MedMij Afsprakenstelsel

Release 1.1 versie 0.8

Auteur Project Afsprakenstelsel

Datum 2 juli 2018

This deliverable contains original unpublished work or work to which the author holds all rights except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Inhoudsopgave

1. Introductie . . . 4
1.1 Afsprakenstelsel in de praktijk . . . 6
1.2 Release- en versiebeschrijving . . . 9
1.3 Changelog . . . 12
1.3.1 Changelog release 1.1 . . . 13
1.3.1.1 Changelog release 1.1 versie 0.8 . . . 14
1.3.2 Changelog release 1.0 . . . 17
1.3.2.1 Changelog release 1.0 versie 1.0 . . . 18
1.3.2.2 Changelog release 1.0 versie 0.991 . . . 19
1.3.2.3 Changelog release 1.0 versie 0.99 . . . 20
1.3.2.4 Changelog release 1.0 versie 0.9 . . . 21
1.3.2.5 Changelog release 1.0 versie 0.8 . . . 23
1.3.2.6 Changelog release 1.0 versie 0.3 . . . 25
1.4 Voorziene wijzigingen . . . 27
2. Grondslagen . . . 29
2.1 Achtergrond . . . 30
2.2 Criteria . . . 36
2.3 Principes . . . 40
2.4 Opzet . . . 45
2.5 Begrippenlijst . . . 47
3. Juridisch kader . . . 49
3.1 Toelichting verwerkingsverantwoordelijkheid . . . 63
4. Overeenkomsten en rechtsrelaties . . . 66
4.1 Deelnemersovereenkomsten . . . 70
4.1.1 Deelnemersovereenkomst Dienstverlener persoon . . . 71
4.1.2 Deelnemersovereenkomst Dienstverlener zorgaanbieder . . . 80
4.2 Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener zorgaanbieder . . . 88
4.3 Zelfverklaring integriteit . . . 96
5. Architectuur en technische specificaties . . . 99
5.1 Juridica . . . 102
5.2 Processen en informatie . . . 103
5.2.1 UC Verzamelen . . . 111
5.2.2 UC Delen . . . 117
5.2.3 UC Opvragen ZAL . . . 124
5.2.4 UC Opvragen OCL . . . 125
5.2.5 UC Opvragen GNL . . . 126
5.3 Applicatie . . . 127
5.3.1 UCI Verzamelen . . . 141
5.3.2 UCI Delen . . . 153
5.3.3 UCI Opvragen ZAL . . . 165
5.3.4 UCI Opvragen OCL . . . 166
5.3.5 UCI Opvragen GNL . . . 167
5.3.6 Gegevens en performance in UCI Verzamelen en UCI Delen . . . 168
5.3.7 Gegevens en performance inzake opvragen lijsten . . . 173
5.3.8 XML-bestanden voor lijsten . . . 174
5.4 Netwerk . . . 175
5.4.1 UCI Opvragen Whitelist . . . 182
5.5 Metamodel . . . 183
5.6 XML-schema's . . . 197
6. Governance . . . 202
6.1 Rollen . . . 204
6.2 Inrichting . . . 208
6.2.1 Beheerverantwoordelijkheden . . . 214
6.3 Beleid . . . 217
6.3.1 Toetredingsbeleid . . . 218
6.3.2 Gegevensdienstenbeleid . . . 219
6.3.3 Kwalificatie- en acceptatiebeleid . . . 220
6.3.4 Samenwerkings- en escalatiebeleid . . . 221
6.3.5 Klachten- en geschillenbeleid . . . 222
6.3.6 Nalevingsbeleid . . . 223
6.3.7 Change- en releasebeleid . . . 225

6.3.8 Privacy- en informatiebeveiligingsbeleid . . . 227
6.3.9 Intellectueel eigendomsbeleid . . . 228
6.3.10 Zorgaanbiedersnamenbeleid . . . 230
6.3.11 OAuthclient-namenbeleid . . . 231
6.4 Operationele processen . . . 232
7. Normenkader informatiebeveiliging . . . 235
7.1 A.5.1.1 Beleidsregels voor informatiebeveiliging . . . 239
7.2 A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging . . . 240
7.3 A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging . . . 241
7.4 A.8.2.1 Classificatie van informatie . . . 242
7.5 A.9.1.1 Beleid voor toegangsbeveiliging . . . 243
7.6 A.9.2.5 Beoordeling van toegangsrechten van gebruikers . . . 244
7.7 A.9.4.1 Beperking toegang tot informatie . . . 245
7.8 A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen . . . 246
7.9 A.12.1.2 Wijzigingsbeheer . . . 247
7.10 A.12.1.3 Capaciteitsbeheer . . . 248
7.11 A.12.3.1 Back-up van informatie . . . 249
7.12 A.12.4.1 Gebeurtenissen registreren . . . 250
7.13 A.12.4.4 Kloksynchronisatie . . . 251
7.14 A.12.5.1 Software installeren op operationele systemen . . . 252
7.15 A.12.6.1 Beheer van technische kwetsbaarheden . . . 253
7.16 A.14.2.1 Beleid voor beveiligd ontwikkelen . . . 254
7.17 A.16.1.1 Verantwoordelijkheden en procedures . . . 255
7.18 A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging . . . 256
7.19 A.16.1.7 Verzamelen van bewijsmateriaal . . . 257
7.20 A.18.2.3 Beoordeling van technische naleving . . . 258
8. Communicatie . . . 259
8.1 Merkgebruik . . . 260
8.2 Gebruikersvoorlichting . . . 262
8.3 Toestemmingsverklaring . . . 263
8.4 Bevestigingsverklaring . . . 265
9. Managementinformatie . . . 267
10. Catalogus . . . 268

Introductie

Voor u ligt het MedMij Afsprakenstelsel release 1.1, een afsprakenset voor veilige, interoperabele en betrouwbare gegevensuitwisseling tussen persoonlijke gezondheidsomgevingen en informatiesystemen van zorgaanbieders. Het MedMij Afsprakenstelsel release 1.1 betreft een verzameling samenhangende producten op juridisch, technisch, semantisch en organisatorisch gebied. Deze afspraken moeten partijen voldoende vertrouwen geven om de onderlinge gegevensuitwisseling tot stand te brengen en het afsprakenstelsel te toetsen op bruikbaarheid in praktijksituaties. 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 zorgaanbieders, 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 en kunnen diensten aanbieden op basis van de reeds overeengekomen afspraken.

Release 1.1 versie 0.8 is een tussentijdse werkversie van de eerste productierelease van het stelsel en is bedoeld voor oriëntatie op deelname. Het gebruik van deze producten heeft nog geen formele status en er is nog geen sprake van een formeel afsprakenstelsel. Formalisering moet nog plaatsvinden met de vaststelling van de afsprakenset door Stichting MedMij.

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 het afsprakenstelsel. Het stelsel beschrijft alleen dat wat nog niet in wet- en regelgeving is vastgelegd en wat nodig is voor het vertrouwen van deelnemers in de onderlinge gegevensuitwisseling. Deelnemers dienen zowel op de hoogte te zijn van de wet- en regelgeving als van de aanvullende afspraken in het stelsel. Om die reden is de belangrijkste wet- en regelgeving en de toepassing daarvan opgenomen in een Juridisch kader. De opbouw van dit kader veronderstelt enig begrip van de opzet van het afsprakenstelsel. Het is daarom aan te bevelen om eerst de Grondslagen te lezen.

De documentatie van het stelsel is als volgt opgebouwd:

- **Introductie:** De introductie maakt de lezer wegwijs in de documentatie. Het hoofdstuk beschrijft de wijze waarop het stelsel is opgebouwd, de kenmerken van de huidige release en versie en een overzicht van wijzigingen per versie. Daarnaast is de werking van het stelsel op toegankelijke wijze beschreven in het verhaal van Roos Dalstra (Afsprakenstelsel in de praktijk).
- **Grondslagen:** De basale uitgangspunten van het MedMij Afsprakenstelsel zijn zoveel mogelijk beschreven in de grondslagen. Alle specifieke afspraken op juridisch, organisatorisch, financieel, semantisch en technisch gebied komen voort uit deze grondslagen en worden hieraan getoetst.
- **Juridisch kader:** Het juridisch kader geeft een overzicht van de belangrijkste wet- en regelgeving die op de deelnemers in het afsprakenstelsel van toepassing is bij de uitvoering van hun activiteiten.
- **Overeenkomsten en rechtsrelaties:** De afspraken binnen MedMij zijn aanvullend op de wet- en regelgeving en vertaald in deelnemersovereenkomsten en een modelverwerkersovereenkomst.
- **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.
- **Governance:** De governance omschrijft op welke wijze het afsprakenstelsel wordt beheerd, welke rollen daarin te onderscheiden zijn en door welke partijen deze rollen worden vervuld.
- **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 te beginnen met de algemene teksten uit de Introductie, Grondslagen en het Juridisch kader. Deze drie hoofdstukken samen vormen een goed beeld van de achtergrond bij en de reikwijdte van het afsprakenstelsel. De Overeenkomsten en rechtsrelaties, Architectuur en technische specificaties, Normenkader informatiebeveiliging, Governance, Communicatie en Managementinformatie beschrijven vervolgens per onderwerp de verschillende afspraken.

Afsprakenstelsel in de praktijk

Doel

Het klantverhaal van Roos Dalstra beschrijft op toegankelijke wijze de praktische toepassing van het afsprakenstelsel.

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.

Release- en versiebeschrijving

Doel

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	1.1
Versie	0.8: Versie bedoeld voor oriëntatie op deelname aan de eerste productiefase. De versie heeft nog geen formele status.
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 technische specificaties. De overeenkomst en de specificaties zijn opgenomen in de afsprakenset.
Doelgroep	• Potentiële deelnemers (dienstverleners persoon en dienstverleners zorgaanbieder) • Beheerorganisatie MedMij • Programma MedMij • Geïnteresseerden in de doorontwikkeling van het MedMij Afsprakenstelsel
Totstandkoming	Deze versie is tot stand gekomen onder leiding van het project MedMij Afsprakenstelsel in samenwerking met diverse partijen in de zorg, zoals ICT-leveranciers, het ministerie van VWS, Patiëntenfederatie Nederland en vertegenwoordigers van zorgaanbieders. Bij de nadere uitwerking van het N ormenkader Informatiebeveiliging en de Governance zijn ook NEN, certificeringsbureaus en de uitvoeringsorganisatie betrokken geweest. De nadere uitwerking van de Architectuur en technische specificaties is maandelijks voorgelegd aan de Werkgroep Gegevensuitwisseling.
Inwerkingtreding	Nadat de afsprakenset is vastgesteld door het bestuur.
Operationeel toepassingsgebied	• Alle deelnemers aan de eerste productiefase van het MedMij Afsprakenstelsel. • De beheerorganisatie MedMij.
Status (juli 2018)	Het gebruik van de producten heeft nog geen formele status en er is nog geen sprake van een formeel afsprakenstelsel. Formalisering moet nog plaatsvinden via vaststelling van het afsprakenstelsel door Stichting MedMij. Operationele situaties waarin gebruik wordt gemaakt van het afsprakenstelsel vallen buiten de verantwoordelijkheid van MedMij. Gebruik van de producten is op eigen risico.

Componenten	Release 1.1 is de tweede release van de MedMij-afsprakenset. Deze openbare afsprakenset bestaat uit: • Een beschrijving van de grondslagen (achtergrond, criteria, principes, rollen, interacties en begrippenlijst) van het afsprakenstelsel; • Een juridisch kader met een analyse van relevante wet- en regelgeving; • Deelnemersovereenkomsten, te sluiten tussen een deelnemer en de beheerorganisatie; • Een modelverwerkersovereenkomst tussen de zorgaanbieder en de dienstverlener zorgaanbieder; • Een zelfverklaring integriteit om te toetsen op eventuele integriteitsrisico's bij potentiële deelnemers; • Een architectuurbeschrijving in termen van rollen en verantwoordelijkheden; • Specificaties voor de interacties tussen deelnemers en met externe voorzieningen; • Een metamodel met een samenhangende beschrijving van de begrippen en relaties die worden gebruikt in de zorgaanbiederslijst, whitelist, catalogus, oauthclientlist, gegevensdienstnamenlijst en het register van informatiestandaarden; • Een gegevensmodel voor de opbouw van de lijsten die door de beheerorganisatie voor uiteenlopende doelen beschikbaar worden gesteld (XML-schema's); • Een normenkader informatiebeveiliging met daarin de maatregelen die deelnemers en beheerorganisatie minimaal moeten treffen in aanvulling op de eigen risicoanalyse; • Een beschrijving van de rollen en de inrichting van de governance; • Een beschrijving van het beleid rondom toetreding, gegevensdiensten, kwalificatie en acceptatie, samenwerking en escalatie, naleving, klachten en geschillen, change en release, privacy en informatiebeveiliging, intellectueel eigendom, zorgaanbiedersnamen en oauthclientnamen; • Een overzicht van de belangrijkste operationele beheerprocessen, waarbij zowel beheerorganisatie als deelnemers een rol spelen; • Richtlijnen voor het gebruik van het merk MedMij in communicatie; • Een verwijzing naar de gebruikersvoorlichting die deelnemers moeten hanteren richting personen en zorgaanbieders; • Een toestemmingsverklaring voor het verkrijgen van toestemming van personen voor specifieke gegevensverstrekkingen door de zorgaanbieder aan de dienstverlener persoon; • Een bevestigingsverklaring waarmee personen op uniforme wijze kunnen bevestigen dat zij gegevens bij de dienstverlener persoon willen delen met de zorgaanbieder; • Een beschrijving van de managementinformatie die deelnemers periodiek aan de beheerorganisatie moeten aanleveren.
Functionele scope	Het afsprakenstelsel ondersteunt in deze release: • Het opvragen van gezondheidsgegevens door een persoon bij een zorgaanbieder, voor bewaring in een persoonlijke gezondheidsomgeving; • Het delen van gezondheidsgegevens door een persoon met een zorgaanbieder, voor gebruik bij de behandeling;
Licentie	Creative Commons: Naamsvermelding-GeenAfgeleideWerken 4.0 Internationaal (CC BY-ND 4.0).

Changelog

De changelog beschrijft de wijzigingen die zijn doorgevoerd bij releases van het afsprakenstelsel.

Changelog release 1.1

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

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

Voorziene wijzigingen

Release 1.1 versie 0.8

MedMij Afsprakenstelsel release 1.1 versie 0.8 is een tussentijdse werkversie van de eerste productierelease van het stelsel. Met deze publicatie kunnen potentiële deelnemers een goede inschatting maken wat deelname aan het MedMij Afsprakenstelsel betekent.

Deze zomer wordt de laatste stap gezet richting release 1.1 versie 1.0. Op dit moment lopen nog een Privacy Impact Assessment, een herijking van de risicoanalyse voor informatiebeveiliging en de tweede fase van Proves (het programma waarin de werking van het MedMij Afsprakenstelsel in praktijk wordt beproefd). Op grond van deze onderzoeken, praktijkbeproeving en andere ingediende verzoeken en verbetervoorstellen kunnen nog wijzigingen worden doorgevoerd in het stelsel. In deze publicatie is al wel getracht de issues met impact op de deelnemers zoveel mogelijk te verwerken of aan te geven waar nog dingen gaan veranderen. Deelnemers kunnen alleen nog geen rechten ontlenen aan de publicatie.

