en het verlagen van de kosten.

Een andere optie is om deelnemers te laten betalen voor het beheren van de afspraken. Daarmee worden deelnemers mede-eigenaar van dat Afsprakenstelsel. Deze optie ligt nu minder voor de hand. Het programma MedMij is juist opgestart omdat er vanuit de markt onvoldoende initiatief ontstond om op non-concurrentiele basis interoperabiliteitsafspraken te maken. ICT-leveranciers hebben dan ook niet direct profijt van hun investering in het beheer. Indien zij optreden als financier zullen zij daarnaast ook als eigenaar invloed willen uitoefenen, waarmee zij direct invloed krijgen op de set van eisen waar zij zelf aan moeten voldoen. Een risico hierbij is dat een 'race-to-the-bottom' ontstaat doordat de deelnemers zo min mogelijk kwijt willen zijn aan het beheer van de afspraken, waardoor een goede taakuitvoering lastig wordt. Eventueel is het mogelijk om in de toekomst nadat de markt verder is ontwikkeld de deelnemers een rol te laten spelen als financier.

Het voorstel is om overheid en zorgverzekeraars (tijdelijk) het beheer te laten financieren. Omdat de financiers geen eigenaar zijn van het stelsel, moeten zij bereid zijn om de financiering op zich te nemen zonder daarvoor 'zeggenschap' over de afspraken te verlangen. Zorgverzekeraars en overheid hebben via financiering van het beheer wel een rol in het stellen van randvoorwaarden en de besteding van de middelen. Deze financiering vanuit overheid en zorgverzekeraars is eindig, in die zin dat na een zekere periode heroverweging van de financiering aan de orde is.

Financier MedMij Afsprakenstelsel

De rijksoverheid en/of de zorgverzekeraars nemen voor de eerste jaren de financiering van het afsprakenstelsel MedMij (beheer) voor haar rekening. Dit geeft ruimte aan alle andere financiële vragen die nog voorliggen en benadrukt het belang van de overheid en de zorgverzekeraars om te komen tot een stelsel van afspraken als randvoorwaarde waarbinnen ICT-leveranciers in de zorg invulling kunnen aan de totstandkoming van diensten en producten die nodig zijn om gezondheidsgegevens uit te wisselen.

Beheerder

Gezien de grote belangen die rond het stelsel gaan spelen, is goed beheer een vereiste. Dit beheer moet uitgevoerd kunnen worden zonder dat hierbij verstrengeling van belangen kan ontstaan. Een toegewijde beheerorganisatie, de MedMij-beheerorganisatie, wordt daarom op- en ingericht om de eindverantwoordelijkheid over het pakket van Beheerverantwoordelijkheden rondom het beheer van het afsprakenstelsel te beleggen. Waar dit synergievoordelen oplevert, kunnen beheerverantwoordelijkheden door de MedMij-beheerorganisatie worden uitbesteed bij (een) bestaande beheerorganisatie(s). De verantwoordelijkheden krijgen in de dagelijkse praktijk vorm via processen. Niet met alle beheerprocessen hebben deelnemers direct te maken. De beheerprocessen waarin deelnemers zelf een rol spelen en de processen die zijn ingericht als dienstverlening vanuit de beheerorganisatie, staan beschreven bij Operationele processen.

Beheerder MedMij Afsprakenstelsel

De eindverantwoordelijkheid voor het pakket van verantwoordelijkheden rondom het beheer van het afsprakenstelsel wordt belegd bij een nieuw op te richten MedMij-beheerorganisatie. Waar dit synergievoordelen oplevert, kunnen beheerverantwoordelijkheden door de MedMij-beheerorganisatie worden uitbesteed aan (een) bestaande beheerorganisatie(s).

Toezichthouder

Toezicht is belangrijk om de integriteit van het stelsel te waarborgen. Het toezicht is voor MedMij tweeledig, namelijk extern en intern. Onder extern toezicht wordt allereerst het toezicht door de wettelijke toezichthouders verstaan. Omdat het afsprakenstelsel geen wettelijke basis heeft, is er geen wettelijk toezicht op het stelsel an sich. Wel is er toezicht op de deelnemers en de beheerder(s) in de uitvoering van wet- en regelgeving door deze partijen. De belangrijkste wet- en regelgeving die hierbij van toepassing is, staat genoemd in het Juridisch kader. Deelnemers en de beheerder(s) zijn door de toezichthouders zelf aanspreekbaar op hun handelen en de bevoegdheden van de wettelijke toezichthouders zijn van kracht ongeacht de afspraken in het stelsel. De MedMij-beheerorganisatie stemt af met de toezichthouders vanuit het belang van het stelsel. Hiermee wordt ervoor gezorgd dat deelnemers en beheerorganisatie bij het hanteren van de afspraken kunnen voldoen aan de geldende wet- en regelgeving.

Een tweede vorm van extern toezicht, is het toezicht door de financiers. Zij hebben een rol in het toezicht op de besteding van de middelen.

Ten slotte is er dan nog het interne toezicht. Het gaat dan om het dagelijkse toezicht op de uitvoering van afspraken in de deelnemersovereenkomst door deelnemers. De eigenaar is verantwoordelijk voor dit interne toezicht. De beheerder voert het toezicht uit.

Toezichthouder MedMij Afsprakenstelsel

Voor MedMij is sprake van wettelijk toezicht door toezichthouders, toezicht op de besteding van de middelen door de financiers en toezicht door de beheerder op het handelen van de deelnemers.

Inrichting

Inrichting beschrijft voor de Rollen de positie en verantwoordelijkheden binnen de governance.

Een goede borging, doorontwikkeling en naleving van de afspraken is cruciaal voor het vertrouwen in en de continuïteit van MedMij. Er is op dit moment (april 2018) in de zorg geen bestaande organisatie waar de eindverantwoordelijkheid over het stelsel kan worden belegd, zonder taakvertroebeling te creëren. Een toegewijde rechtspersoon, Stichting MedMij, wordt daarom ingericht om de eindverantwoordelijkheid voor het beheer van het afsprakenstelsel bij te beleggen. Deze rechtspersoon borgt het belang van het afsprakenstelsel, neemt verantwoordelijkheid voor het beheer en is eigenaar van het merk MedMij.