Het streven is om in september de definitieve versie van release 1.1 te publiceren om deze vervolgens op gecontroleerde wijze in productie te brengen.

Voorziene wijzigingen release 1.1 versie 1.0

Nr.	Voorgenomen wijziging
AF-846	Bij de XML-schema's zal een toelichting op uniciteitscontroles worden toegevoegd.
AF-830	In het beleid wordt verwezen naar een licentietekst buiten het afsprakenstelsel gericht op de zorgaanbieder. In deze tekst wordt beschreven op welke manier zorgaanbieders die gegevens uitwisselen via MedMij, het merk mogen gebruiken.
AF-829	In het afsprakenstelsel wordt beschreven hoe met versienummering van de catalogus wordt omgegaan.
AF-825	In het afsprakenstelsel wordt beschreven hoe te handelen bij onbeschikbaarheid van MedMij Registratie.
AF-822	In de architectuur en technische specificaties wordt beschreven hoe de adressering van MedMij Registratie eruit ziet.
AF-777	In het afsprakenstelsel wordt verduidelijkt hoe de verantwoordelijkheden liggen rondom BSN in ongestructureerde data.
AF-463	In het afsprakenstelsel worden de aanbevelingen uit de risico-analyse verwerkt.
AF-296	In het afsprakenstelsel worden de maatregelen uit de Privacy Impact Assessment verwerkt.
AF-420	De catalogus wordt aangevuld met gegevensdiensten op basis van nieuwe informatiestandaarden.
AF-447	Aan het beleid wordt informatieclassificatiebeleid toegevoegd.
AF-	In het OAuthclient-namenbeleid wordt toegevoegd bij welk type naam uit het handelsregister de

863	OAuthclientnaam moet aansluiten.

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

Groeimodel

De achtergrond beschrijft mede het afsprakenstelsel zoals dat uiteindelijk beoogd is te werken. In release 1.1 van het afsprakenstelsel worden nog niet alle functionaliteiten aangeboden. De Release- en versiebeschrijving geeft een overzicht van de inhoud van release 1.1 van het afsprakenstelsel.

Doel

De achtergrond beschrijft welke problematiek met het afsprakenstelsel moet worden opgelost en waarom is gekozen voor een afsprakenstelsel als oplossing.

Het programma MedMij streeft ernaar dat persoonlijke gezondheidsomgevingen een prominente plek gaan innemen in de Nederlandse zorg. In 2020 moet een kritische massa zijn bereikt voor wat betreft gebruik en aanbod van persoonlijke gezondheidsomgevingen onder zorgaanbieders, patiënten of personen in het algemeen en leveranciers van de technische oplossingen.

De persoonlijke gezondheidsomgeving geeft de mogelijkheid tot regie over de eigen gezondheid en over het delen van gegevens. Het biedt rust, vertrouwen en inzicht doordat een goed beeld ontstaat van hoe de persoonlijke gezondheid zich ontwikkelt en wat de persoon eraan kan doen om die te verbeteren. Het gebruik van een persoonlijke gezondheidsomgeving kan tevens de professional helpen om de juiste en beste zorg en ondersteuning te leveren. Het biedt ook kansen voor efficiëntere besteding van de tijd van zowel de professional als van de persoon. De persoonlijke context komt met het gebruik van een persoonlijke gezondheidsomgeving beter tot zijn recht. Ook kunnen professionals eenvoudiger toegang krijgen tot relevante informatie die gedeeld wordt door de persoon. Mensen zijn zelf beter geïnformeerd. Dit bevordert de samenwerking en communicatie tussen professionals en de persoon: zij worden meer en meer partners in gezondheid.

Het programma bevordert de opkomst van persoonlijke gezondheidsomgevingen door gericht barrières weg te nemen die de ontwikkeling en het gebruik in de weg staan en randvoorwaarden te stellen aan de kwaliteit en rechtmatigheid. Op dit moment wordt het potentieel van persoonlijke gezondheidsomgevingen onderbenut. Personen en zorgaanbieders hebben nog onvoldoende vertrouwen in elektronische gegevensuitwisseling en hebben weinig ervaring op kunnen doen met het concept. Leveranciers van ict-oplossingen zijn op hun beurt terughoudend met investeringen zolang personen en zorgaanbieders geen vraag articuleren; daarbovenop zijn er vraagstukken rond interoperabiliteit en authenticatie. Het programma zet in op een afsprakenstelsel en heeft daarvoor het label MedMij gelanceerd.

De persoonlijke gezondheidsomgeving

Patiëntenfederatie Nederland hanteert de volgende definitie van een persoonlijke gezondheidsomgeving:

Definitie persoonlijke gezondheidsomgeving

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 persoonlijke gezondheidsomgevingen maken gebruik van informatie uit achterliggende systemen van zorgaanbieders en kunnen via hun persoonlijke gezondheidsomgeving waarde toevoegen aan die gegevens met behulp van digitale zorgdiensten. Ook zullen er aanbieders van losse functionaliteit zijn, zoals van mobiele apps, die via het MedMij Afsprakenstelsel gegevens kunnen uitwisselen.

Grip op je eigen gezondheidsgegevens en toegang tot digitale functionaliteit 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 persoonlijke gezondheidsomgevingen komen moeizaam op gang. De voordelen van persoonlijke gezondheidsomgevingen, als middelen die de persoon in staat stellen regie over het zorgproces te nemen en zelfmanagement toe te passen, blijven daardoor grotendeels uit. De doelstelling van het programma MedMij om in 2020 een kritische massa bereikt te hebben, zal niet worden gerealiseerd zonder ingrijpen.

De ontwikkeling van persoonlijke gezondheidsomgevingen wordt gehinderd door een aantal barrières, die spelen bij personen, zorgaanbieders en de leveranciers van de persoonlijke gezondheidsomgevingen. We benoemen de belangrijkste daarvan.

Personen – al dan niet reeds patiënt – hebben niet altijd voldoende vertrouwen om gevoelige gegevens over hun gezondheid te delen met andere partijen dan de zorgaanbieder zelf, zoals leveranciers van persoonlijke gezondheidsomgevingen. De bestaande wet- en regelgeving die eisen stelt aan de omgang met persoonsgegevens gaat nog uit van medische dossiers die beheerd worden door zorgaanbieders met een medisch beroepsgeheim en niet van persoonlijke gezondheidsomgevingen waarbij personen zelf individuele afwegingen maken over het wel of niet willen gebruiken van een persoonlijke gezondheidsomgeving. De waarborgen die nodig zijn om hun relatief kwetsbare positie te beschermen zijn nog onvoldoende aanwezig; zo is er bijvoorbeeld geen patiëntgeheim naar analogie met het medisch beroepsgeheim van zorgaanbieders.

Zorgaanbieders ervaren eveneens terughoudendheid bij het delen van gegevens over patiënten via persoonlijke gezondheidsomgevingen van veelal andere ict-leveranciers en organisaties. Juist doordat zij zijn gehouden aan het medisch beroepsgeheim, willen zij zeker weten dat de gegevens alleen bij de patiënt zelf (of een gemachtigde) terechtkomen. Ook willen zij zekerheid over de vraag in welke mate zij aansprakelijk gesteld kunnen worden bij medische schade die het gevolg is van informatie uit persoonlijke gezondheidsomgevingen. Verder speelt dat de technische en organisatorische complexiteit van veel initiatieven rond elektronische dossiers niet bijdragen aan het vertrouwen in de bescherming van gegevens. Daarnaast speelt bij zorgaanbieders onzekerheid over de te kiezen oplossing voor hun interactie met

persoonlijke gezondheidsomgevingen; er zijn verschillende niet-gestandaardiseerde oplossingen denkbaar die geen van alle (nog) in staat zijn alle patiënten te bereiken. De vrees voor een lock-in of relatief hoge investeringen in de verkeerde oplossing leidt tot conservatief gedrag en een keuze voor oplossingen die vaak niet verder komen dan een aan de zorgaanbieder zelf verbonden digitale gezondheidsomgeving. Tot slot is er onduidelijkheid over de financiering van functionaliteiten en randvoorwaardelijke diensten rond de persoonlijke gezondheidsomgevingen. Het is niet helder op welke wijze investeringen door zorgaanbieders worden terugverdiend, hetzij doordat afzonderlijk wordt betaald voor informatiediensten, hetzij als component in de bekostiging van zorgproducten.

Voor de leveranciers van persoonlijke gezondheidsomgevingen speelt net zo goed onzekerheid over interoperabiliteit. Bij gebrek aan standaardisatie zijn veel investeringskeuzes risicovol, terwijl het daarbij niet gaat om verschillen waar de patiënt iets van zal merken. Het zijn veeleer keuzes van het type ‘rijden we links of rechts op de weg?’. Hoe meer partijen ‘op dezelfde weg rijden’, hoe groter het effect van een investering in de gestandaardiseerde optie. In termen van persoonlijke gezondheidsomgevingen betekent dit dat zoveel mogelijk zorginformatie kan worden ontsloten met dezelfde oplossing. Leveranciers van zorginformatiesystemen zien interoperabiliteit soms juist als bedreiging voor huidig marktaandeel, in plaats van als een kans voor vergroting ervan. Naast interoperabiliteitsvraagstukken spelen ook onzekerheden over de mogelijkheid om te voldoen aan de wettelijke eisen rond privacy. Zo zijn er nauwelijks generieke authenticatievoorzieningen beschikbaar die voldoende sterk zijn om omgevingen met persoonlijke gezondheidsinformatie te beveiligen. Ten slotte is voor leveranciers onduidelijk wie de financier en wie de klant is van diensten rond een persoonlijke gezondheidsomgeving.

Voor alle partijen geldt dat de afwezigheid van standaardisatie zich niet beperkt tot technische afspraken of ict alleen. Ook de variëteit die zich voordoet aan afspraken (of het gebrek daaraan) rond privacy, beveiliging, besturing, toezicht, handhaving, financiering, communicatie en dergelijke is een belemmering. Het many-to-many-kenmerk van de beoogde gegevensuitwisseling - een veelheid aan personen wisselt met behulp van een veelheid aan leveranciers gegevens uit met een veelheid aan zorgaanbieders - vereist een stevige standaardisatie, omdat het anders vrijwel onmogelijk is om een voor personen en zorgaanbieders werkbare en maatschappelijk betaalbare gegevensuitwisseling van de grond te krijgen.

De barrières bij personen, zorgaanbieders en leveranciers hebben een blokkerend effect op elkaar. Als vraag ontbreekt komt ook het aanbod niet van de grond, en vice versa. Er is sprake van een nog nauwelijks bestaande tweezijdige ‘markt’ die pas op gang komt als er een significante eerste stap wordt gezet door een van de spelers. De sleutel ligt bij het beïnvloeden van de karakteristieken van het aanbod, omdat daarmee zowel de barrières bij de aanbieders (zorgaanbieders en softwareleveranciers) als die bij personen kunnen worden geslecht.

Wat is er nodig om de barrières te overwinnen?

Personen zullen vertrouwen krijgen in persoonlijke gezondheidsomgevingen als zij zekerheid verkrijgen over de vertrouwelijkheid van hun gegevens. Transparantie – zien dat aan normen wordt voldaan – en reële aansprakelijkheid – toegankelijke verhaalsmogelijkheden als er toch schade ontstaat – zijn daarbij cruciaal. Deze combinatie zorgt ervoor dat papieren normen ook in de praktijk worden nageleefd.

Voor zorgaanbieders is van het belang dat het mogelijk is om personen betrouwbaar online te authenticeren, zodat vertrouwen ontstaat in het verstrekken van gegevens aan de juiste persoon. Voor aanbieders van persoonlijke gezondheidsomgevingen is het daarbij van belang dat er ook generieke authenticatiemogelijkheden beschikbaar zijn; het gaat om oplossingen die niet afhankelijk zijn van de specifieke ict-partij of zorgaanbieder, maar die tegen geringe kosten het gewenste hoge niveau van betrouwbaarheid bieden.

Interoperabiliteit is zowel voor zorgaanbieders als ict-leveranciers van groot belang om de risico’s van investeringen te verkleinen en voor een positief netwerkeffect te zorgen, waarbij zoveel mogelijk personen, ict-oplossingen en zorgaanbieders met elkaar worden verbonden. Dit vergroot de mogelijkheden tot kwalitatief betere en veiligere zorgverlening. De gegevensuitwisseling moet dan wel met zekerheid veilig zijn

en de privacy van betrokkenen voldoende beschermen. Onzekerheid over de financiering kan worden opgelost met een financieringsstructuur waarin duidelijk is welk type partijen bereid is waarvoor te betalen.

Welke opties zijn er om de barrières te overwinnen?

Om de eerdergenoemde barrières te overwinnen is een interventie nodig. De vorm van deze interventie kent vier opties:

1. Veelal wordt wetgeving ingezet als manier om collectieve belangen te borgen en eisen te stellen aan het gedrag van partijen op een markt. Ook in het domein van persoonlijke gezondheidsomgevingen is al veel generieke wetgeving van kracht en wordt op afzienbare termijn verdere aanscherping voorzien, onder andere door de Europese Algemene Verordening Gegevensbescherming. Voor de aanvullende interventies die specifiek betrekking hebben op persoonlijke gezondheidsomgevingen, zoals de hiervoor genoemde vraagstukken rond het ontbreken van een 'patiëntgeheim' en vraagstukken rond aansprakelijk kan de wenselijkheid van mogelijke wet- en regelgeving worden verkend. Er is echter nog weinig ervaring opgedaan met een succesvolle markt voor persoonlijke gezondheidsomgevingen, waardoor het verstandig is om voorlopig behoedzaam te zijn met wet- en regelgeving zodat voldoende flexibiliteit blijft bestaan. Wetgeving heeft als nadeel dat de doorlooptijd lang is, wat maakt dat het instrument vooral geschikt is als de gewenste richting al uitgekristalliseerd is.
2. Partijen als zorgaanbieders en eventueel zorgverzekeraars kunnen de markt ook stimuleren door hun inkoopmacht te gebruiken. Artsen schrijven nu soms ook al apps voor. Als er voldoende vragers op de markt zijn die hetzelfde kader hanteren, stimuleren zij daarmee andere partijen om hun normen over te nemen. Dit model vereist dat de vragende partijen hun wensen goed kunnen formuleren en ook bereid zijn om aanzienlijk te investeren. Op dit moment zijn de kaders voor een persoonlijke gezondheidsomgeving echter nog niet helder genoeg en kennen zorgaanbieders nog belemmeringen bij de uitwisseling ermee, waaronder juridische vraagstukken en andere zoals eerder genoemd.
3. Een model dat in het verleden veel is gehanteerd, is dat van centraal aangeboden voorzieningen. Door vanuit de overheid of andere dominante partijen zoals zorgverzekeraars een infrastructuur aan te bieden, worden veel keuzes op collectief niveau gemaakt en conformeren deelnemers zich als vanzelf. Voor persoonlijke gezondheidsomgevingen is dit model minder voor de hand liggend. Het concept van persoonlijke gezondheidsomgevingen is nog pril, en een duidelijke keuze voor een specifieke randvoorwaardelijke oplossing kan innovatie in de weg staan. Voor de aansluiting van zorgaanbieders geldt dat er al verschillende decentrale oplossingen bestaan. Een decentraal model sluit daarmee goed aan bij de ervaringen die de sector de afgelopen jaren heeft opgedaan met het ontsluiten van gezondheidsinformatie en maakt hergebruik van instituties en investeringen. Daarbovenop speelt dat er in de zorgsector weinig animo lijkt te zijn voor een centrale voorziening, mede vanwege politieke standpunten. Een keuze voor een centrale voorziening zal daarmee minder vertrouwen genieten, naast het feit dat met een dergelijke oplossing een potentieel single point of failure wordt geïntroduceerd.
4. De optie voor vrijwillige afspraken resteert. Deze afspraken zullen al snel de vorm krijgen van een afsprakenstelsel, omdat er tussen verschillende typen actoren verschillende typen afspraken nodig zijn. Vrijwillige afspraken hebben als kenmerk dat toe- en uittreding (onder voorwaarden) vrijwillig is. Wil een afsprakenstelsel effectief zijn, dan zal het zowel normstellend moeten zijn – in staat om de barrières te overwinnen – als aantrekkelijk genoeg voor partijen om zich aan te willen conformeren.