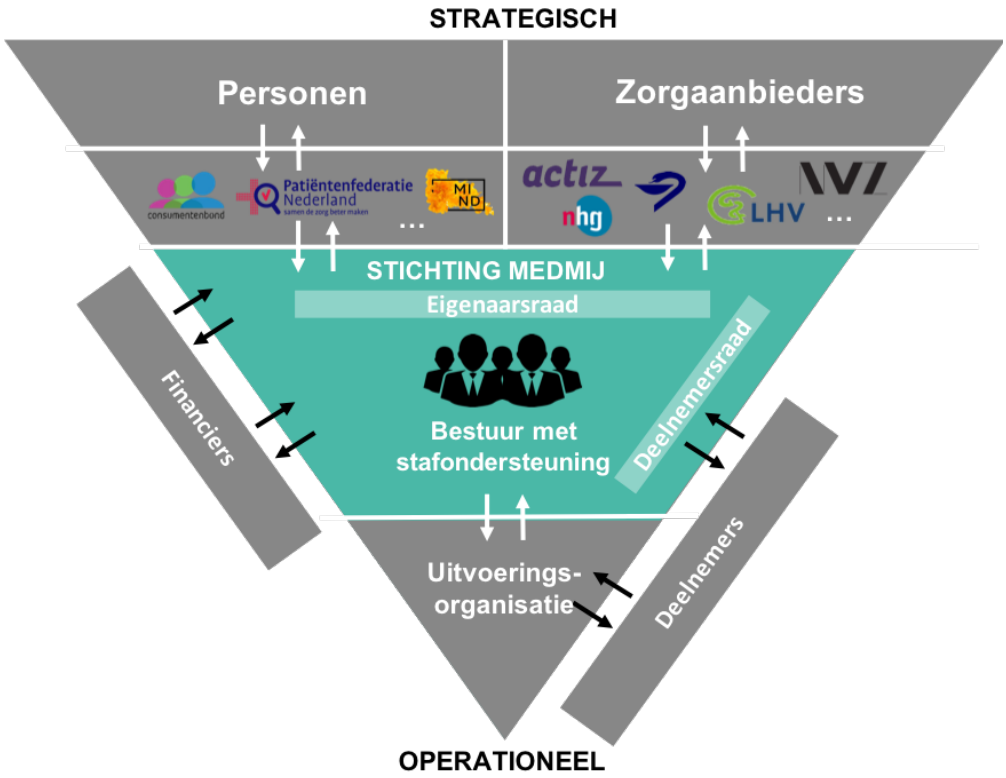
De inrichting van Stichting MedMij betekent niet dat geen hergebruik wordt gemaakt van bestaande beheerexpertise in de zorg en dat alle processen bij Stichting MedMij opnieuw worden ingericht. Een van de belangrijke uitgangspunten van het afsprakenstelsel is om zoveel mogelijk aan te sluiten bij bestaande, geaccepteerde standaarden. Met wat creativiteit kan dit uitgangspunt worden vertaald naar een uitgangspunt om, waar mogelijk en gewenst, zoveel mogelijk gebruik te maken van bestaande beheerexpertise in het veld. Na een verkenning van de mogelijkheden, is daarom gekozen om een deel van de beheertaken uit te besteden aan een gevestigde beheerder, VZVZ Servicecentrum (hierna: uitvoeringsorganisatie). De verantwoordelijkheden die echt bij Stichting MedMij moeten worden ingericht kunnen hierdoor beperkt blijven. Stichting MedMij en de uitvoeringsorganisatie vormen samen het MedMij Beheer.

Invulling rollen

De eerder gedefinieerde rollen moeten een plek krijgen in de governance:

- **Eigenaar/gebruiker:** De eigenaren en tevens gebruikers van het stelsel vormen de eigenaarsraad van Stichting MedMij.
- **Deelnemer:** Deelnemers zijn geen eigenaar van het stelsel, maar krijgen vanwege hun belangrijke rol in de uitvoering een expliciete plek in de governance in de vorm van een deelnemersraad. Deze deelnemersraad heeft een adviserende rol richting het bestuur. De deelnemersraad is onderdeel van Stichting MedMij.
- **Beheerder:** Beheerverantwoordelijkheden zijn er op verschillende niveaus. De meer strategische beheerverantwoordelijkheden gaan over de koers van MedMij en de dagelijkse regie daarop moet daarom belegd zijn bij Stichting MedMij. De meer tactische/operationele verantwoordelijkheden worden zoveel mogelijk belegd bij de uitvoeringsorganisatie.
- **Financier:** Financiers zijn geen eigenaar van het stelsel. Zij stellen wel kaders aan de financiering van het beheer via de financieringsrelatie. Hoe deze financiering eruit komt te zien, wordt nog uitgewerkt.
- **Toezichthouder:** Deelnemers en beheerders hebben zich per definitie te houden aan wet- en regelgeving. Voor het wettelijke toezicht op hun handelen conform deze wet- en regelgeving, zijn er de daartoe ingestelde instanties (zie Juridisch kader voor een overzicht van de toezichthouders). Daarnaast zijn de privaatrechtelijke afspraken uit het stelsel van kracht. De beheerorganisatie ziet toe op de naleving van de afspraken van deelnemers. De beheerder wint hierbij advies in van anderen, waaronder van een trusted third party voor controle op de toepassing van het normenkader door de deelnemer, van het Handelsregister, van Nictiz voor de kwalificatie op de informatiestandaarden, etc.

Schematisch vertaalt dit zich in het volgende governance-model, dat hieronder nader wordt uitgewerkt:



Stichting MedMij

Rechtsvorm

Bij de keuze voor een rechtsvorm is belangrijk wie eindverantwoordelijk is. Bij Rollen is beargumenteerd dat een vertegenwoordiging van patiënten en zorgaanbieders eigenaar is van het stelsel. Er moet dan ook een rechtsvorm worden gekozen waarin private partijen een rol kunnen spelen. Binnen publieke rechtsvormen, zoals een afdeling op het Ministerie van Volksgezondheid, Welzijn en Sport of een zelfstandig bestuursorgaan, kan dit eigenaarschap onvoldoende vorm krijgen.

Resteren de private rechtsvormen zonder winstoogmerk, de stichting en de vereniging. Een ‘stichting’ kenmerkt zich door snelheid en onafhankelijkheid, een vereniging (of als speciale vorm: de coöperatie) door haar legitimiteit vanwege grote inspraak van leden. In een vereniging heeft de algemene ledenvergadering het laatste woord. Hierdoor kan de besluitvorming in een vereniging veel tijd kosten. Ook de afstand van leden tot de materie komt de kwaliteit van besluitvorming vaak niet ten goede. Dat, gecombineerd met de grote fragmentatie in de zorg, maakt de kans groot dat een vereniging door te grote stroperigheid niet slagvaardig genoeg is bij het beheren en doorontwikkelen van het afsprakenstelsel. Een stichting kent dit probleem niet, omdat het bestuur eindverantwoordelijk is. Hoewel het democratisch gehalte van een vereniging groter is en er meer inspraak is van verschillende betrokkenen, kan ook in een stichting een goede relatie met het veld worden vormgegeven om de legitimiteit van de besturing te borgen. Er is daarom gekozen voor de rechtsvorm stichting.

De keuze voor de rechtsvorm stichting sluit tevens goed aan bij de wens om de rol van financier en eigenaar te scheiden. Dit kan via subsidieregelingen worden geregeld.

Doel en middelen

Stichting MedMij heeft een afgebakend doel dat in grote mate de bewegingsvrijheid van de stichting bepaalt. Stichting MedMij wordt opgericht met als doel personen meer regie te geven over hun eigen

gezondheid door gegevensuitwisseling overeenkomstig het MedMij Afsprakenstelsel mogelijk te maken en te stimuleren. De stichting tracht dit doel te bereiken door het beheren van het MedMij Afsprakenstelsel, het doorontwikkelen van het stelsel en het waarborgen van de optimale vertrouwelijkheid, veiligheid en betrouwbaarheid van de gegevensuitwisseling volgens de afspraken uit het stelsel. Stichting MedMij zet zich daarnaast ook in om het gebruik van het MedMij Afsprakenstelsel door (potentiële) deelnemers en eindgebruikers te stimuleren.

Bestuur en toezicht: bestuursmodel

Voor de besturing van de stichting kan worden gekozen tussen een bestuurs- en een raad-van-toezichtmodel. Het verschil tussen beide modellen ligt in de scheiding tussen toezicht en uitvoering. Bij een bestuursmodel liggen zowel toezicht als uitvoering in handen van het bestuur en zorgt vooral een evenwichtige invulling van het bestuur voor het onderlinge toezicht. In een raad-van-toezichtmodel zijn de verantwoordelijkheden voor toezicht en uitvoering duidelijk gescheiden.