Wat zijn kenmerken van een goed afsprakenstelsel?

Om tot een goed afsprakenstelsel voor gegevensuitwisseling met persoonlijke gezondheidsomgevingen 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 persoonlijke gezondheidsomgevingen is een dergelijk model voorzienbaar; het zijn immers niet de persoon en de zorgaanbieder 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 zorgverleners) er zelf voor kiezen om wel of niet deel te nemen. Uiteraard is het wenselijk dat genoeg serieuze partijen deelnemen aan het afsprakenstelsel, omdat alleen dan een functionerende markt voor persoonlijke gezondheidsomgevingen zal ontstaan én het afsprakenstelsel dan niet gedomineerd kan worden door een handvol partijen. 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. Deelname moet ook voldoende voordelen bieden voor degenen die er moeite in steken; dit kan de vorm krijgen van kansen in de marketing, kennisvoordelen of in de operationele efficiëntie. Ook partijen die niet deelnemen aan het stelsel (free-riders) kunnen voordelen ondervinden van het ontstaan van een markt, maar het moet voor een serieuze partij aantrekkelijker blijven om wel te participeren in MedMij dan om alleen te profiteren van de beweging van anderen.

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 persoonlijke gezondheidsomgevingen enerzijds en anderzijds zorgaanbieders (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 personen en zorgaanbieders. Hiertoe wordt een afsprakenstelsel overeengekomen, bestaande uit afspraken op juridisch, organisatorisch, financieel, communicatief, semantisch en technisch gebied, zodat personen en zorgaanbieders 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.

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

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

Een persoonlijke gezondheidsomgeving met het MedMij-stempel is een waarborg voor betrouwbare grip op je gezondheidsgegevens. En dat biedt toegevoegde waarde voor de persoon. MedMij zegt dus iets over integriteit, validiteit, actualiteit en interoperabiliteit, maar niet over de inhoudelijke functionaliteit. Het gebruik van aanvullende functionaliteit 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 persoon via marktwerking. MedMij zegt om deze redenen niets over inhoudelijke functionaliteit en apps. Dat kan veranderen onder invloed van de verdere afspraken tussen persoon, zorgaanbieders, overheid en leveranciers over hetgeen preconcurrentieel en/of standaard gegarandeerd moet zijn voor de persoon in het MedMij-afsprakenstelsel.

Criteria

Doel

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.

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**

Regie over gezondheid versus zelfmanagement

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 patient en wat eHealth daaraan kan bijdragen.

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.
R1a	Voldoen aan Algemene Verordening Gegevensbescherming	De AVG zal van kracht zijn (25 mei 2018) kort nadat het MedMij-netwerk operationeel wordt. Het afsprakenstelsel baseert zich in haar ontwerp daarom direct al op de AVG.
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

Doel

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 zorgaanbieders en gezondheidsinformatie.
- Ontwikkelingsprincipes gaan over hoe het MedMij Afsprakenstelsel zich ontwikkelt en hoe die ontwikkeling gestuurd wordt.

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 zorgaanbieder	Informatieregie
6	MedMij spreekt alleen af wat nodig is	Neutraliteit
7	De persoon en de zorgaanbieder kiezen hun eigen dienstverlener	Speelveld
8	Aan de dienstverlener voor de persoon en voor de zorgaanbieder worden verschillende eisen gesteld	Informatieregie
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

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 zorgaanbiedersdomein. 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 zorgaanbieder vrij om wel of niet een zekere uitwisseling aan te gaan met een zekere zorgaanbieder respectievelijk persoon. Elke uitwisseling in het kader van het MedMij Afsprakenstelsel vindt plaats met goedvinden van persoon en zorgaanbieder. 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 zorgaanbieder 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 Zorgaanbieders, 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 Zorgaanbieders niet gehinderd in hun professionele praktijk en worden Personen in de gelegenheid gesteld regie te voeren over (de informatie over) hun gezondheid.

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, gateways naar 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 en dezelfde gegevens bij meerdere dienstverleners kan onderbrengen en actueel kan blijven houden.

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 zorgaanbieder kiezen hun eigen dienstverlener

De persoon en de zorgaanbieder 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 zorgaanbieder alle deelnemende dienstverleners persoon op het MedMij Netwerk gelijk moet behandelen en dat elke deelnemende dienstverlener persoon alle deelnemende dienstverleners zorgaanbieder 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.

Informatieregie

P5 - De persoon wisselt gegevens uit met de zorgaanbieder

Personen wisselen gezondheidsgegevens uit met zorgaanbieders. Veel van de gegevens zijn geregistreerd of worden gebruikt door 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 zorgaanbieder, waarbij de zorgaanbieder 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 zorgaanbieder 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.

P8 - Aan de dienstverlener voor de persoon en voor de zorgaanbieder worden verschillende eisen gesteld

De persoon en de zorgaanbieder staan in een ongelijke verhouding tot elkaar. Zo neemt de persoon het initiatief tot gegevensuitwisselingen, de zorgaanbieder is daarin volgend. De persoon is een niet-professionele partij die enige mate van bescherming verdient ten opzichte van de professionele zorgaanbieder. Wetgeving stelt in de regel eisen aan de zorgaanbieder en maar beperkt aan de persoon, maar is er wel op gericht om de persoon te beschermen. Vanuit de verschillende positie van de persoon en de zorgaanbieder volgt dat ook andere eisen gesteld moeten kunnen worden aan de dienstverlener persoon dan aan de dienstverlener zorgaanbieder. Dit betreft zowel de commerciële als de professionele afspraken.

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 zorgaanbiedersdomein. 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 zorgaanbieders. 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 zorgaanbieder. 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

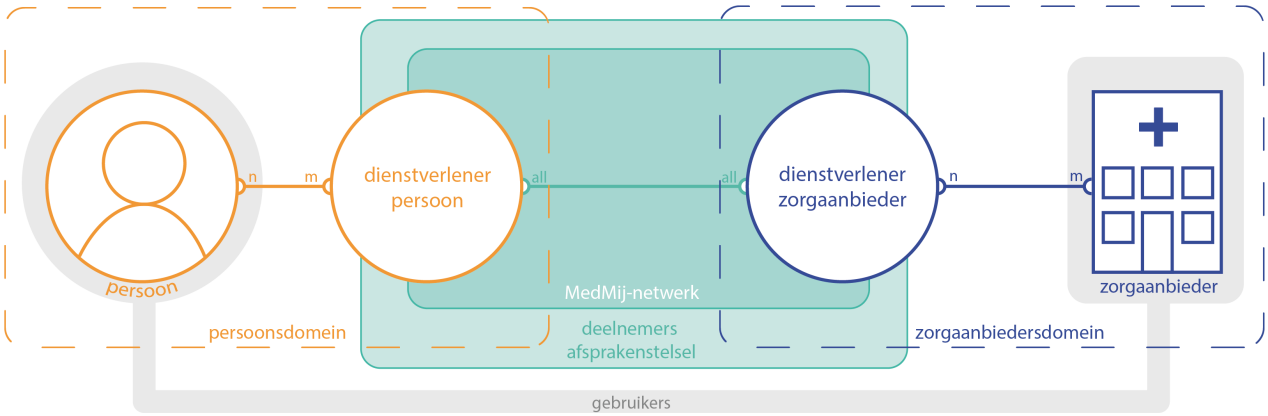
Het afsprakenstelsel wordt ontwikkeld in samenspraak met de belangrijkste stakeholders, waaronder vertegenwoordigers van de deelnemers, de gebruikers en partijen met een belang bij het functioneren van het stelsel. Dit zorgt ervoor dat ontwikkeling en gebruik zoveel mogelijk van elkaar profiteren, versnelling 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 initieel bepaald door het programma MedMij.

Opzet

Doel

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 Zorgaanbiedersdomein. 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 Zorgaanbieder (door hemzelf of namens hem door zijn Dienstverlener zorgaanbieder). 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 Zorgaanbieder en de door hem gekozen Dienstverlener zorgaanbieder vormen het Zorgaanbiedersdomein. De Zorgaanbieder kiest een of meer Dienstverleners zorgaanbieder. Een Dienstverlener zorgaanbieder kan actief zijn voor een of meer Zorgaanbieders. In de afbeelding is dit weergegeven als een n-op-m-relatie.

De Persoon en de Zorgaanbieder zijn Gebruiker van MedMij. De Dienstverlener persoon en de Dienstverlener zorgaanbieder zijn Deelnemer in het afsprakenstelsel. Alle Dienstverleners persoon en alle Dienstverleners zorgaanbieder vormen samen het MedMij-netwerk. Elke Dienstverlener persoon moet elke Dienstverlener zorgaanbieder 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 (dat volgt uit onder andere de technische en juridische uitwerking), 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 Zorgaanbieder digitaal over hem of haar beschikbaar heeft.	De Persoon verzoekt de Dienstverlener persoon om namens hem of haar de Dienstverlener zorgaanbieder te verzoeken de gevraagde gegevens zoals die bij de Zorgaanbieder bekend zijn te verzenden naar de Dienstverlener persoon.
2	De Persoon heeft de Zorgaanbieder gegevens over de gezondheid van de Persoon verstrekt.	De Persoon verzoekt de Dienstverlener persoon om namens hem of haar aan de Dienstverlener zorgaanbieder een door de Persoon aan de Dienstverlener persoon beschikbaar gestelde gegevensset te verzenden. De Dienstverlener zorgaanbieder informeert de Zorgaanbieder over de nieuwe gegevens.

Begrippenlijst

Doel

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

Begrip	Definitie	Synoniemen
Afsprakenstelsel	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
Deelnemer	Een partij die dienstverlening aanbiedt binnen het MedMij Afsprakenstelsel. De Dienstverlener persoon en de Dienstverlener zorgaanbieder zijn Deelnemer in het afsprakenstelsel en daarmee gebonden aan de afspraken, bekrachtigd door het tekenen van een deelnemersovereenkomst.	Dienstverlener persoon, Dienstverlener zorgaanbieder
Dienstverlener persoon	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 Zorgaanbieder mogelijk maakt middels het MedMij Afsprakenstelsel.	
Dienstverlener zorgaanbieder	Dit betreft een rol in het MedMij Afsprakenstelsel. 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.	
Gebruiker	Een partij die gebruik maakt van dienstverlening van deelnemers aan het afsprakenstelsel. De Persoon en de Zorgaanbieder zijn Gebruiker van MedMij.	
Gegevensdienst	Een gestandaardiseerde dienst voor gegevensuitwisseling met waarde voor de Gebruiker die door een Dienstverlener kan worden aangeboden 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.	
Gezondheidsgegeven	Gegeven betreffende de geestelijke en/of lichamelijke gesteldheid van een persoon.	Persoonlijke gezondheidsinformatie,

		gezondheidsinformatie
MedMij-netwerk	Alle Dienstverleners persoon en alle Dienstverleners zorgaanbieder vormen samen het MedMij-netwerk. Elke Dienstverlener persoon moet elke Dienstverlener zorgaanbieder kunnen bereiken, en vice versa.	Netwerk
Persoon	Degene, 16 jaar of ouder, op wie G ezondheidsgegevens betrekking hebben die via MedMij worden uitgewisseld en tevens de Gebruiker in het Persoonsdomein.	Betrokkene, burger, individu, gebruiker, patiënt, cliënt, zorgconsument
Persoonlijke gezondheidsomgeving	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.	PGO, persoonlijk gezondheidsplatform
Persoonsdomein	Alle Personen en alle Dienstverleners personen vormen samen het Persoonsdomein.	
Rol	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.	Functierol
Zorgaanbieder	Een instelling dan wel een solistisch werkende zorgverlener en tevens de Gebruiker in het Zorgaanbiedersdomein.	Zorginstelling, zorgorganisatie, brondossierhouder
Zorgaanbiedersdomein	Alle Zorgaanbieders en alle Dienstverleners zorgaanbieder vormen samen het Zorgaanbiedersdomein.	
Zorginformatiesysteem	Het systeem of geheel van de systemen waarin de zorgaanbieder het medisch dossier van de persoon bijhoudt.	XIS
Zorgverlener	Een natuurlijke persoon die beroepsmatig zorg verleent.	Professional

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.

Wetgeving	Toelichting	Toepassing
Wet bescherming persoonsgegevens (Wbp) (geldend vanaf 10-03-2017) Algemene Verordening Gegevensbescherming (AVG) (gepubliceerd 27-04-2016, geldend vanaf 25-05-2018)	MedMij-deelnemers verwerken persoonsgegevens. De Wet bescherming persoonsgegevens (Wbp) is daarmee van toepassing. De Wbp behelst de waarborgen voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. Een belangrijk onderdeel hiervan zijn de rechten van betrokkenen, zoals het recht op informatie en inzage. Vanaf 25 mei 2018 vervangt de Algemene Verordening Gegevensbescherming (AVG) de Wbp. Vanaf dat moment geldt in heel Europa dezelfde wetgeving. Ook de AVG beschrijft wanneer een verwerking van persoonsgegevens rechtmatig, behoorlijk en transparant is. De AVG gaat tegelijkertijd verder dan de Wbp. Zo moet iedere organisatie die persoonsgegevens verwerkt actief en controleerbaar kunnen aantonen dat zij zich aan de beginselen van een rechtmatig, behoorlijke en transparante verwerking van persoonsgegevens houdt. Door aan deze	Of een partij die met gebruik making 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 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

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.

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 aan de Persoon aanbiedt. 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. De AVG schrijft voor dat er passende beveiligingsmaatregelen moeten worden getroffen en dat partijen privacy by design en default hanteren als uitgangspunt (art. 25 AVG). Dit houdt in dat de gehanteerde instellingen standaard de meest privacyvriendelijke moeten zijn en dat al vroeg bij het ontwerp en in het ontwikkelproces aandacht moet zijn voor het zorgvuldig verwerken van de persoonsgegevens. Kortom, de verwerkingsverantwoordelijke dient bij de verwerking van de persoonsgegevens een zo klein

		mogelijke inbreuk te maken op persoonlijke levenssfeer. De beveiligingsmaatregelen die deelnemers op basis van het MedMij Afsprakenstelsel moeten nemen, staan uitgewerkt in het Normenkader informatiebeveiliging. 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. Aangezien het hier bijzondere persoonsgegevens betreft dient er extra aandacht te zijn voor deze risico's. Verder is het artikel onder meer de meldplicht datalekken van belang: artikel 33 AVG. In het afsprakenstelsel zijn partijen gebonden aan deze meldplicht. Zie hiervoor ook de Guidelines on Personal data breach notification van de Europese privacytoezichthouders. In de AVG wordt dataportabiliteit verplicht. Hierdoor moet een persoon kunnen wisselen van persoonlijke gezondheidsomgeving zonder dat de persoon hierbij data verliest. Daarbij moet de opgeslagen informatie over de persoon probleemloos meegenomen kunnen worden. Het recht op dataportabiliteit is ook van belang in de relatie tussen Persoon en Zorgaanbieder. De Zorgaanbieder moet de persoonsgegevens aan de persoon kunnen aanbieden in een gangbaar machineleesbaar (gestructureerd) bestandsformaat. MedMij geeft invulling aan deze wettelijke bepaling doordat informatie gestructureerd uitgewisseld kan worden. 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. De toestemming moet zijn gebaseerd op duidelijke informatie over de verwerking van de persoonsgegevens. Hierbij dient ten minste aandacht te zijn voor het

		doel van het verwerken, welke specifieke gegevens verwerkt worden en dat de toestemming is in te trekken. Het intrekken van de toestemming dient net zo eenvoudig te zijn als het verlenen van de toestemming. Indien de Dienstverlener persoon het ook mogelijk maakt via het MedMij Afsprakenstelsel gegevens te delen met een zorgaanbieder dient in de toestemmingsverklaring tevens duidelijk te zijn welke gegevens voor dit doel met instemming van de Persoon worden verwerkt. Zie ook Toelichting verwerkingsverantwoordelijkheid voor een nadere toelichting op dit onderwerp. Wanneer de Dienstverlener persoon met een 'derde partij' werkt dient ook dit duidelijk vermeld te zijn in de toestemmingsverklaring en dient de Dienstverlener persoon met deze derde een verwerkersovereenkomst te sluiten voor dit specifieke doel. Overige verplichtingen die voor de 'verwerkingsverantwoordelijke' en 'verwerker' uit de AVG voortvloeien zijn onder andere het aanstellen van een Functionaris voor gegevensbescherming, het opstellen van een privacy- en gegevensbeschermingsbeleid, de uitvoering van een PIA en de inrichting van een zogenoemd register van verwerkingsactiviteiten (hierna: verwerkingsregister) voor de verwerkingen van persoonsgegevens. In dit verwerkingsregister dient onder andere informatie te worden opgenomen over de doelen voor de verwerking van persoonsgegevens, de gehanteerde bewaartermijnen en een beschrijving van de beveiligingsmiddelen. Voor de verwerkingen die in het verwerkingsregister zijn opgenomen, zullen ook de benodigde procedures en maatregelen moeten worden ingericht om aantoonbaar en controleerbaar te voldoen aan de AVG. Het gaat dan bijvoorbeeld om de eerder genoemde procedure in het kader van de meldplicht datalekken,

		maar ook om procedures en maatregelen voor de informatieverstrekking en de communicatie over de verwerking van persoonsgegevens, het binnen de wettelijke termijn opvolging geven aan rechten van betrokkenen, de waarborging van de kwaliteit van de gegevensverwerking en procedures die betrekking hebben op de naleving van bewaartermijnen en de kwaliteit van de verwerking van persoonsgegevens. Zie ook de artikelen 5, 12 t/m 23, 24, 25, 28, 29, 30, 32, 33, 34, 35, 36 en 37 AVG. 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.
Wet op de geneeskundige behandelingsovereenkomst (WGBO) (geldend vanaf 01-02-2006)	De Wet op de geneeskundige behandelingsovereenkomst (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).	Zorgaanbieders dienen de wettelijke bepalingen te volgen voor dossiervorming. Een persoonlijke 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 Gebruiksvoorlichting persoonsdomein 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)	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

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.

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

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 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

		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. 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.	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 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.
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 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	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 kunnen wel gevolgen hebben voor de positie van de Deelnemer in het MedMij Afsprakenstelsel.

	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 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. Leveranciers van dergelijke toepassingen dienen zelf een afweging te maken met betrekking tot de toepassing van deze verordening voor hun eigen dienstverlening.

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.
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 verkoopruimten (bijvoorbeeld colportage) geregeld. Ook wordt er voor verkoop op afstand en buiten verkoopruimten het herroepingsrecht (bedenktijd voor de consument) geregeld.	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 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

Aansprakelijkheid	Voor de aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en 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 het MedMij Afsprakenstelsel is iedere deelnemer aansprakelijk voor zijn eigen handelen en/of nalaten 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.

Toelichting verwerkingsverantwoordelijkheid

Inleiding

Het MedMij Afsprakenstelsel onderscheidt een tweetal use cases voor de gegevensuitwisseling tussen de Persoon en zijn Zorgaanbieder, namelijk de use case Verzamelen en de use case Delen. Op basis van de use case Verzamelen kan de Persoon zijn gegevens en gezondheidsinformatie in zijn PGO inkijken, opslaan en beheren. Op basis van de use case Delen kan de Persoon gegevens en gezondheidsinformatie vanuit zijn PGO aan zijn Zorgaanbieder aanbieden opdat de Zorgaanbieder deze informatie kan opnemen in zijn medisch dossier.

In de uitvoering van de use case Verzamelen en de use case Delen zijn verschillende partijen betrokken. Hieronder wordt voor de voornoemde use cases 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 zowel de use case Verzamelen als de use case Delen geldt dat in het geval de Persoon gegevens en /of gezondheidsinformatie met zijn Zorgaanbieder wil uitwisselen, de Zorgaanbieder de Persoon 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. Immers de Zorgaanbieder is 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 - de 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 ZA 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 DVZA en de ZA 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. Authenticatie van de Persoon is derhalve een aparte rechtstreekse rechtshandeling tussen de Zorgaanbieder (via de Dienstverlener zorgaanbieder) en de Persoon. Zonder deze authenticatie worden er geen gegevens uitgewisseld.

UC Verzamelen en UC Delen

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 persoonsgegevens en/of 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 de 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 voor de verwerking van de gegevens over de gezondheid van persoon (bijzonder persoonsgegeven) in relatie tot de PGO in deze is 'uitdrukkelijke toestemming' (art 9 lid 2 sub a AVG). Daarnaast is de rechtmatigheidsgrondslag ‘noodzakelijk voor de uitvoering van de overeenkomst’ (art. 6 lid 1 sub b AVG) voor de verwerking van de gewone persoonsgegevens. 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.

In het kader van de use case Verzamelen van de persoonsgegevens en/of gegevens over de gezondheid van de Persoon dient de Persoon zijn toestemming aan de Zorgaanbieder te hebben verleend opdat de Dienstverlener persoon deze gegevens die hij - via het MedMIj-netwerk (via de DVZA) - over de Persoon van de ZA 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 ZA (via de DVZA) 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.

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 (via de Dienstverlener persoon persoonsgegevens en/of gegevens over de gezondheid van de Persoon (via 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 (via 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 zogenaamde autorisatiecode aan de Dienstverlener Persoon van de Persoon op basis waarvan de Dienstverlener 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 autorisatiecode te gebruiken bij de ue case Delen wordt gewaarborgd dat de Dienstverlener persoon ook in de use case Delen geen BSN verwerkt. Gelet op het feit dat de Dienstverlener wel een autorisatiecode 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.

Overeenkomsten en rechtsrelaties

Het MedMij Afsprakenstelsel waarborgt dat binnen het MedMij-netwerk op een veilige en betrouwbare manier persoonsgegevens en/of gezondheidsinformatie tussen de Deelnemers worden uitgewisseld. Om dit te bewerkstelligen behelst het MedMij Afsprakenstelsel informatiestandaarden, technische, organisatorische en juridische afspraken. Als gevolg van het afsluiten van de Deelnemersovereenkomst met de Stichting MedMij - nadat hiertoe de toetredingsprocedure succesvol is doorlopen - worden de Dienstverleners Zorgaanbieders en Dienstverlener Personen Deelnemer van het MedMij Afsprakenstelsel. Iedere partij die aantoonbaar voldoet aan de afspraken van het MedMij Afsprakenstselsel 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 onder de merknaam MedMij. Om deze Diensten via het MedMij-netwerk te kunnen leveren zijn deze partijen toegetreden tot het MedMij Afsprakenstelsel. De Persoon en de Zorgaanbieder zijn Gebruiker van Diensten van Deelnemers in het MedMij Afsprakenstelsel.

De Deelnemers zijn zelf verantwoordelijk voor het afsluiten van dienstverleningsovereenkomsten met hun Gebruikers. Deelnemers zijn immers ook 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 wel goed aansluiten op de Diensten, die met inzet van het MedMij-netwerk, worden geleverd, wordt vanuit het MedMij Afsprakenstelsel informatie ter beschikking gesteld die door de Deelnemer kan worden gebruikt bij het afsluiten van zijn dienstverleningsovereenkomst met de Gebruiker. Voorbeelden van informatie die via het MedMij Afsprakenstelsel voor Deelnemers ter beschikking wordt gesteld zijn de Gebruiksvoorlichting persoonsdomein, Gebruiksvoorlichting zorgdomein en de Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener Zorgaanbieder.

De Gebruiker bepaalt zelf of hij/zij gebruik wil maken van een persoonlijke gezondheidsomgeving. Zo ja, kiest hij/zij een persoonlijke gezondheidsomgeving en kan controleren of deze tevens Deelnemer is en Diensten aanbiedt conform het MedMij Afsprakenstelsel in de lijst van Deelnemers die op de website van het MedMij Afsprakenstelsel is 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 deze partijen binnen de architectuur vervullen, de functies die zij op de verschillende netwerklagen 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. Het gaat dan om de volgende 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 als Gebruiker die Diensten afneemt van de Dienstverlener Zorgaanbieder, en
6. de Persoon als Gebruiker die Diensten afneemt van de Dienstverlener Persoon.

Rechtsrelaties MedMij Afsprakenstelsel

Hieronder is het overzicht opgenomen van rechtsrelaties tussen de 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 voor hun Gebruikers fungeren. Er is sprake van vertegenwoordiging. 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 de Deelnemers en de Stichting MedMij binden aan het nakomen van de afspraken in het MedMij Afsrakenstelsel. De Deelnemers zijn verantwoordelijk voor de doorvertaling van de afspraken naar hun klanten en derden. 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 overzicht opgenomen van rechtsrelaties die van wezenlijke invloed zijn op het vertrouwen in en een veilige en betrouwbare verwerking van en gegevensuitwisseling via het MedMij Afsprakenstelsel. 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

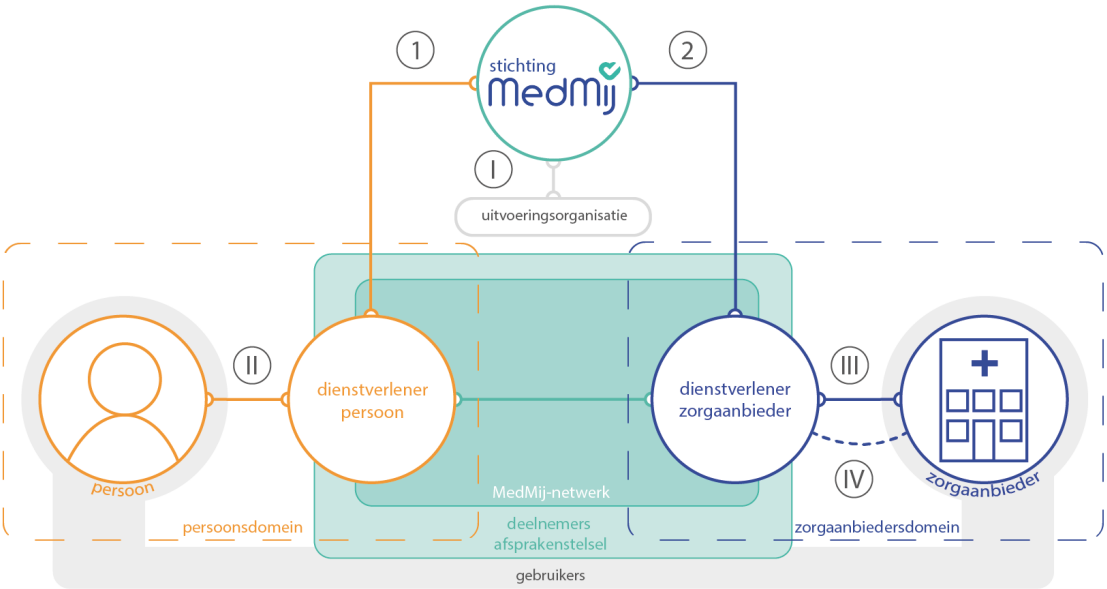
hebben. Dat betekent dat afspraken tussen deze partijen ook randvoorwaardelijk zijn voor een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de persoonlijke gezondheidsomgeving MedMij en de informatiesystemen van de Zorgaanbieders.

Rechtsrelaties die van belang zijn voor MedMij	Type overeenkomst
I. Stichting MedMij - Beheer /uitvoeringsorganisatie	Opdrachtverlening voor ondersteuning en uitvoering van taken van Stichting MedMij zoals: 1. De instandhouding van de goede technische werking van de gemeenschappelijke voorzieningen in het afsprakenstelsel. 2. Het voeren van de regie over de werking van het Netwerk en het beheer van het MedMij Afsprakenstelsel.
II. Dienstverlener Persoon - Gebruiker	Dienstverleningsovereenkomst Persoon. Binnen het MedMij Afsprakenstelsel wordt voor deze rechtsrelatie de Gebruiksvoorlichting persoonsdomein ter beschikking gesteld.
III. Dienstverlener Zorgaanbieder - Gebruiker	Binnen het MedMij Afsprakenstelsel wordt voor deze rechtsrelatie de Gebruiksvoorlichting zorgdomein ter beschikking gesteld
IV. Zorgaanbieder – Dienstverlener Zorgaanbieder	Verwerkersovereenkomst

De rechtsrelaties genoemd onder I t/m IV vallen buiten 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 - wel degelijk tussen de betrokken partijen te worden afgesloten. Partijen zijn echter zelf verantwoordelijk voor het afsluiten van deze overeenkomsten.

De uitvoering van verwerkingen door een Verwerker dient 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 de Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener zorgaanbieder te gebruiken. In het geval er al een bestaande overeenkomst is afgesloten tussen Verwerker en Verwerkingsverantwoordelijke kunnen partijen ervoor kiezen de specifieke bepalingen in relatie tot de verwerking van persoonsgegevens voor MedMij uit de Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener zorgaanbieder te integreren in de bestaande verwerkersovereenkomst. Hierbij is te denken aan zaken zoals het verwerken van burgerservicenummer ten behoeven van authenticatie, 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.

Alle rechtsrelaties zijn privaatrechtelijk van aard en alle deelnemers zijn gebonden aan Nederlands recht. De figuur hieronder geeft de verschillende rechtsrelaties weer.


1
stichting MedMij
2
I
uitvoeringsorganisatie
II
dienstverlener persoon
dienstverlener zorgaanbieder
III
IV
persoon
zorgaanbieder
MedMij-netwerk
deelnemers afsprakenstelsel
persoonsdomein
zorgaanbiedersdomein
gebruikers

Deelnemersovereenkomsten

De Deelnemersovereenkomst bevat de basisafspraken tussen Stichting MedMij en een deelnemer aan het afsprakenstelsel. Aangezien er twee type deelnemers zijn, wordt onderscheid gemaakt tussen een Deelnemersovereenkomst Dienstverlener persoon en een Deelnemersovereenkomst Dienstverlener zorgaanbieder. 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

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 zorgaanbieder.