Het is zeer gebruikelijk om bij de ontwikkeling van een stichting te beginnen met een bestuursmodel. Deze invulling past ook bij het uitgangspunt om de stichting licht te houden, het hanteren van een groeimodel en het feit dat er al min of meer toezichthoudende organen in het model zijn opgenomen in de vorm van een eigenaarsraad en de deelnemersraad. Het bestuursmodel wordt daarom als uitgangspunt genomen.

Bestuur

Doordat de eigenaren zitting nemen in de eigenaarsraad, hoeft de dagelijkse besturing geen afspiegeling te zijn van personen en zorgaanbieders. Er wordt daarom een onafhankelijk bestuur ingericht dat bestaat uit minimaal drie en maximaal vijf bestuursleden. Dit aantal mag gedurende het eerste jaar na oprichting van de stichting ook lager zijn dan drie om klein op te kunnen starten naast het programma. Het bestuur wordt voorgezeten door een voorzitter, die tevens eerste aanspreekpunt is voor de dagelijkse operatie.

Het bestuur bestaat uit meerdere bestuursleden zodat verschillende perspectieven en expertise kunnen worden ingebracht, waaronder in ieder geval het perspectief van de persoon, het perspectief van de zorgaanbieder en expertise over technische, juridische, privacy- en beveiligingsaspecten van de gegevensuitwisseling. Aanvullend dienen bestuursleden bij voorkeur te beschikken over een relevant bestuurlijk netwerk, affiniteit te hebben met de digitale uitwisseling van gezondheidsgegevens (met patiënten) en affiniteit te hebben met netwerksamenwerking en het ontwikkelen van afspraken met diverse belanghebbenden. Bestuursleden dienen daarnaast gemotiveerd zijn om als ambassadeur bij te dragen aan het succes van MedMij.

Bestuursleden treden aan voor een periode van drie jaar en kunnen eenmalig herbenoemd worden voor eenzelfde periode. Alleen in uitzonderlijke gevallen is het mogelijk hier een derde periode aan vast te plakken. Het bestuur stelt een rooster van aftreden op om ervoor te zorgen dat bestuursleden gecoördineerd aftreden en ervaring zoveel mogelijk behouden blijft. Mocht een bestuurslid niet functioneren, dan kunnen de overige in functie zijnde bestuursleden gezamenlijk besluiten om dit bestuurslid te ontslaan. De eigenaarsraad kan alleen het vertrouwen in het volledige bestuur opzeggen. In dat geval defungeren alle bestuurders en stelt de eigenaarsraad een nieuw bestuur aan.

Nieuwe bestuursleden worden voorgedragen door het bestuur in lijn met de profielschetsen zoals afgestemd tussen bestuur en eigenaarsraad. De eigenaarsraad stemt in met deze voordrachten.

Het bestuur van de stichting vergadert minimaal vier keer per jaar. Deze bestuursvergaderingen zijn niet openbaar om een vrije discussie te kunnen laten plaatsvinden. Wel wordt een verslag opgesteld dat gekuist is voor openbaarmaking. Dit verslag wordt gedeeld met de belanghebbenden. Op die manier kunnen zij de overwegingen en besluiten van het bestuur blijven volgen.

Het bestuur is eindverantwoordelijk voor het functioneren van het stelsel en neemt daarbij, op basis van voorbereidingen van de staf van de stichting, besluiten over de te hanteren strategie (visie en meerjarenkoers), deelname en uittreding van deelnemers, het optreden van de stichting en de

uitvoeringsorganisaties en het accorderen van releases en ketenwijzigingen. Het streven is om dit te doen door middel van consensus. In het geval consensus niet tot stand komt en er behoefte is aan een stemming, dan moet dit ook mogelijk zijn. Besluitvorming vindt in dat geval plaats op basis van meerderheid van stemmen. Voor de onderwerpen waarbij dat statutair is vastgelegd, betrekt het bestuur de eigenaarsraad in de besluitvorming.

Eigenaarsraad

Een eigenaarsraad wordt ingericht om het eigenaarschap van personen en aanbieders in de stichting een plek te geven. De eigenaarsraad is te vergelijken met de ledenraad van een vereniging, maar kent alleen die verantwoordelijkheden die nodig zijn om de rol van eigenaar goed te vervullen en is qua omvang beperkt. Statutair dient de eigenaarsraad goedkeuring te geven op de besluiten van het bestuur omtrent:

- Majeure aanpassingen van het MedMij Afsprakenstelsel;
- De strategische releaseplanning van het MedMij Afsprakenstelsel;
- De vaststelling van het aantal tot de stichting toe te laten eigenaars;
- De toelating van eigenaars;
- De opzegging van het eigenaarschap;
- De vaststelling van het aantal bestuurders;
- De vaststelling van de actuele profielschets voor het bestuur;
- De (her)benoeming van een bestuurder;
- De wijziging van de statuten van de stichting;
- De ontbinding van de stichting.

Personen en aanbieders zijn grote, gedifferentieerde groepen en het is onpraktisch om zelf uit deze groepen leden voor eigenaarsraad te werven. De koepels van personen en aanbieders dienen daarom als vertegenwoordiging van deze groepen. Het begrip koepel wordt ruim opgevat. MedMij gaat over een breed spectrum van de zorg, sociaal domein, preventie en gezondheid en is er zowel voor uitwisseling met zieke als gezonde personen. Een vertegenwoordiging van gezonde personen (bijvoorbeeld via de Consumentenbond en de Ouderenbond), moet ook zitting kunnen nemen in de eigenaarsraad.

De koepels nemen als rechtspersoon deel aan de eigenaarsraad. Voorafgaand aan deelname maken Stichting MedMij en de desbetreffende koepel afspraken over wie de koepel vertegenwoordigd. Vertegenwoordigers beschikken bij voorkeur over deskundigheid op het gebied van de digitale uitwisseling van gezondheidsgegevens (met patiënten) en visie op de ontwikkeling van de zorg en eHealth in de toekomst.

De eigenaarsraad bestaat uit minimaal zes en maximaal twaalf leden. Personen en aanbieders zijn samen eigenaar van het stelsel. Daarom moet altijd sprake zijn van een gelijkwaardige verdeling van zetels.

Het streven is om de besluitvorming in de eigenaarsraad te laten plaatsvinden door middel van consensus. In het geval consensus niet tot stand komt en er behoefte is aan een stemming, dan is dit ook mogelijk. Ieder lid heeft één stem en besluiten worden aangenomen bij volstrekte meerderheid van uitgebrachte stemmen. Bij staking van de stemming is het voorstel verworpen.

De eigenaarsraad vergadert minimaal één keer per jaar en wordt in de regel voorgezeten door de voorzitter van het bestuur. De vergaderingen zijn niet openbaar om een vrije discussie te kunnen laten plaatsvinden. Wel wordt een verslag opgesteld dat gekuist is voor openbaarmaking. Dit verslag wordt gedeeld met de belanghebbenden. Op die manier kunnen zij de overwegingen en besluiten blijven volgen.

Deelnemersraad

Deelnemers zijn geen eigenaar van het stelsel. Hun input is wel belangrijk om te komen tot gedragen en toekomstbestendige strategische keuzes. Zonder deze input loopt MedMij het risico dat belangrijke perspectieven, zoals economische motieven (bedrijfseconomische haalbaarheid voor aanbieders bij nieuwe functionaliteit) en het uitvoeringsbelang (technische haalbaarheid, implementeerbaarheid binnen een

bepaalde termijn, kwetsbaarheid), onvoldoende worden meegenomen in de keuzes. Binnen Stichting MedMij wordt daarom statutair een deelnemersraad ingericht. Deze deelnemersraad geeft gevraagd advies aan het bestuur op het gebied van de strategische doorontwikkeling van het MedMij Afsprakenstelsel en fungeert bovenal als klankbordgroep van het bestuur. De adviezen van de deelnemersraad zijn niet bindend. Indien het bestuur afwijkt van adviezen van de deelnemersraad, dan heeft zij een motiveringsplicht richting de raad. Een van de bestuursleden van Stichting MedMij is voorzitter van de deelnemersraad en de staf van de stichting voert het secretariaat. Er worden verslagen bijgehouden van de bijeenkomsten.

Elke deelnemer neemt als rechtspersoon deel aan de deelnemersraad. Voorafgaand aan deelname maken Stichting MedMij en de desbetreffende deelnemer afspraken over wie de deelnemer vertegenwoordigd. Vertegenwoordigers beschikken bij voorkeur over deskundigheid op het gebied van de digitale uitwisseling van gezondheidsgegevens (met patiënten) en visie op de ontwikkeling van de zorg en eHealth in de toekomst.

Naast een rol op strategisch niveau, worden deelnemers ook op tactisch/operationeel niveau door de uitvoeringsorganisatie betrokken bij de verdere ontwikkeling van het afsprakenstelsel.

Dagelijkse operatie

Binnen de kaders van het bestuur geeft de staf van Stichting MedMij op dagelijkse basis invulling aan het strategische beheer. De staf zorgt voor nadere invulling van de grote lijnen, behartigt het belang van het stelsel en waarborgt het vertrouwen van betrokken bij het stelsel. Voor een beschrijving van de beheerverantwoordelijkheden van Stichting MedMij, zie Beheerverantwoordelijkheden.

Uitvoeringsorganisatie

De uitvoeringsorganisatie geeft in opdracht van Stichting MedMij invulling aan de tactisch /operationele beheertaken. Een belangrijke taak van de uitvoeringsorganisatie is om de dagelijkse gang van zaken in het stelsel te verbinden met de strategische koers van het stelsel. Het gaat dan zowel om het vertalen van strategische besluiten naar de tactisch/operationele toepassing binnen het afsprakenstelsel, als om het ophalen van wensen bij leveranciers en deze vertalen naar adviezen voor besluitvorming. Op dagelijkse basis regelt de uitvoeringsorganisatie het beheer van de afsprakenset, de regie op toe- en uittreding van deelnemers, de regie op het afhandelen van incidenten en calamiteiten en de regie op ketenwijzigingen. De volledige opdracht is uitgewerkt in een programma van eisen. De verantwoordelijkheid voor de doorontwikkeling van de afspraken ligt begin 2018 nog bij het project Afsprakenstelsel, maar moet vanaf halverwege dat jaar ook een plek vinden bij de uitvoeringsorganisatie.

Voor een beschrijving van de beheerverantwoordelijkheden van de uitvoeringsorganisatie, zie Beheerverantwoordelijkheden.

Relatie met financiers

Om het scenario te voorkomen dat pas aan het eind van een financieringsperiode duidelijk wordt dat verwachtingen van financiers en het bestuur te ver uit elkaar lagen, is het belangrijk om gedurende het jaar (enige) betrokkenheid te organiseren. Deze betrokkenheid is onderdeel van het financieringsarrangement met de desbetreffende financier. Het bestuur heeft de vrijheid om via het financieringsarrangement met de desbetreffende financier afspraken te maken over de voorwaarden aan de financiering. Hierbij dient zij wel te waarborgen dat zij voldoende vrijheid krijgt om haar taak vanuit het belang van personen en aanbieders uit te oefenen.

Mogelijke partijen voor de financiering van het beheer van het stelsel zijn de overheid en Zorgverzekeraars Nederland. VWS heeft aangegeven geen rol te kunnen spelen in de financiering en/of governance van de beoogde stichting en zich afzijdig te houden als het gaat om besluitvorming over de inrichting van de stichting.

Relatie met het Programma MedMij

Het Programma MedMij heeft in 2018 nog een belangrijke rol bij:

- De doorontwikkeling van het afsprakenstelsel en het verwerken van de resultaten van Proves. De stuurgroep is daarmee nog verantwoordelijk voor de sturing op deze doorontwikkeling totdat de nieuwe versie van het afsprakenstelsel op advies van de stuurgroep wordt vastgesteld door de stichting en in beheer wordt gegeven bij de uitvoeringsorganisatie;
- Het inrichten van de governance en de bijkomende taken, zoals het opstellen van statuten, het werven van bestuursleden, het werven van ondersteunende staf, het regelen van duurzame financiering voor het beheer, etc.;
- Het uitvoeren van de staftaken van de stichting.

Beheerverantwoordelijkheden

De volgende beheerverantwoordelijkheden worden ingevuld door Stichting MedMij en de uitvoeringsorganisatie:

Stichting MedMij

- **Eindverantwoordelijkheid functioneren stelsel:** Het gehele beheertakenpakket dat hoort bij het in stand houden van een afsprakenstelsel vereist een vorm van aan- en besturing. Het bestuur van Stichting MedMij heeft deze eindverantwoordelijkheid. Zij dient onder andere over toekomstige afspraken en (criteria voor) toe- of uittreding te besluiten en ervoor te zorgen dat de activiteiten van alle bestuurslagen gericht blijven op het maatschappelijke doel van MedMij.
- **Besluitvorming bestuur:** Bestuursvergaderingen moeten worden voorbereid en bestuurders worden geadviseerd om de besluitvorming soepel te laten verlopen. De besluitvorming zelf moet ook georganiseerd worden.
- **Wijzigingsautoriteit:** Een belangrijk onderwerp voor besluitvorming van het bestuur zijn de nieuwe releases. Deze releases met wijzigingen aan het stelsel moeten worden goedgekeurd.
- **Visie/meerjarenplan:** Het stelsel zal mee moeten en willen ontwikkelen met de behoeften vanuit de twee grote belanghebbende partijen, de patiënten en de aanbieders, en met de steeds verder toenemende mogelijkheden die de ICT ons biedt om gezondheidsgegevens te genereren en uit te wisselen. Ook moeten ontwikkelingen in de zorg, de maatschappij en wet- en regelgeving (bijv. vanuit de EU), in de gaten worden gehouden. Het hebben van een stappenplan waar het afsprakenstelsel zich naartoe ontwikkelt, is van groot belang voor alle betrokkenen, opdat voldoende vroegtijdig daarop geanticipeerd kan worden. Het afsprakenstelsel zal zich blijven ontwikkelen, en daarmee is deze beheertaak essentieel om blijvend richting te kunnen geven aan die verdere ontwikkeling.
- **Omgevingsmanagement:** De koers van het afsprakenstelsel staat niet los van andere ontwikkelingen in het zorgveld. Het succes van het Afsprakenstelsel is afhankelijk van een aantal maatschappijbrede ontwikkelingen, zoals de ontwikkeling van betrouwbare elektronische identificatiemiddelen. Afstemming daarmee is van essentieel belang. Ook zal het afsprakenstelsel een zeker beslag gaan leggen op de capaciteit van bestaande toezichthouders zoals Autoriteit Persoonsgegevens, Inspectie Gezondheidszorg en Jeugd en de Nederlandse Zorgautoriteit. Wat precies de impact van de komst van MedMij is voor deze toezichthouders en hoe die zich ontwikkelt, is nog onbekend. Juist daarom is afstemming met hen van groot belang.
- **Financiering:** Het in stand houden van het beheer van het afsprakenstelsel kost geld. Er zal derhalve een financiële functie moeten zijn ingericht die ervoor zorg draagt dat de te maken kosten gedekt worden.
- **Risicomanagement en uitvoeren privacy- en informatiebeveiligingsbeleid:** Voor het vertrouwen in het stelsel is het noodzakelijk informatiebeveiligingsrisico's te beheersen. Doorlopend risicomanagement is dan ook onontbeerlijk. Duidelijk moet zijn welke risico's het stelsel loopt, wie deze bewaakt en wie verantwoordelijk is voor het nemen van maatregelen.
- **Aansturen uitvoeringsorganisatie:** Het programma geeft, binnen de kaders van het bestuur van Stichting MedMij, sturing aan de uitvoeringsorganisatie. Ook maakt het programma afspraken over de gehanteerde service levels.