Partijen

De <Stichting MedMij>, voor deze <functie> , <naam>,

Verder te noemen: Stichting MedMij

en

<Naam partij > gevestigd te <adres>, te dezen vertegenwoordigd door <naam> , voor deze <functie>, <naam>,

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 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 Deelnemer: een organisatie die is toegetreden tot het MedMij Afsprakenstelsel en overeenkomstig hetgeen daarover in het MedMij Afsprakenstelsel is opgenomen de rol van Dienstverlener persoon of Dienstverlener zorgaanbieder vervult.

1.3 Dienstverlener persoon: dit betreft een rol in het MedMij Afsprakenstelsel. De Dienstverlener persoon levert een Persoonlijke gezondheidsomgeving, 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.

1.4 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

1.5 Dienst(en): activiteiten, processen en functionaliteit van de Dienstverlener persoon aan de Persoon ten einde de gegevensuitwisseling tussen Gebruikers te realiseren overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

1.6 Gebruiker: de afnemer van de Dienst(en) van de Dienstverlener persoon of een afnemer van de Dienst (en) van de Dienstverlener zorgannbieder.

1.7 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.

1.8 MedMij Afsprakenstelsel: de door de Stichting MedMij vastgestelde laatst geldende release van het MedMij Afsprakenstelsel.

1.9 Merk: (de) woordmerk(en) en/of beeldmerk(en) ten aanzien waarvan Stichting MedMij het merkenrecht uitoefent.

1.10 Netwerk: het MedMij-netwerk zoals gedefinieerd in het MedMij Afsprakenstelsel.

1.11 Overeenkomst: deze Deelnemersovereenkomst.

1.12 Persoon: Persoon die gebruik wenst te maken van een PGO welke gegevens kan uitwisselen met de Zorgaanbieder conform het MedMij Afsprakenstelsel.

1.13 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.

1.14 Stichting MedMij: beheerder van het MedMij Afsprakenstelsel

1.15 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.

1.16 Zorgaanbieder: zorgaanbieder 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 ten minste één Gegevensdienst aan de Persoon aan te bieden.

2.4 De Deelnemer is 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 zijn rol zijn vastgesteld en in werking zijn getreden, na te komen. Dit houdt in dat Deelnemer zich conformeert en houdt 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 Communicatie.

2.5 De Deelnemer erkent de Governance van het MedMij Afsprakenstelsel.

2.6 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.

2.7 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.

2.8 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.

2.9 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 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 gebuikt voor de koppeling met de netwerkverbindingen en/of - systemen van de Persoon.

5.5 Persoonsgegevens mogen door de Deelnemer alleen met uitdrukkelijke toestemming van de Persoon worden verwerkt met als doel het geven van inzicht en regie over de gezondheid van de desbetreffende Persoon. Deze gegevens mogen door de Deelnemer niet verder worden verwerkt op een manier die onverenigbaar is met het oorspronkelijke doel waarvoor de persoonsgegevens zijn verkregen, tenzij ook daar uitdrukkelijke toestemming van de Persoon voor is gegeven.

5.6 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.

5.7 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 één op één door naar (sub)verwerkers. De uitvoering van 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 naleeft.

9.2 De Deelnemer verleent zijn medewerking aan een onderzoek tot naleving van het MedMij Afsprakenstelsel 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 en MedMij Afsprakenstelsel en die via het MedMij Afsprakenstelsel openbaar worden gemaakt, komen toe aan Stichting MedMij.

11.2 Alle auteursrechten die 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 persoon.

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 eerder overeenkomsten en/of bindende afspraken tussen Partijen in relatie tot het MedMij Afsprakenstelsel.

14.2 De Deelnemer is in de Europese Unie ingeschreven in het 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 zorgaanbieder

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 zorgaanbieder.

Partijen

De <Stichting MedMij>, voor deze <functie> , <naam>,

Verder te noemen: Stichting MedMij

en

<Naam partij> gevestigd te <adres>, te dezen vertegenwoordigd door <naam> , voor deze <functie>, <naam>,

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. het de Deelnemer wordt toegestaan Diensten aan te bieden. De Deelnemer committeert zich hiervoor aan de laatst geldende release 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 Deelnemer: een organisatie die is toegetreden tot het MedMij Afsprakenstelsel en overeenkomstig hetgeen daarover in het MedMij Afsprakenstelsel is opgenomen de rol van Dienstverlener zorgaanbieder of Dienstverlener persoon vervult.

1.3 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.

1.4 Dienstverlener persoon: dit betreft een rol in het MedMij Afsprakenstelsel. De Dienstverlener persoon levert een Persoonlijke gezondheidsomgeving, 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 Dienst(en): activiteiten, processen en functionaliteit van de Dienstverlener zorgaanbieder aan de Zorgaanbieder ten einde de gegevensuitwisseling tussen de Zorgaanbieder en de Persoon van 16 jaar of ouder te realiseren overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

1.6 Gebruiker: afnemer van de Dienst(en) van de Dienstverlener zorgaanbieder of een afnemer van de Dienst (en) van de Dienstverlener persoon.

1.7 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.

1.8 MedMij Afsprakenstelsel: de door de Stichting MedMij vastgestelde laatst geldende release van het MedMij Afsprakenstelsel.

1.9 Merk: (de) woordmerk(en) en/of beeldmerk(en) ten aanzien waarvan Stichting MedMij het merkenrecht uitoefent.

1.10 Netwerk: het MedMij-netwerk zoals gedefinieerd in het MedMij Afsprakenstelsel.

1.11 Overeenkomst: deze Deelnemersovereenkomst.

1.12 Persoon: Persoon die gebruik wenst te maken van een PGO welke gegevens kan uitwisselen met de Zorgaanbieder conform het MedMij Afsprakenstelsel.

1.13 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.

1.14 Stichting MedMij: beheerder van het afsprakenstelsel MedMij.

1.15 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.

1.16 Zorgaanbieder: zorgaanbieder 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 ten minste één Gegevensdienst aan zijn Gebruikers aan te bieden.

2.4 De Deelnemer is 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 zijn rol zijn vastgesteld en in werking zijn getreden, na te komen. Dit houdt in dat Deelnemer zich conformeert en houdt 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 Communicatie.

2.5 De Deelnemer erkent de Governance van het MedMij Afsprakenstelsel.

2.6 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.

2.7 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.

2.8 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.

2.9 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 zijn Gebruiker;
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 thans 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 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 gebuikt voor de koppeling met de netwerkverbindingen en/of - systemen van de Zorgaanbieder.

5.5 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.

5.6 Voor de Diensten van de Deelnemer die geschieden in opdracht van de Zorgaanbieder wordt gebruik gemaakt van de Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener zorgaanbieder, tenzij Deelnemer en Zorgaanbieder anders overeen zijn gekomen in een eigen verwerkersovereenkomst die dezelfde dienstverlening en bijbehorende onderwerpen omvat.

5.7 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 één op één door naar (sub)verwerkers. De uitvoering van verwerking door een 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 naleeft.

9.2 De Deelnemer verleent zijn medewerking aan een onderzoek tot naleving van het MedMij Afsprakenstelsel 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 en MedMij Afsprakenstelsel en die via het MedMij Afsprakenstelsel openbaar worden gemaakt, komen toe aan Stichting MedMij.

11.2 Alle auteursrechten die 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 als 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 eerder overeenkomsten en/of bindende afspraken tussen Partijen in relatie tot het MedMij Afsprakenstelsel.

14.2 De Deelnemer is in de Europese Unie ingeschreven in het 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>

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 zorgaanbieder 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 Opdrachtnemer verwerkt geen Persoonsgegevens buiten een land van de Europese Unie/Europese Economische ruimte zonder een passend beschermingsniveau, tenzij Opdrachtgever daarvoor uitdrukkelijk toestemming heeft gegeven.

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 in een land buiten de EU zonder een passend beschermingsniveau toestemming vereist is in overeenstemming met artikel 3.10 van deze Verwerkersovereenkomst.

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, 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.

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.

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]

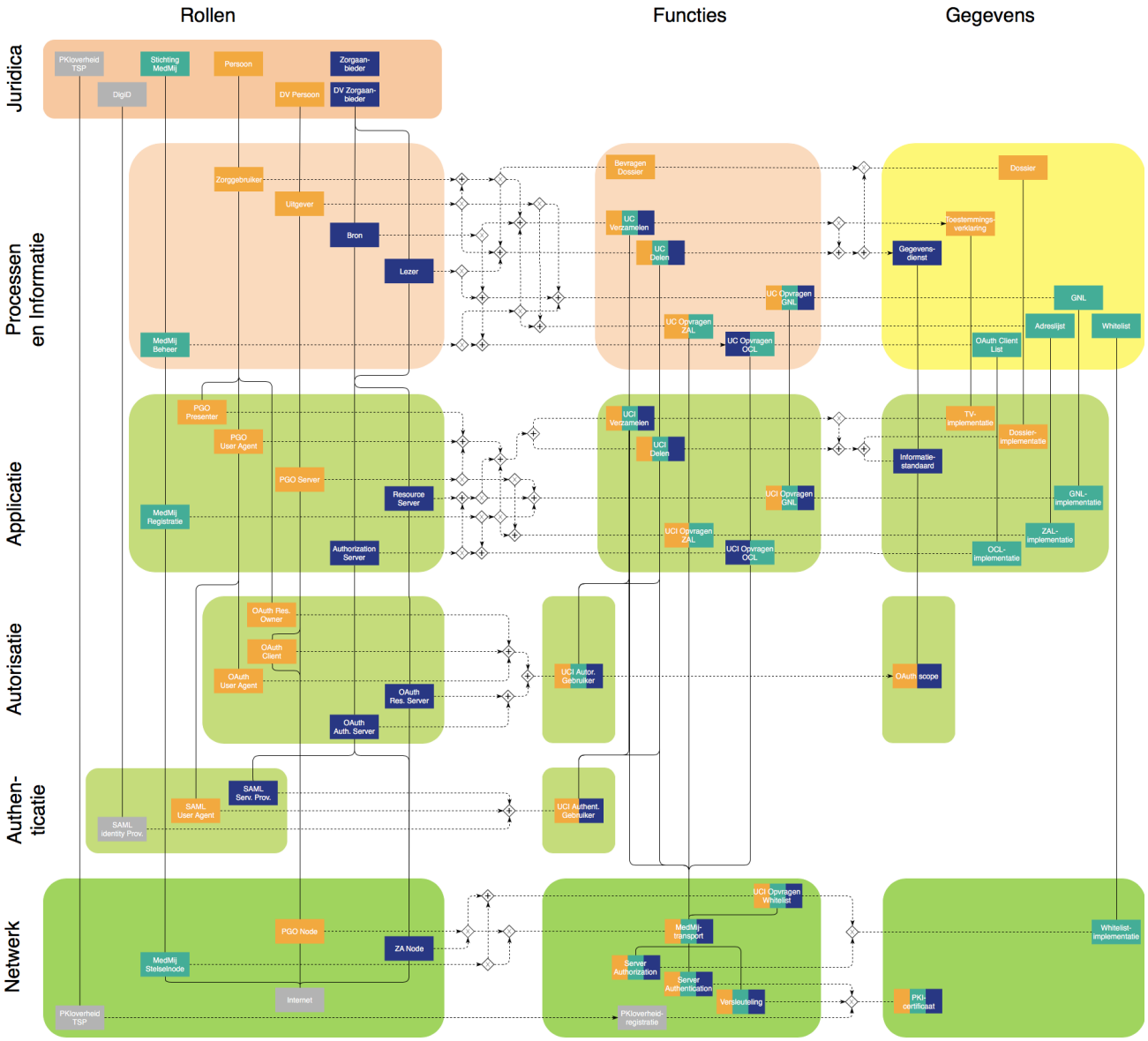
Noot

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.

Architectuur en technische specificaties

De totale architectuur van het MedMij Afsprakenstelsel is weergegeven in onderstaande figuur.



Toelichting De architectuur is geïnspireerd op het interoperabiliteitsmodel van Nictiz. Dit model is op een aantal wezenlijke punten aangepast voor gebruik binnen MedMij. Er is een driedeling in kolommen toegevoegd: rollen, functies en gegevens. Op elke laag spelen voor die laag specifieke rollen, die voor die laag specifieke functies uitvoeren met behulp van voor die laag specifieke gegevens. Om die reden zijn de proceslaag en de informatielaag uit het interoperabiliteitsmodel van Nictiz gecombineerd in één laag, waaraan bovendien een rollenkolom is toegevoegd.

Omdat het om een architectuur van een afsprakenstelsel gaat, niet om die van een oplossing, speelt de rollenkolom een sleutelrol in de samenhang van de gehele architectuur. Rollen zijn immers bundels van verantwoordelijkheden. Die verantwoordelijkheden zijn gekoppeld aan uit te voeren functies (tweede kolom), die op hun beurt gebruik maken van gegevens (derde kolom).

Verder is de applicatielaag verfijnd door twee deellagen af te zonderen: een autorisatielaag en een authenticatielaag. Dat komt doordat voor deze twee kwesties standaarden worden gebruikt die hun eigen rollenmodel hebben, waarmee dus expliciete binding moet worden gerealiseerd. Bovendien is het zo mogelijk om de afspraken die specifiek voortvloeien uit het ontwerp van die standaard een herkenbare en beheersbare plaats te geven.

Niet op alle lagen zijn in de architectuur van het MedMij Afsprakenstelsel alle kolommen ingevuld:

- De bovenste laag kent alleen juridische rollen, niet de andere twee kolommen. Die laatste staan behandeld op de pagina Overeenkomsten en rechtsrelaties. De koppeling van de rest van de architectuur met juridische rollen is evengoed van groot belang, zodat duidelijk wordt welke architecturale en technische verantwoordelijkheden verbonden zijn aan welke juridische rollen.
- Op de authenticatielaag is het niet nodig nadere afspraken te maken over gegevens. Daarvoor kan geheel teruggevallen worden op de specificaties van het SAML-koppelvlak van DigiD.

De kleuren van de grote vlakken komen overeen met de kleuren die Nictiz aan de betreffende architectuuraspecten geeft in haar interoperabiliteitsmodel. De kleuren van de architectuurelementen (de kleine rechthoeken) geven aan in welk domein het betreffende architectuurelement geplaatst is. Daarbij is allereerst de huisstijl van MedMij aangehouden, zodat:

- oranje staat voor het Persoonsdomein;
- blauw staat voor het Zorgaanbiedersdomein en
- groen staat voor het MedMij-domein.

De grijze kleur staat voor externe rollen waarvan het MedMij Afsprakenstelsel gebruik maakt. Waar meerdere kleuren zijn gecombineerd, geeft dat aan dat in het betreffende architectuurelement de domeinen samenwerken.

De verticale lijnen in de architectuur verbinden de rollen, functies en gegevens tussen de verschillende lagen. Met de horizontale stippellijnen staat aangegeven welke rollen welke functies uitvoeren, respectievelijk welke functies welke gegevens gebruiken. Om te voorkomen dat er een onoverzichtelijke wirwar van stippellijnen ontstaat, maakt de figuur gebruik van joins en splits. Joins en splits zijn getekend als ruitjes. Een join (samenkomst) kenmerkt zich door meerdere inkomende pijlen en één uitgaande, een split (splitsing) juist door één inkomende en meerdere uitgaande pijlen.