Uitvoeringsorganisatie

- **Beheer van de afsprakenset:** De kern van het afsprakenstelsel zijn de afspraken waar deelnemers zich aan moeten houden. Deze afspraken moeten worden bijgehouden en beheerd. In de afspraken wordt verwezen naar standaarden. De verantwoordelijkheid voor het beheer van deze standaarden is belegd bij andere partijen (veelal standaardisatieorganisaties). Het beheer van de afspraken is dus niet hetzelfde als het beheer van de standaarden. De grote afhankelijkheid van de beheerders van de

standaarden maakt afstemming noodzakelijk. De uitvoeringsorganisatie is hiervoor verantwoordelijk. Naast deze afstemming, moeten de uitvoeringsorganisatie er ook voor zorgen dat de documentatie wordt onderhouden en dat er tekst en uitleg kan worden gegeven bij de afspraken.

- **Regie op doorontwikkeling afspraken:** Het afsprakenstelsel moet meeveranderen met ontwikkelingen in de omgeving, veranderende dienstverlening bij betrokken deelnemers en de wensen van eindgebruikers. Bij deze doorontwikkeling komt veel kijken. Zo moeten afspraken een plek krijgen binnen de bredere architectuur en moeten keuzes worden gemaakt over de ondersteuning van informatie- en andere technische standaarden. Concrete afspraken moeten worden gemaakt met de organisaties die de standaarden beheren. Ook is het van groot belang om in nauw overleg met de deelnemers te onderzoeken wat de impact van keuzes is op de bestaande voorzieningen die al door de deelnemers worden aangeboden. En in vervolg daarop te onderzoeken wat een goede ontwikkelstrategie is om die nieuwe versie ook geïmplementeerd te krijgen in de voorzieningen van de deelnemers. Er moet voldoende voeding uit het veld en de deelnemers worden verzameld om goede beslissingen te kunnen nemen bij de ontwikkeling van afspraken. Deze nieuwe afspraken moeten worden verwerkt in een nieuwe versie van het afsprakenstelsel.
- **Regie op ketenwijzigingen:** Deelnemers zijn voor de uitwisselling via MedMij van elkaar afhankelijk. Bij wijzigingen aan de afspraken is daarom regie nodig op de implementatie.
- **Regie op toe- en uittreding:** De uitvoeringsorganisatie ziet erop toe dat deelnemers die willen participeren in het stelsel ook daadwerkelijk hun zaken op orde hebben. Ook bij een eventuele uittreding ziet de uitvoeringsorganisatie toe op een goede afhandeling van zaken. De eindverantwoordelijkheid voor toe- en uittreding ligt bij Stichting MedMij. De uitvoeringsorganisatie bereidt toe- en uittredingen voor en Stichting MedMij zorgt voor de besluitvorming.
- **Deelnemersmanagement:** Deelnemende partijen moeten goed geïnformeerd zijn en er moet op worden toegezien dat mededinging niet in gevaar komt. Hiervoor moeten relaties worden onderhouden.
- **Implementatieondersteuning:** De uitvoeringsorganisatie ondersteunt deelnemers waar nodig en gepast bij het wegnemen van barrières.
- **Aanspreekpunt, voorlichting en communicatie:** De uitvoeringsorganisatie vormt het eerste aanspreekpunt voor (potentiële) deelnemers inzake (door)ontwikkeling, implementatie en naleving van het afsprakenstelsel, dan wel bij de stagnatie of onduidelijkheid in onderlinge samenwerking tussen de deelnemers. Voor de deelnemers moet duidelijk zijn voor welke vraag, informatie of ondersteuning zij waar moeten zijn. Er moet voor deelnemers één ingang zijn waar vandaan de deelnemer naar het antwoord wordt begeleid. Tevens wordt proactief informatie aan (potentiële) deelnemers verstrekt, onder andere via bijeenkomsten, waardoor betrokkenheid ontstaat bij het afsprakenstelsel.
- **Regie op het afhandelen van incidenten en calamiteiten:** In geval van incidenten en calamiteiten zal er vanuit het stelsel geacteerd moeten worden om de impact van de ernstige verstoring te mitigeren en daarmee het vertrouwen in het stelsel niet te beschadigen.
- **Handhaven deelnemersovereenkomst:** De uitvoeringsorganisatie ziet erop toe dat deelnemers zich houden aan de afspraken uit de deelnemersovereenkomst.
- **Bevorderen samenwerking deelnemers:** De uitvoeringsorganisatie faciliteert samenwerking tussen deelnemers en draagt bij aan een fair playfield. Deelnemers worden betrokken in de afstemming op verschillende onderwerpen en er wordt voorkomen dat bepaalde partijen hierin een te dominante positie verwerven.
- **Regie centrale voorzieningen:** Centrale voorzieningen die de uitwisseling in het netwerk faciliteren, moeten voor zover ze niet door de markt zelf geleverd kunnen worden, centraal worden geregeld /ingekocht. Denk hierbij bijvoorbeeld aan de inrichting van MedMij Registratie.
- **Afhandelen klachten en geschillen:** De uitvoeringsorganisatie is eerste ingang voor het registreren en behandelen van klachten. Zij hanteert hierbij een bemiddelende aanpak. Op het moment dat de klacht niet door de uitvoeringsorganisatie kan worden afgehandeld, dan volgt een doorgeleiding naar Stichting MedMij.
- **Afhandelen algemene vragen en klachten van eindgebruikers:** Deelnemers bedienen met het afsprakenstelsel uiteindelijk de gebruikers. Eindgebruikers moeten een neutrale plek kennen waarbij ze terecht kunnen voor meer informatie over MedMij, met vragen over het gebruik daarvan en/of met eventuele klachten.

Statuten Stichting MedMij

De statuten van Stichting MedMij zijn een vertaling van de Rollen en Inrichting en formaliseren de positie van actoren binnen de governance.

Modelverwerkersovereenkomst

Modelverwerkersovereenkomst is in deze versie van het afsprakenstelsel gericht op het domein Zorg, omdat dit het enige domein is dat in deze versie van het afsprakenstelsel ondersteund wordt. Zodra een nieuw domein aan MedMij wordt toegevoegd, moet deze pagina herzien worden. Er moet dan een generieke tekst geschreven worden, of per domein wordt een tekst opgesteld.

Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener zorgaanbieder

Doel

De zorgaanbieder is als verwerkingsverantwoordelijke verantwoordelijk om verwerkingsovereenkomsten af te sluiten in het geval persoonsgegevens in opdracht van hem door een derde (lees: verwerker) worden verwerkt. Binnen het MedMij Afsprakenstelsel opereert de Dienstverlener zorgaanbieder onder verantwoordelijkheid van de Zorgaanbieder. Daarmee dient er altijd een verwerkingsovereenkomst tussen Zorgaanbieder en Dienstverlener zorgaanbieder getekend te worden.

Deze verwerkersovereenkomst is een modelovereenkomst die door de Zorgaanbieder kan worden gebruikt voor MedMij specifieke onderdelen, zoals het verwerken van BSN ten behoeven van authenticatie, het verkrijgen van toestemming van de Persoon voor gegevensuitwisseling met zijn Dienstverlener persoon en het verwerken van persoonsgegevens ten behoeve van de gegevensuitwisseling zelf zoals logging en de verwerking van de betreffende persoonsgegevens door de Dienstverlener zorgaanbieder overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

De ondergetekenden:

1. << naam Zorgaanbieder >> , gevestigd te << plaatsnaam + adres >>, te dezen rechtsgeldig vertegenwoordigd door << naam + functie >>

hierna te noemen: '*Opdrachtgever*',

en

2. << naam Dienstverlener zorgaanbieder >>, (statutair) gevestigd te << plaatsnaam + adres >>, te dezen rechtsgeldig vertegenwoordigd door << functie + naam >>.

hierna te noemen: '*Opdrachtnemer*',

hierna gezamenlijk te noemen: '*Partijen*';

Overwegende dat:

I. Partijen in overeenstemming met de Algemene Verordening gegevensbescherming (AVG) in deze Verwerkersovereenkomst hun afspraken opnemen over het verwerken van persoonsgegevens ten behoeve

van de gegevensuitwisseling tussen persoonlijke gezondheidsomgevingen MedMij en de informatiesystemen van de Opdrachtgever.

II. In het kader van de uitvoering van deze Verwerkersovereenkomst de Persoonsgegevens in de zin van artikel 4 sub 1 AVG worden verwerkt binnen de scope van de afspraken zoals opgesteld in het MedMij Afsprakenstelsel.

III. De Opdrachtgever verantwoordelijk is voor het verlenen van toegang tot de persoonsgegevens aan de Persoon en het vaststellen van de identiteit van de Persoon aan de hand van een BSN. De Opdrachtnemer voert dit proces uit, conform de afspraken in het MedMij Afsprakenstelsel, in opdracht van de Opdrachtgever. De wettelijke basis voor de verwerking van het BSN door Opdrachtgever ten behoeve van authenticatie van de Persoon, met als doel de gegevensuitwisseling tussen Persoon en Opdrachtgever, overeenkomstig het bepaalde in het MedMij Afsprakenstelsel, volgt uit artikel 4 en artikel 5 van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

IV. De Opdrachtgever alleen gegevens en/of gezondheidsinformatie met de Persoon via MedMIj uitwisselt met wie hij een (actuele) behandelrelatie in de zin van de Wet op geneeskundige behandelingsovereenkomst heeft.

V. Opdrachtnemer een zogenaamde ‘Dienstverlener Zorgaanbieder’ binnen het MedMij Afsprakenstelsel is en daarvoor de Deelnemersovereenkomst Dienstverlener aanbieder met de Stichting MedMij heeft afgesloten.

VI. Krachtens artikel 4 sub 7 AVG de Opdrachtgever “Verwerkingsverantwoordelijke” is voor de Persoonsgegevens en krachtens artikel 4 sub 8 AVG de Opdrachtnemer “Verwerker” is in het kader van de uitvoering van deze Verwerkersovereenkomst.

VII. Deze overeenkomst is aan te merken als een ‘Verwerkersovereenkomst’ in de zin van artikel 28 lid 3 AVG.

Verklaren te zijn overeengekomen als volgt

Artikel 1. Begrippen

De hierna en hiervoor in deze Verwerkersovereenkomst vermelde, met een hoofdletter

geschreven begrippen, hebben de volgende betekenis:

1.1 Deelnemersovereenkomst: *'Deelnemersovereenkomst Dienstverlener zorgaanbieder'* die is gesloten tussen Stichting *MedMij en* Opdrachtnemer en op basis waarvan Opdrachtnemer is toegetreden tot het MedMij Afsprakenstelsel.

1.2 Bijlage: aanhangsels bij deze Verwerkersovereenkomst of onder deze Verwerkersovereenkomst aangegane nadere overeenkomst die onlosmakelijk zijn verbonden met deze Verwerkersovereenkomst.

1.3 BSN; het nummer, bedoeld in artikel 1, onder b, van de Wet algemene bepalingen Burgerservicenummer.

1.4 Functionaris voor de gegevensbescherming: de door Opdrachtgever benoemde functionaris als bedoeld in artikel 37 AVG.

1.5 Gegevensdienst: een gestandaardiseerde dienst voor gegevensuitwisseling met waarde voor de gebruiker die door een Dienstverlener persoon of Dienstverlener zorgaanbieder wordt aangeboden over het MedMij-netwerk. De Het MedMij Afsprakenstelsel definieert welke Gegevensdiensten over het MedMij-netwerk aangeboden mogen worden en biedt een faciliteit om het aanbod van de Dienstverlener persoon en

Dienstverlener zorgaanbieder inzichtelijk te maken. Opdrachtnemer levert Gegevensdiensten in opdracht van en volgens schriftelijke instructie van de Opdrachtgever via het MedMij-netwerk en heeft voor de verwerking van persoonsgegevens in relatie tot deze Gegevensdiensten de Verwerkersovereenkomst met Opdrachtgever afgesloten.

1.6 MedMij Afsprakenstelsel: de door de Stichting MedMij vastgestelde laatst geldende release van het MedMij Afsprakenstelsel.

1.7 Persoon: degene op wie een Persoonsgegeven betrekking heeft,16 jaar of ouder is, en zich bij Opdrachtnemer authentiseert met een authenticatiemiddel.

1.8 Persoonsgegeven: persoonsgegeven in de zin van artikel 4 sub 1 en sub 15 Algemene Verordening Gegevensbescherming.

1.9 Verwerking: verwerking in de zin van artikel 4 sub 2 Algemene Verordening Gegevensbescherming.

1.10 Verwerkersovereenkomst: deze overeenkomst inclusief Overwegingen en bijbehorende Bijlage(n).

Artikel 2. Totstandkoming, duur van de Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst geldt vanaf de datum van ondertekening en wordt aangegaan voor de duur van de Deelnemersovereenkomst.

2.2 De Verwerkersovereenkomst eindigt van rechtswege wanneer de Deelnemersovereenkomst eindigt.

Artikel 3. Voorwerp van de Verwerkersovereenkomst

3.1 Opdrachtnemer verwerkt het BSN ten behoeven van authenticatie en verwerkt Persoonsgegevens voor:

- het verkrijgen van toestemming van de Persoon voor het verstrekken van Persoonsgegevens aan een derde partij namelijk de Dienstverlener persoon;
- de inhoud van de gegevensuitwisseling;
- handelingen ten behoeve van de gegevensuitwisseling;

overeenkomstig het bepaalde in het MedMij Afsprakenstelsel voor Opdrachtgever op basis van de G egevensdiensten van het MedMij Afsprakenstelsel zoals opgenomen in Bijlage I. De verwerking van Persoonsgegevens vindt uitsluitend plaats in opdracht en volgens schriftelijke instructie van de Opdrachtgever en zoals in Bijlage I aangegeven, behoudens afwijkende wettelijke verplichtingen.