De twee soorten onderscheiden zich door het teken in het ruitje:

- Een maalteken staat voor exclusief, wat wil zeggen dat slechts één van de inkomende pijlen (bij joins) of uitgaande pijlen (bij splits) tegelijk aan de orde is.
- Een plusteken staat voor inclusief, wat wil zeggen dat altijd alle inkomende pijlen (bij joins) of uitgaande pijlen (bij splits) tegelijk aan de orde zijn.

Zo is bijvoorbeeld, op de laag *Processen en Informatie*, de rol *MedMij Beheer* betrokken:

- in zes use cases: *UC Verzamelen*, *UC Delen*, *UC Opvragen ZAL*, *UC Opvragen OCL*, *UC Opvragen Whitelist* en *UC Opvragen GNL* maar niet tegelijk (exclusief).
- in de use case *UC Opvragen ZAL* tegelijk (inclusief) met de rol *Uitgever*.

Voor elke laag staan de afspraken uitgewerkt op een aparte pagina:

- Juridica
- Processen en Informatie
- Applicatie, inclusief Authenticatie en Autorisatie

- Netwerk

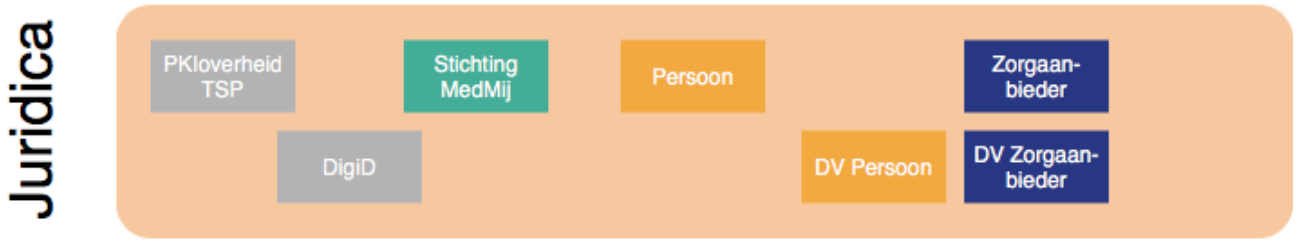
Die afspraken bestaan steeds uit:

- de identificatie van de rollen op die laag en de binding van die rollen aan de rollen op de laag erboven;
- de verantwoordelijkheden die de rollen op deze laag hebben in het uitvoeren van zekere functies met zekere gegevens.

Vaak wordt er in de verantwoordelijkheden verwezen naar een specificatie. Dit kan een specifiek voor MedMij gespecificeerde use case zijn, bijvoorbeeld, maar is vaak ook een standaard, vooral voor informatie. De specificatie zal niet in de verantwoordelijkheid zelf staan uitgeschreven; er zal naar verwezen worden. Zo hoeft voor detailaanpassingen in de specificatie niet steeds de verantwoordelijkheid te worden aangepast. Dat zou, zeker bij standaardspecificaties, een ongewenste beheerslast van het afsprakenstelsel opleveren.

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 setje 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?*

Juridica



Toelichting

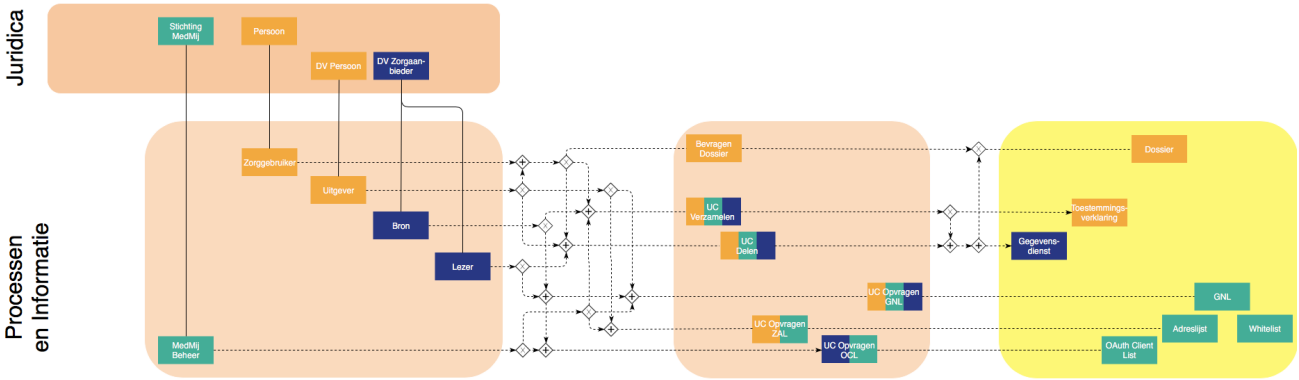
In deze laag staan de juridische rollen, als juridische basis voor de rollen op andere lagen van de architectuur. De enige reden dat deze laag in deze architectuur is opgenomen is dat rollen voor de samenhang tussen de verschillende architectuurlagen zorgen en de architectuur ook geborgd moet zijn in de juridische rollen in het MedMij Afsprakenstelsel. Bij een juridische rol horen verplichtingen voor het spelen van rollen op verschillende architectuurlagen.

De rollen die we hier in de architectuur noemen vallen uiteen in twee groepen:

1. de *directe* juridische rollen, die partij zijn in MedMij-deelnemersovereenkomsten: *Dienstverlener persoon*, *Dienstverlener zorgaanbieder* en *Stichting MedMij*.
2. de *indirecte* juridische rollen die geen partij zijn in MedMij-deelnemersovereenkomsten, maar niettemin een uitvoerende verplichting hebben in de architectuur. Dat betekent dat de toepasselijke deelnemersovereenkomst van een deelnemer zal eisen dat deze een juridische relatie aangaat met die juridische rol. Het gaat hier om *DigiD*, *PKIoverheid TSP*, *Persoon* en *Zorgaanbieder*.

In de architectuur van het afsprakenstelsel heeft de *Persoon* een operationele rol bij authenticatie en autorisatie van het gegevensverkeer. De *Zorgaanbieder* wordt operationeel geheel vertegenwoordigd door de *Dienstverlener Zorgaanbieder*.

Processen en informatie



Toelichting

Voor een overzicht over alle lagen van de architectuur, en voor een toelichting van de betekenis van de symbolen en lijntjes, zie de overzichtspagina.

In deze figuur zijn de rollen, functies en gegevens-elementen uit de proces- en informatie-architectuur weergegeven, inclusief de binding (verticale lijnen) van deze rollen aan de juridische (zie Juridica). Met de horizontale stippellijnen staat aangegeven welke rollen welke functies uitvoeren, respectievelijk welke functies welke gegevens gebruiken. Om te voorkomen dat er een onoverzichtelijke wirwar van stippellijnen ontstaat, maakt de figuur gebruik van joins en splits. Joins en splits zijn getekend als ruitjes. Een join (samenkomst) kenmerkt zich door meerdere inkomende pijlen en één uitgaande, een split (splitsing) juist door één inkomende en meerdere uitgaande pijlen.

Rollen

1. *Dienstverlener persoon* neemt de functionele rol van *Uitgever* op zich.
2. *Dienstverlener zorgaanbieder* neemt de functionele rol van *Bron* en/of *Lezer* op zich.
3. *Stichting MedMij* neemt de functionele rol van *MedMij Beheer* op zich.
4. *Persoon* neemt de functionele rol van *Zorggebruiker* op zich.

Toelichting

Met de rollen *Uitgever, Bron* en *Lezer* staat hier de principiële keus die het afsprakenstelsel maakt voor de aard van de regie die zij aan personen wil geven over de gezondheidsinformatie waarvan zijzelf het onderwerp zijn. Er zijn andere regiemodellen mogelijk, zwakkere en sterkere. In dit model is de *Dienstverlener persoon*, namens de *Persoon*, *Uitgever* van zijn/haar gezondheidsinformatie, betrekt die informatie daartoe van *Bronnen* en stelt die informatie beschikbaar aan *Lezers*. Zo krijgt de *Persoon* de regie die MedMij hem wil bieden. In deze release van het afsprakenstelsel haalt *Uitgever* de informatie op bij *Bronnen*, maar deelt hij nog geen informatie met *Lezers.*

In het persoonsdomein is er naast de rol *Uitgever* ook de rol *Zorggebruiker.* Hoewel *Uitgever* namens *Zorggebruiker* handelt, kan *Zorggebruiker* niet ongenoemd blijven (verborgen achter de rol *Uitgever*) in de afspraken op deze en onderliggende lagen. Dat komt doordat *Zorggebruiker* niet enkel de gebruiker van *Uitgever*, maar allereerst het onderwerp van de gezondheidsinformatie die *Bron* ter beschikking moet stellen en *Lezer* ter beschikking gesteld wordt; daarvoor is authenticatie nodig. In het zorgaanbiedersdomein ligt dat anders. In deze release van het afsprakenstelsel

volstaat het om de *Bron en Lezer* te zien als de rollen die samen volledig verantwoordelijk zijn voor wat een zorgaanbieder operationeel zou moeten doen. Alle complexiteit voor de implementatie van die verantwoordelijkheid ligt bij de *Bron*, respectievelijk *Lezer*. Dat werkt door in de Applicatielaag en de Netwerklaag.

Omdat ook de *Stichting MedMij* operationele verantwoordelijkheden heeft, staat hier de functionele rol van *MedMij Beheer*.

Verantwoordelijkheden

Toelichting

De verantwoordelijkheden op deze laag en die op de Applicatielaag hebben een vergelijkbare opbouw. Ze zijn geordend in hoofdstukken en secties als volgt:

- Dossier
  - Use cases
  - Gegevensdiensten
  - Authenticatie
  - Autorisatie
- Lijsten
  - Zorgaanbiederslijst
  - OAuth Client List
  - Gegevensdienstnamenlijst
  - Whitelist
- Logging

Op meerdere plaatsen komen daarbij use cases (op deze laag) en use case-implementatie (op de applicatielaag) aan de orde. Een use case-implementatie is de implementatie van de use case met dezelfde naam. In deze release van het afsprakenstelsel zijn er zes use cases, waarvan vijf zich afspelen tussen het Persoons- en het Zorgaanbiedersdomein. Van deze vijf maken, om de interoperabiliteit in het MedMij-netwerk te borgen, stroomdiagrammen deel uit van het afsprakenstelsel. De zesde speelt zich helemaal binnen het Persoonsdomein af. Hiervan eist het MedMij Afsprakenstelsel wel dat erin moet worden voorzien, maar niet hoe; dat wordt aan de vrijheid van de MedMij-deelnemers gelaten.

Het gaat om de volgende use cases:

Use case	Stroomdiagram
UC Verzamelen	met
UC Delen	met
Raadplegen dossier	zonder
UC Opvragen ZAL	met
UC Opvragen OCL	met
UC Opvragen GNL	met

Voor registratie van MedMij-deelnemers en van hun vanwege hun deelname belangrijke gegevens zijn vooralsnog geen separate use cases geïdentificeerd, omdat registratie een secundair en vooralsnog niet geautomatiseerd proces is.

De interpretatie door een *Zorggebruiker* van zorg- en gezondheidsinformatie die hij heeft verzameld bij een *Zorgaanbieder*, en de interpretatie door een *Zorgaanbieder* van zulke informatie die met hem /haar gedeeld is door een *Zorggebruiker,* hangt niet alleen af van de inhoud van die informatie, maar ook van de partij die de betreffende informatie oorspronkelijk heeft geregistreerd. We gebruiken hiervoor niet zomaar de term *Bron*, omdat deze term in de zin van het MedMij afsprakenstelsel niet per se de oorspronkelijke herkomst (de auteur) betekent, maar alleen de onmiddellijke herkomst, gezien vanuit de *Uitgever*. In het MedMij afsprakenstelsel is de auteursrol geen juridische rol. Dat betekent niet alleen dat er binnen de grenzen van het MedMij afsprakenstelsel 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*.

Dossier

Use cases

1a. *Uitgever* biedt *Zorggebruiker* de use case *UC Verzamelen* om bij *Bron* gezondheidsinformatie te verzamelen die op deze *Zorggebruiker* betrekking heeft en laat deze in een persoonlijk gezondheidsdossier (kortweg *Dossier*) van *Zorggebruiker* bewaren. Bij deze use case betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.

Toelichting

Deze regel introduceert ook de notie van een persoonlijk gezondheidsdossier. Voor het voldoen aan deze regel is het dus niet voldoende aan de *Zorggebruiker* 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.

1b. *Uitgever* biedt *Zorggebruiker* de use case *UC Dele*n om bij *Lezer* ten behoeve van een *Zorgaanbieder*, indien deze daartoe ontvankelijk is, gezondheidsinformatie te plaatsen die op deze *Zorggebruiker* betrekking heeft en die afkomstig is uit het *Dossier*. Bij deze use case betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.

Toelichting

De nummering van de verantwoordelijkheden is zo gekozen om in dezen achterwaartse compatibiliteit te behouden met release 1.0. Voor een beschrijving van overeenkomsten en verschillen tussen UC Verzamelen en UC Delen, zie de pagina over UC Delen.

1c. *Uitgever* draagt ervoor zorg dat in het *Dossier* bij alle bij *Bron* in het kader van een *Gegevensdienst* verzamelde informatie onlosmakelijk deze *Bron* en *Gegevensdienst* als bron en verzamelcontext worden aangetekend. *Uitgever* draagt ervoor zorg dat, in geval van het delen van informatie met een (andere) *Zorgaanbieder* deze bron- en context-informatie wordt meegeleverd aan de *Lezer*. Voor de benoeming van

de *Bron* wordt daarbij gebruik gemaakt van de *Zorgaanbiedersnaam*. Voor de benoeming van de context wordt daarbij gebruik gemaakt van de betreffende *Gegevensdienstnaam* uit de *Gegevensdienstnamenlijst*.

> **Toelichting**
>
> Hiermee wordt geborgd dat bij de uitgewisselde zorg- en gezondheidsinformatie altijd duidelijk is bij welke Bron en in welke context (*Gegevensdienst*) deze is verzameld. Een *Lezer* van deze informatie kan deze meta-informatie gebruiken voor een betere interpretatie van de betreffende informatie. Mochten hieruit alsnog interpretatievragen komen, kan de Lezer zich vervoegen bij betreffende *Bron*.

2. *Uitgever* biedt *Zorggebruiker* de use case *Bevragen dossier* om het persoonlijk gezondheidsdossier te raadplegen.

> **Toelichting**
>
> Zie onder 1. Omdat deze functie zich niet over meerdere functionele rollen uitstrekt, is zij niet nader gespecificeerd in een stroomdiagram. Het is aan de vrijheid van de deelnemer in het afsprakenstelsel om deze naar behoefte van haar klanten in te richten. Maar zij mag niet ontbreken, omdat dan de Zorggebruiker geen regie over het dossier kan voeren.

3. In het kader van de use case *Bevragen dossier* zal *Zorggebruiker* te allen tijde moeten kunnen nagaan:

- welke inhoud van het *Dossier* wel, en welke niet, via MedMij-verkeer van *Bron* is betrokken van welke *Zorgaanbieder,* en sindsdien niet is veranderd;
- welke inhoud van het *Dossier* wel, en welke niet, via MedMij-verkeer bij *Lezer* is geplaatst ten behoeve van welke *Zorgaanbieder*.