3.2 Indien op verzoek van de Persoon, de Persoon Persoonsgegevens met Opdrachtgever wil delen, vergewist Opdrachtnemer zich ervan, overeenkomstig het bepaalde in het MedMij Afsprakenstelsel, dat Opdrachtgever een (actuele) behandelrelatie in de zin van artikel 7:446 van het Burgerlijk Wetboek met de Persoon heeft.

3.3 Opdrachtnemer zal de Persoonsgegevens aantoonbaar op behoorlijke en zorgvuldige wijze en in overeenstemming met de op hem als Verwerker op grond van de privacy- en andere toepasselijke wet- en regelgeving betreffende de verwerking van Persoonsgegevens verwerken.

3.4 Opdrachtnemer verwerkt de Persoonsgegevens niet voor eigen doeleinden. Voor zover niet anders is bepaald in deze Verwerkersovereenkomst, neemt Opdrachtnemer geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over het doel en de middelen voor de Verwerking van de Persoonsgegevens berust nimmer bij Opdrachtnemer.

3.5 Opdrachtnemer schakelt geen derden in zonder voorafgaande specifieke of algemene schriftelijke toestemming van Opdrachtgever. Opdrachtgever kan aan de toestemming om derden in te schakelen voorwaarden verbinden.

3.6 Indien Opdrachtnemer op grond van een wettelijke verplichting gegevens dient te verstrekken, verifieert Opdrachtnemer de grondslag van het verzoek en de identiteit van de verzoeker en informeert hij onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, Opdrachtgever ter zake.

3.7 Opdrachtnemer verleent Opdrachtgever volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de privacy- en andere toepasselijke wet- en regelgeving betreffende de verwerking van Persoonsgegevens, meer in het bijzonder met betrekking tot de rechten van betrokkenen, zoals, maar niet beperkt tot, een verzoek om inzage, verbetering, aanvulling, verwijdering, afscherming of de overdraagbarheid van Persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet. Tevens verleent Opdrachtnemer volledige medewerking aan het adequaat informeren van de betrokkenen in het kader van de meldplicht datalekken. De eventuele kosten die voortvloeien uit het niet of niet tijdig voldoen aan de meldplicht met betrekking tot datalekken komen voor rekening van Opdrachtnemer.

3.8 Indien Opdrachtnemer (pogingen tot) onrechtmatige of anderszins ongeautoriseerde verwerkingen of inbreuken op de beveiligingsmaatregelen van de Persoonsgegevens signaleert, zal hij Opdrachtgever hierover onmiddellijk inlichten en op eigen kosten alle redelijkerwijs benodigde maatregelen treffen om een (dreigende) schending van de privacy- en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens te voorkomen of te beperken; één en ander onverminderd de verplichting van Opdrachtnemer om de eventueel door Opdrachtgever daardoor geleden schade te vergoeden.

3.9 Opdrachtgever en Opdrachtnemer betrekken de Functionaris voor de gegevensbescherming tijdig en naar behoren bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

3.10 Overeenkomstig het bepaalde in Hoofdstuk V van de Algemene Verordening Gegevensbescherming verwerkt Opdrachtnemer geen Persoonsgegevens buiten een land van de Europese Unie/Europese Economische ruimte zonder een passend beschermingsniveau.

Artikel 4. Beveiliging

4.1 Opdrachtnemer zal overeenkomstig de voor Opdrachtgever geldende wet- en regelgeving voor beveiliging de benodigde maatregelen implementeren die het vertrouwen en de continuïteit van de Verwerking borgen. De maatregelen, die zijn opgenomen in het Normenkader informatiebeveiliging van het MedMij Afsprakenstelsel, dienen met inachtneming van de stand der techniek een passend beschermingsniveau te verzekeren voor de Verwerking in relatie tot het MedMij Afsprakenstelsel, zulks met inachtneming van de risico’s die de Verwerking met zich meebrengen.

4.2 Opdrachtnemer rapporteert aan Opdrachtgever over de door hem genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin. De rapportage dient betrekking te hebben op de in het eerste lid bedoelde beveiligingsmaatregelen. Daarnaast toont Opdrachtnemer aan dat hij voldoet aan de voor hem geldende normen op het gebied van informatiebeveiliging. Opdrachtnemer kan aan de hand van geldige certificering of een gelijkwaardig bewijsmiddel aantonen dat hij hieraan voldoet.

Artikel 5. Geheimhouding

5.1 Opdrachtnemer is gehouden tot geheimhouding van alle Persoonsgegevens en informatie die zij als uitvloeisel van deze Verwerkersovereenkomst verwerkt, behoudens in zoverre die gegevens of informatie klaarblijkelijk geen geheim of vertrouwelijk karakter hebben, dan wel reeds algemeen bekend zijn.

5.2 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer ten aanzien van de daarbij aangeduide gegevens of informatie bijzondere maatregelen treffen met het oog op de geheimhouding daarvan, welke maatregelen onder meer kunnen inhouden de vernietiging van betrokken gegevens of informatie zodra de noodzaak voor Opdrachtnemer om daarvan nog langer kennis te nemen, is komen te vervallen.

5.3 Opdrachtnemer zal in haar overeenkomsten met het personeel van Opdrachtnemer bedingen dat door die personen op overeenkomstige wijze als in artikel 5.1 en 5.2 bepaald geheimhouding zal worden betracht ten aanzien van alle gegevens en informatie die zij in het kader van hun werkzaamheden voor Opdrachtnemer verwerken. Opdrachtnemer staat er jegens Opdrachtgever voor in dat de bedoelde bedingen door de betrokken personen zullen worden nageleefd.

Artikel 6. Gebruik onderaannemers (subverwerkers)

6.1 Opdrachtnemer zal aan de door hem ingeschakelde derde dezelfde of strengere verplichtingen opleggen als voor hemzelf gelden op basis van deze Verwerkersovereenkomst en uit de wet- en regelgeving voortvloeien en ziet toe op de naleving daarvan door de derde. De betreffende afspraken met de derde worden schriftelijk vastgelegd. Opdrachtnemer zal Opdrachtgever op eerste verzoek een afschrift verstrekken van deze overeenkomsten(en).

6.2 Niettegenstaande de toestemming van de Opdrachtgever voor het inschakelen van een derde partij blijft Opdrachtnemer volledig aansprakelijk jegens Opdrachtgever voor de gevolgen van het uitbesteden van werkzaamheden aan een derde. De toestemming van Opdrachtgever voor het uitbesteden van werkzaamheden aan een derde partij laat onverlet dat voor de inzet van subverwerkers artikel 3.10 van overeenkomstige toepassing is.

Artikel 7. Controle

7.1 Opdrachtgever kan de Verwerking en de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen van Opdrachtnemer, dan wel die van door Opdrachtnemer ingeschakelde derden, op elk door hem gewenst moment controleren of doen controleren. In verband daarmee verstrekt Opdrachtnemer op eerste verzoek van Opdrachtgever een (zelf)verklaring waarin een oordeel wordt gegeven over de genoemde naleving.

7.2 Opdrachtnemer zal alle redelijkerwijs benodigde medewerking verlenen aan de controle en er voor zorg dragen ook de door hem ingeschakelde derden hiertoe de redelijkerwijs benodigde medewerking zullen verlenen.