> **Toelichting**
>
> Hiermee is het voor de *Zorggebruiker* 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.

Gegevensdiensten

4. *Uitgever* laat *Zorggebruiker* met een *Gegevensdienst* uit de *Gegevensdienstnamenlijst* gezondheidsinformatie verzamelen door een *Bron* of, ten behoeve van een *Zorgaanbieder*, plaatsen bij een *Lezer*.

> **Toelichting**
>
> Een *Gegevensdienst* is een op een specifieke en gestandaardiseerde set gezondheidsinformatie gerichte dienst waarmee *Bron* zulke informatie ontsluit naar *Uitgever* in het kader van de *UC Verzamelen* of *Lezer* zulke informatie geplaatst krijgt ten behoeve van een *Zorgaanbieder*. In de *Gegevensdienstnamenlijst* zijn de *Gegevensdiensten* opgenomen die in deze release kunnen worden geboden.

5. Elke *Bron* biedt op elk moment minstens één *Gegevensdienst*. Elke *Lezer* biedt op elk moment minstens één *Gegevensdienst*.

Toelichting

Het bieden van een *Gegevensdienst* is, in deze versie van het MedMij Afsprakenstelsel, hetzij het door een *Bron* bij zich laten verzamelen of het door een *Lezer* met zich laten delen van zekere gezondheidsinformatie.

6. *MedMij Beheer* zal alleen in de *Zorgaanbiederslijst* opnemen dat een zekere *Gegevensdienst* voor een zekere *Zorgaanbieder* via een zekere *Bron*, respectievelijk *Lezer,* wordt aangeboden, indien zij (*Stichting MedMij*) heeft vastgesteld dat de *Dienstverlener zorgaanbieder* die daarbij de *Bron*, respectievelijk *Lezer*, is, voldoet aan de specifiek op die *Gegevensdienst* toepas-selij-ke eisen.

Toelichting

Omdat er een indirectie speelt, via de *Dienstverlener zorgaanbieder* naar de *Zorgaanbieder*, moet gezegd worden dat één *Zorgaanbieder* genoeg is (die een bepaalde *Informatiestandaard* ontsluit) om ervoor te zorgen dat de *Dienstverlener zorgaanbieder* zich voor die *Informatiestandaard* moet kwalificeren in het afsprakenstelsel.

7a. Voor elke *Gegevensdienst* waarvan de *Zorgaanbiederslijst* aan-geeft dat een zekere*Zorgaanbieder* deze aanbiedt, zal *Bron*, respectievelijk *Lezer*, ervoor zorgdragen dat daaraan opvol-ging gegeven wordt, zonder daarbij welke *Uitgever* dan ook bij voorbaat uit te sluiten.

Toelichting

Net als regel 6, moet regel 7a rekening houden met de indirectie via *Dienstverlener zorgaanbieder* naar de *Zorgaanbieder* zelf. Deze regel legt het bij de *Dienstverlener zorgaanbieder* om ervoor zorg te dragen dat de *Zorgaanbieder* met wie hij een dienstverleningsovereenkomst heeft, ook de gegevensdienst levert die hij toegezegd heeft. Zo ontzorgt de *Dienstverlener zorgaanbieder* zijn tegenspelers in het afsprakenstelsel.

7b. Het is verantwoordelijkheid 7a bepaalde is ook van toepassing zolang de geldigheid van de toepasselijke vermelding in de *Zorgaanbiederslijst* niet langer dan één uur (3600 seconden) geleden is verstreken.

Toelichting

Zo wordt ervoor ruimte geboden dat naijlende sessies, die nog gebruik maken van de verstrijkende versie van de *Zorgaanbiederslijst*, nog kunnen worden afgemaakt.

Autorisatie

8a. *Bron* vergewist zich ervan, elke keer opnieuw voordat hij *Zorggebruiker* gezondheidsinformatie van *Zorgaanbieder* laat verzamelen, dat deze *Zorggebruiker* uitdrukkelijk *Toestemming* heeft gegeven aan *Zorgaanbieder* om de in de *Gegevensdienst* betrokken gezondheidsinformatie aan *Uitgever* ter beschikking te laten stellen. De vraag om *Toestemming* heeft een vaste formulering, die is opgenomen in de UC Verzamelen. Deze *Toestemming* geldt niet buiten deze doorloping van de *UC Verzamelen*.

Toelichting

Het is dus de *Bron* die de *Toestemming* ophaalt bij de *Zorggebruiker*. De tweede zin van deze regel maakt de toestemming functioneel zo eenvoudig mogelijk, omdat in de huidige release van het MedMij Afsprakenstelsel alleen met een eenmalige vraag gezondheidsinformatie verzameld kan worden. De toestemming, hoe expliciet ook, heeft precies dezelfde reikwijdte als die eenmalige vraag.

8b. *Lezer* vergewist zich ervan, elke keer opnieuw voordat hij *Zorggebruiker* gezondheidsinformatie ten behoeve van Zorgaanbieder laat plaatsen, dat deze *Zorggebruiker* uitdrukkelijk heeft bevestigd om de in de *Gegevensdienst* betrokken gezondheidsinformatie aan *Zorgaanbieder* ter beschikking te willen stellen. De vraag om *Bevestiging* heeft een vaste formulering, die is opgenomen in de UC Delen. Deze bevestiging geldt niet buiten deze doorloping van de *UC Delen*.

Toelichting

Deze verantwoordelijkheid is welbewust niet geïntegreerd met verantwoordelijkheid 8a omdat de hier bedoelde bevestiging niet de juridische status heeft van de in verantwoordelijkheid 8a bedoelde toestemming. Er is daarvoor om diezelfde reden ook geen voorgeschreven formulering.

Authenticatie

9. *Bron* en *Lezer* dragen ervoor zorg dat de onder 7 bedoelde opvolging, en de onder 8a en 8b bedoelde vraag om *Toestemming*, respectievelijk bevestiging, slechts plaatsvindt wanneer hij de identiteit van de *Zorggebruiker* met passende zekerheid heeft vastgesteld.

Toelichting

Op de applicatielaag wordt beschreven dat de identiteit van de Zorggebruiker wordt met een BSN en die passende zekerheid wordt verkregen door middel van *DigiD*.

Lijsten

Zorgaanbiederslijst

10. *MedMij Beheer* beheert en publiceert een *Zorgaanbiederslijst*, namens de deelnemende *Dienstverleners Zorgaanbieder*. De *Zorgaan-bie-derslijst* beschrijft van elke *Zorgaanbieder* welke *Gegevensdiensten* deze momenteel biedt via welke *Bron* en *Lezer,* en welke technische adressen daarvoor moeten worden aangesproken bij die *Bron* of *Lezer.* De gepubliceerde *Zorgaanbiederslijst* bevat steeds en slechts alle actuele entries.

Toelichting

Deze afspraak wijst *MedMij Beheer* de verantwoordelijkheid toe om ten behoeve van alle *Dienstverleners Persoon* een lijst te verspreiden van *Zorgaanbieders* en de door hen aangeboden *Gegevensdiensten*. Zonder deze functie zou het stelsel niet functioneren.

11. De inhoud van de *Zorgaanbiederslijst* voldoet aan het logische metamodel.

12. *MedMij Beheer* beheert en publiceert, in de *Zorgaanbiederslijst*, unieke en gebruikersvriendelijke namen van *Zorgaanbieders*, van het formaat `<zorgaanbieder>@medmij.` Daarop is naamgevingsbeleid van toepassing.

> **Toelichting**
>
> *Zorgaanbieders* kunnen in hun directe of indirecte contact met *Zorggebruikers* deze naam meegeven als hun "MedMij-naam". *MedMij Beheer* zorgt voor uniciteit en heeft het laatste woord bij het vaststellen ervan.

13. *MedMij Beheer* biedt aan *Uitgever* een use case (*UC Opvragen ZAL*) om de actuele versie van die *Zorgaanbiederslijst* op te vragen: *Opvragen Zorgaanbiederslijst*. Betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.

OAuth Client List

14. *MedMij Beheer* beheert en publiceert een actuele *OAuth Client List*, namens de deelnemende *Dienstverleners persoon*. Deze beschrijft wat de gebruikersvriendelijke namen zijn die voor de *Dienstverleners persoon* worden gebruikt in de toestemmingsverklaring*. De inhoud van de OAuth Client List voldoet aan het logische metamodel.*

> **Toelichting**
>
> De *OAuth Client List* bevat dus geen namen voor *Dienstverleners zorgaanbieder*. Dat is niet nodig, omdat deze niet voorkomen in de toestemmingsverklaring.

15. *MedMij Beheer* biedt aan *Bron* een use case (*UC Opvragen OCL*) om de actuele versie van die *OAuth Client List* op te vragen. Betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.

Gegevensdienstnamenlijst

16. *MedMij Beheer* beheert en publiceert de *Gegevensdienstnamenlijst*. Deze beschrijft welke gebruikersvriendelijke namen horen bij welke *GegevensdienstIds.* De inhoud van de *Gegevensdienstnamenlijst* voldoet aan het logische metamodel.

17. *MedMij Beheer* biedt aan *Uitgever, Bron* en *Lezer* een use case (*UC Opvragen GNL*) om de actuele versie van die *Gegevensdienstnamenlijst* op te vragen. Betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.

Whitelist

18. *MedMij Beheer* beheert en publiceert een actuele *Whitelist*, namens de deelnemende *Dienstverleners zorgaanbieder*en *Dienstverleners persoon*. De *Whitelist* beschrijft welke *Nodes* in MedMij-verkeer mogen deelnemen*.* De inhoud van de *Whitelist* voldoet aan het logische metamodel.

> **Toelichting**
>
> Er bestaat op deze laag geen use case voor het opvragen van de *Whitelist*. De *Whitelist* wordt alleen gebruikt op de Netwerk-laag. Op die laag is er wel een use case-implementatie voor dit doel.

Logging

19. *Uitgever* 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 *Zorggebruiker* bij enige *Bron* verzamelde persoonsgege-vens en door enige Zorggebruiker bij enige *Lezer* geplaatste persoonsgegevens.

Toelichting

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. De revisie, met het nummer NEN 7513:2018, is onderdeel van het Normenkader 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.

20. De bewaartermijn van de logbestanden is ten minste 12 maanden en niet meer dan 15 maanden. Na de bewaartermijn van de logbestanden moeten deze vernietigd worden.

Toelichting

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.

21. *MedMij Beheer* onderhoudt een archief van alle ooit ontsloten versies van de *Zorgaanbiederslijst*, 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 20.

UC Verzamelen

Toelichting

In de platen hieronder staat het stroomdiagram van de use case *Verzamelen*, in vier perspectieven:

- het totaalperspectief;
- het perspectief van de *Uitgever*, die onder de hoede van de *Dienstverlener Persoon* valt. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus deze plaat lezen als zijn verplichte aandeel in de use case *Verzamelen;*
- het perspectief van de *Bron*, die onder de hoede van de *Dienstverlener Zorgaanbieder* valt. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus deze plaat lezen als zijn verplichte aandeel in de use case *Verzamelen;*
- het perspectief van de *Zorggebruiker.*

De stroomdiagrammen tonen allereerst de situatie waarin alle acties slagen tot en met het uiteindelijke verzamelen van de gezondheidsinformatie (de zogenaamde happy flow). De twee oranje banen horen, conform de MedMij-huisstijl, tot het Persoonsdomein, de blauwe tot het Zorgaanbiedersdomein. Menige actie in de stroomdiagrammen is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow; de zachtgeel gekleurde acties vormen samen de authenticatieflow. In de stroomdiagrammen voor de specifieke perspectieven hebben alleen de acties in de bij dat perspectief horende baan namen. De acties in de andere banen zijn gecomprimeerd en anoniem weergegeven.

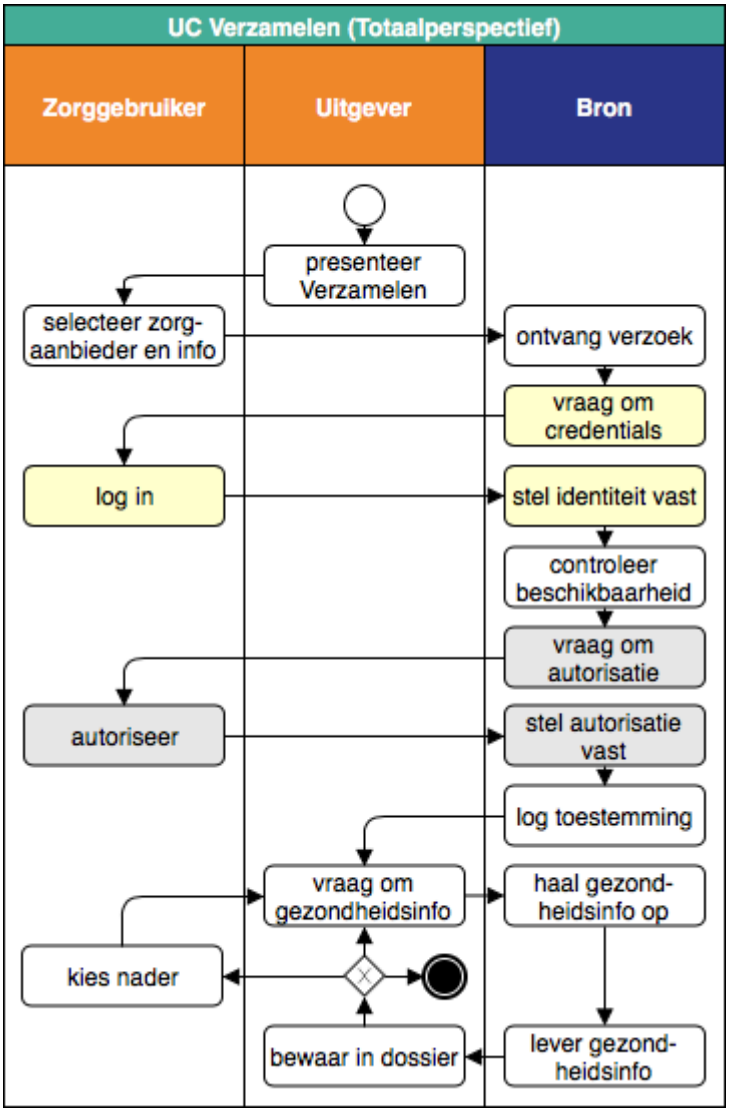
Tot slot bespreken we de uitzonderingen op de happy flow. Daarbij werken we alleen vanuit het totaalperspectief.