7.3 Het uitvoeren van een controle zal niet tot een vertraging van de door Opdrachtnemer in het kader van deze Verwerkersovereenkomst te verrichten werkzaamheden mogen leiden. Indien niettemin vertraging optreedt, zullen Partijen in overleg treden teneinde daarvoor zo snel mogelijk een oplossing te vinden.

7.4 De met de controle gemoeide kosten zijn voor rekening van Opdrachtgever, tenzij uit de controle blijkt dat Opdrachtnemer is tekortgeschoten in de nakoming van zijn verplichting(en) uit deze Verwerkersovereenkomst.

7.5 Opdrachtnemer voert de door Opdrachtgever aangegeven aanbevelingen ter verbetering uit binnen de daartoe door Opdrachtgever te bepalen termijn.

Artikel 8. Opschorting en beëindiging

8.1 Partijen kunnen deze Verwerkersovereenkomst tussentijds opzeggen met inachtneming van een opzegtermijn van één kalendermaand.

8.2 Deze Verwerkersovereenkomst kan door Opdrachtgever met onmiddellijke ingang worden beëindigd indien Opdrachtgever heeft vastgesteld dat Opdrachtnemer niet of onvoldoende voldoet aan de in artikel 4 van deze Verwerkersovereenkomst voorgeschreven technische en organisatorische beveiligingseisen dan wel anderszins de in deze Verwerkersovereenkomst opgenomen voorschriften, verplichtingen of procedures niet nakomt of volgt.

8.3 Verplichtingen welke naar hun aard bestemd zijn ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst gelden. Tot deze bepalingen behorend onder meer de bepalingen betreffende geheimhouding, aansprakelijkheid en toepasselijk recht.

8.4 Partijen zijn gerechtigd, onverminderd hetgeen daartoe bepaalde in de Deelnemersovereenkomst Dienstverlener aanbieder, de uitvoering van de Verwerkersovereenkomst en de daarmee samenhangende Deelenemersovereenkomst op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang te ontbinden, indien:

a) de ander partij wordt ontbonden of anderszins ophoudt te bestaan;

b) de andere partij aantoonbaar tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die ernstige toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling;

c) een partij in staat van faillissement wordt verklaard of surseance van betaling.

8.5 Opdrachtgever is gerechtigd deze Verwerkersovereenkomst per direct te ontbinden indien de Opdrachtnemer te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of rechtspraak aan de verwerking van persoonsgegevens worden gesteld.

Artikel 9. Bewaartermijn, teruggave en vernietiging van Persoongegevens

9.1 Opdrachtnemer bewaart de Persoonsgegevens niet langer dan strikt noodzakelijk voor het doel zoals opgenomen in Bijlage I en conform de bepalingen in het MedMij Afsprakenstelsel.

9.2 Bij beëindiging van de Verwerkersovereenkomst of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, indien blijkt dat overeenkomstig de vergewisplicht van artikel 3.2 van de Verwerkersovereenkomst de Opdrachtgever geen (actuele) behandelrelatie in de zin van artikel 7:446 van het Burgerlijk Wetboek met de Persoon heeft, of op schriftelijke verzoek van Opdrachtgever zal Opdrachtnemer, kosteloos, naar keuze van Opdrachtgever, de Persoonsgegevens vernietigen of teruggeven aan Opdrachtgever. Op eerste verzoek van Opdrachtgever verstrekt Opdrachtnemer bewijs van het feit dat de Persoonsgegevens vernietigd of verwijderd zijn.

Artikel 10. Aansprakelijkheid

10.1 Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen. Gebruikers kunnen zich jegens Partijen onmiddellijk en direct op deze aansprakelijkheid beroepen.

10.2 Partijen zijn jegens elkaar aansprakelijk indien zij de verplichtingen uit de Verwerkersovereenkomst en /of de privacy- en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens schenden door deze niet of niet naar behoren na te komen. Indien en voor zover deze schending toerekenbaar is, heeft deze schadeplichtigheid tot gevolg.

10.3 Opdrachtnemer vrijwaart Opdrachtgever en stelt Opdrachtgever schadeloos voor alle claims, acties, aanspraken van derden voor verliezen, schade of kosten, waaronder boetes van de Autoriteit Persoonsgegevens die Opdrachtgever maakt of lijdt en die rechtstreeks of indirect voortvloeien uit of tot stand komen in verband met een tekortkoming door de Opdrachtnemer en/of diens onderaannemers in de nakoming van zijn verplichtingen onder deze Verwerkersovereenkomst.

Artikel 11. Slotbepalingen

11.1 Afwijkingen van deze Verwerkersovereenkomst zijn slechts bindend voor zover zij uitdrukkelijk tussen Partijen schriftelijk zijn overeengekomen.

11.2 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing

11.3 Geschillen over en die voortvloeien uit deze overeenkomst worden voorgelegd aan de bevoegde rechter in Den Haag.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

<< naam Zorgaanbieder >>

namens deze,

Naam:

Functie:

Datum

Plaats

<< Naam Dienstverlener Zorgaanbieder >>

namens deze,

Naam:

Functie:

Datum:

Plaats:

Bijlage 1. Overzicht Persoonsgegevens en Procedure

Het doel van de Verwerking voor MedMij specifieke onderdelen, overeenkomstig het bepaalde in het MedMij Afsprakenstelsel is op verzoek van de Persoon door de Opdrachtnemer het verwerken van het BSN ten behoeven van authenticatie, het verkrijgen van toestemming van de Persoon voor gegevensuitwisseling, het verwerken van persoonsgegevens ten behoeve van de gegevensuitwisseling, zoals logging, de verwerking van de betreffende persoonsgegevens zelf namens de Opdrachtgever van deze Persoon.

Hiervoor worden uitsluitend de volgende Persoonsgegevens door Opdrachtnemer verwerkt:

- BSN;
- Toestemmingsverklaring van de Persoon voor het verstrekken van gegevens aan een derde partij namelijk de Dienstverlener persoon;
- Informatie ten behoeve van het zich vergewissen van het bestaan van een (actuele) behandelrelatie tussen de Persoon en de Opdrachtgever;
- Bevestigingsverklaring van de Persoon voor het delen van gegevens met de Opdrachtgever;
- De Persoonsgegevens uit de gegevensdiensten die door de Opdrachtgever conform de afspraken uit het MedMij Afsprakenstelsel via het MedMij-netwerk worden verstrekt of verkregen;
- De persoonsgegevens ten behoeve van de gegevensuitwisseling (zoals logging).

De categorie betrokkenen van wie bovenstaande persoonsgegevens worden verwerkt zijn: Personen die willen beschikken over hun gezondheidsinformatie in de PGO en 16 jaar of ouder zijn.

Overeenkomstig artikel 3.1 van deze Verwerkersovereenkomst worden de Persoonsgegevens overeenkomstig de beschreven Processen & Informatie met de bijbehorende use cases door 'Dienstverlener zorgaanbieder' zoals opgenomen in het MedMij Afsprakenstelsel door Opdrachtnemer verwerkt.

Issues

Loopt u als (potentiële) deelnemer aan tegen problemen bij de implementatie van de afspraken of heeft u suggesties voor doorontwikkeling? Laat dat dan vooral aan MedMij weten door het issueformulier in te vullen en te sturen naar productmanagement@medmij.nl. Zie verder het Change- en releasebeleid voor een nadere beschrijving van de afhandeling.

pdf.images

Deze plaatjes worden gebruikt bij de PDF export.