Totaalperspectief (happy flow)

Toelichting

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

- De *Uitgever* presenteert aan de *Zorggebruiker* de mogelijkheid om te verzamelen.
- De *Zorggebruiker* kiest expliciet de zorgaanbieder waarbij hij de informatie wenst te verzamelen en de specifieke soort te verzamelen informatie. Daarvoor kunnen desgewenst de *Gegevensdienstnamen* worden gebruikt uit de *Gegevensdienstnamenlijst*. Het verzoek gaat naar de passende *Bron*.
- De *Bron* laat de *Zorggebruiker* zich authenticeren.
- Als dat slaagt, controleert de *Bron* alvast of de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft.
- Zo ja, dan vraagt de *Bron* aan de *Zorggebruiker* of hij toestemming geeft tot het verstrekken van de gevraagde informatie aan de *Uitgever*.
- De *Bron* logt die toestemming en laat de *Uitgever* weten of de autorisatie geslaagd is.
- Zo ja, dan kan de *Uitgever* de *Bron* vragen om de gezondheidsinformatie.
- Bij ontvangst slaat de *Uitgever* die informatie op in het persoonlijke dossier.
- Mocht de *Gegevensdienst* waartoe de *Zorggebruiker* heeft geautoriseerd uit meerdere *Transacties* bestaan, bevraagt de *Uitgever* de *Bron* daarna mogelijk opnieuw voor de nog resterende *Transacties*, eventueel na nieuwe gebruikersinteractie.
- Bij de informatie wordt ook de meta-informatie opgeslagen die wordt bedoeld in verantwoordelijkheid 20 van de Processen- en Informatielaag.

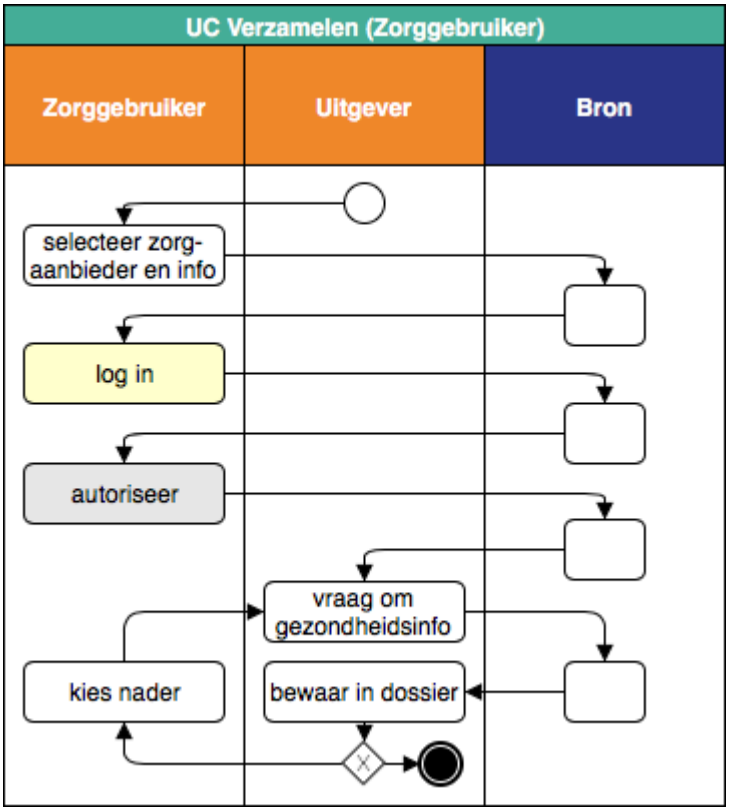


De vraag die aan de *Zorggebruiker* gesteld moet worden in de stap "autoriseer" staat op de pagina Toestemmingsverklaring. Op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen is omschreven hoe de variabelen in deze verklaring gevuld worden.

Perspectief van de Zorggebruiker (happy flow)

Toelichting

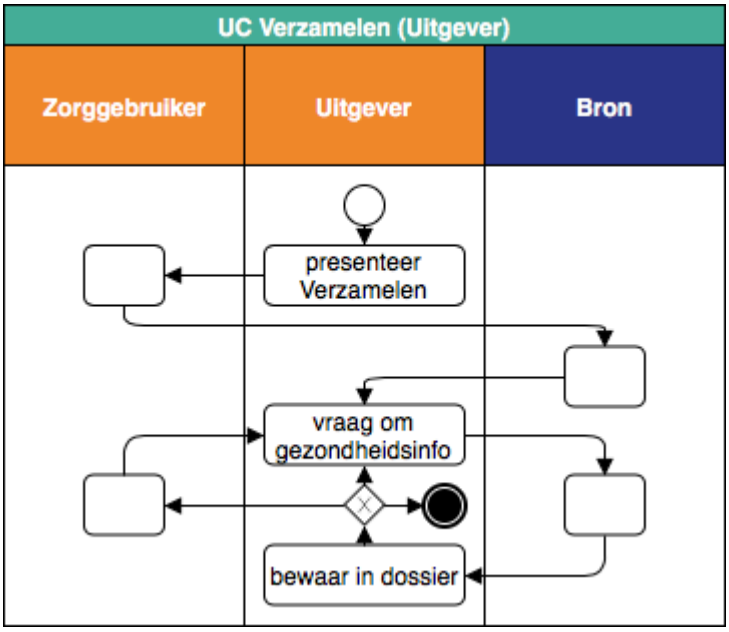
De *Zorggebruiker* moet drie stappen doorlopen: selectie van zorgaanbieder en soort informatie, inloggen en autoriseren. Als alles slaagt, slaat de Uitgever voor hem zowel de toestemming als de verkregen gezondheidsinformatie op.



Perspectief van de Uitgever (happy flow)

Toelichting

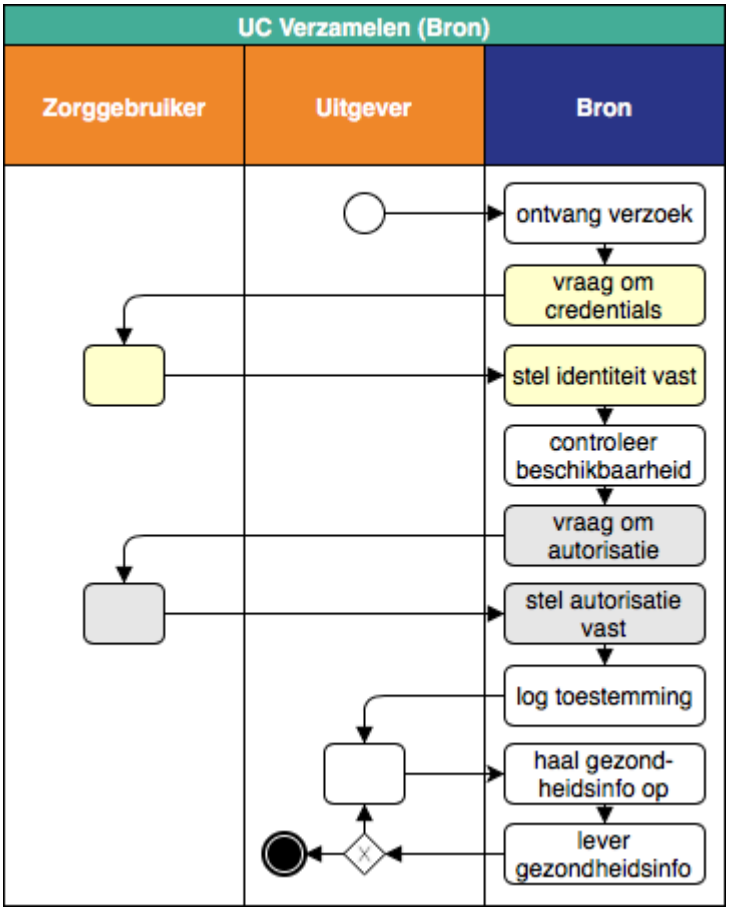
De *Uitgever* start de use case door aan de *Zorggebruiker* de mogelijkheid tot verzamelen te presenteren. Van de *Bron* krijgt hij na enige tijd het bericht dat de toestemming daarvoor is verleend, waarna hij die toestemming logt en de gezondheidsinformatie ophaalt bij de *Bron*, en opslaat.



Perspectief van de Bron (happy flow)

Toelichting

De *Bron* regisseert, na ontvangst van het verzoek tot Verzamelen, de authenticatie en de autorisatie. Als die geslaagd zijn logt hij de toestemming en stuurt deze naar de Uitgever. Die zal uiteindelijk de bevraging terugsturen en het antwoord in ontvangst nemen.



Uitzonderingen (Totaalperspectief)

Toelichting

In onderstaande tabel staan de uitzonderingssituaties beschreven. Alle worden door de *Bron* ontdekt. In deze release 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. Om te voorkomen dat de *Uitgever* 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 *Uitgever*.

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

In deze versie van het MedMij afsprakenstelsel controleert de beschikbaarheidstoets minimaal twee voorwaarden: het bestaan van een behandelrelatie die als grondslag kan dienen voor het verzamelen en de controle of de Zorggebruiker wel minstens zestien jaar oud is. Er kunnen echter ook andere redenen voor niet-beschikbaarheid zijn, zoals technische. 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 beschikbaarheidstoets worden opgevat. Wanneer een toekomstige release van het MedMij afsprakenstelsel wel zulke toestemmingen of machtigingen omvat, zal de leeftijdstoets gescheiden moeten worden van de beschikbaarheidstoets.

nr.	uitzondering	actie	vervolg
UC Verzamelen 1	*Bron* vindt het ontvangen verzoek ongeldig.	*Bron* informeert *Uitgever* over deze uitzondering. *Uitgever* informeert daarop *Zorggebruiker* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Verzamelen 2	*Bron* kan de identiteit van de *Zorggebruiker* niet vaststellen.	*Bron* informeert *Uitgever* dat verzamelen niet toegelaten wordt.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Verzamelen 3	*Bron* stelt vast dat van *Persoon* bij *Zorgaanbieder* geen gezondheidsinformatie voor die *Gegevensdienst* beschikbaar is. Hiervan is in elk geval sprake indien hetzij: • er geen behandelrelatie is als grondslag voor het verzamelen; • *Zorggebruiker* nog geen zestien jaar oud is.		
UC Verzamelen 4	De autorisatievraag wordt ontkennend beantwoord.		
UC Verzamelen 5	*Bron* kan het antwoord op de autorisatievraag niet vaststellen.	*Bron* informeert *Uitgever* over deze uitzondering. *Uitgever* informeert daarop *Zorggebruiker* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Verzamelen 6	*Bron* kan, zelfs na autorisatie, de gezondheidsinformatie alsnog niet ter beschikking stellen aan de *Uitgever*.	*Bron* informeert *Uitgever* over deze uitzondering. *Uitgever* informeert daarop *Zorggebruiker* hierover, met opgave van oorzaak.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

UC Delen

Toelichting

Op deze pagina staan de stroomdiagrammen van de *UC Delen*. De use case is een spiegelbeeld van *UC Verzamelen*. Die spiegeling betekent echter niet dat de rollen van *Uitgever* en *Bron* nu omgekeerd worden belegd, dat wil zeggen bij respectievelijk *Dienstverlener Zorgaanbieder* en *Dienstverlener Persoon*. Een dergelijke omdraaiing zou een zwakkere, meer proces-logistiek-georiënteerde regievorm verraden, en met de rolomdraaiing ook het initiatief bij de *Dienstverlener Persoon*, en dus bij de *Zorggebruiker*, wegnemen. Het MedMij Afsprakenstelsel ondersteunt een sterkere regievorm, waarbij ook in de *UC Delen* het initiatief bij de *Uitgever* ligt. In plaats van met een *Bron* vanwaar de *Uitgever* gezondheidsinformatie betrekt, heeft hij nu echter te maken met een *Lezer* waaraan hij zulke informatie ter beschikking stelt. Net zoals de *Bron*-rol in *UC Verzamelen*, is de *Lezer*-rol in deze versie van het MedMij Afsprakenstelsel enkel nog verbonden aan de juridische rol van *Dienstverlener Zorgaanbieder*.

Een tweede voordeel van deze keuze is dat de *UC Delen* in hoge mate dezelfde opzet kent als de *UC Verzamelen*. Dat geldt dientengevolge ook voor de respectievelijke use case-implementaties, die dus veel van elkaar kunnen hergebruiken. Dat laat onverlet dat er een aantal wezenlijke verschillen zijn. Op het niveau van Processen en Informatie zijn dat de volgende.

- Voor de start van de use case zou de *Zorggebruiker* moeten kunnen volstaan met het aanwijzen van die informatie in zijn *Dossier* die hij zou willen delen met een nader te benoemen *Zorgaanbieder*, en er daarbij vanuit mogen gaan dat de *Uitgever* daarbij weet welke *Gegevensdienst* daarbij aan de orde is.
- In tegenstelling tot in *UC Verzamelen* moet *Zorgaanbieder* in de gelegenheid worden gesteld om zich al dan niet open te stellen voor ontvangst van de betreffende informatie. De *Lezer* moet na authenticatie van de *Zorggebruiker* moet kunnen bepalen of de betreffende informatie welkom is bij de betreffende *Zorgaanbieder*. 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 *Zorggebruiker* vereist aan de *Zorgaanbieder* voor het mogen ontvangen van de gezondheidsinformatie; die volgt uit de verstrekking door de Zorggebruiker. Er zijn wel toestemmingsvereisten in de relatie *Zorggebruiker-Uitgever* (inzake het mogen verstrekken van de gezondheidsinformatie), maar daarop ziet reguliere wet- en regelgeving toe. Niettemin wordt er, net als in *UC Verzamelen*, om een bevestiging gevraagd van de *Zorggebruiker*. Wanneer de *Zorggebruiker* deze vraag wordt gepresenteerd, kan hij daaruit de conclusie trekken dat de de betreffende *Zorgaanbieder* ontvankelijk is voor betreffende informatie. Mocht hij dat niet zijn, dan verschijnt een andere melding. Zo blijft de *Zorggebruiker* niet, te lang, in het ongewisse over de voortgang van de use case.
- Aan het eind van de use case wordt, indien de *Zorgaanbieder* ervoor ontvankelijk bleek, de betreffende informatie door de *Uitgever* geplaatst bij de *Zorgaanbieder,* via de *Lezer*. Net zoals in de *UC Verzamelen* geen nadere eisen worden gesteld aan hoe het ophalen van de informatie door de *Bron* bij de *Zorgaanbieder* geschiedt, geldt dat in de *UC Delen* ook voor de plaatsing. Van belang is slechts dat de *Zorggebruiker* ervan kan uitgaan dat de *Zorgaanbieder* kennis kan hebben genomen van de betreffende informatie. Hoe dat wordt geborgd is niet triviaal, maar wordt gelaten aan de voorzieningen die de *Dienstverlener Zorgaanbieder* treft en de *Dienstverleningsovereenkomst* die hij dienaangaande aangaat met de *Zorgaanbieder*.

In de platen hieronder staat het stroomdiagram van de use case *Delen*, in vier perspectieven:

- het totaalperspectief;
- het perspectief van de *Zorggebruiker;*

- het perspectief van de *Uitgever*, die onder de hoede van de *Dienstverlener Persoon* valt. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus deze plaat lezen als zijn verplichte aandeel in de use case *Delen;*
- het perspectief van de *Lezer*, die onder de hoede van de *Dienstverlener Zorgaanbieder* valt. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus deze plaat lezen als zijn verplichte aandeel in de use case *Delen.*

De stroomdiagrammen tonen allereerst de situatie waarin alle acties slagen tot en met het uiteindelijke delen van de gezondheidsinformatie (de zogenaamde happy flow). De twee oranje banen horen, conform de MedMij-huisstijl, tot het Persoonsdomein, de blauwe tot het Zorgaanbiedersdomein. Menige actie in de stroomdiagrammen is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow; de zachtgeel gekleurde acties vormen samen de authenticatieflow. In de stroomdiagrammen voor de specifieke perspectieven hebben alleen de acties in de bij dat perspectief horende baan namen. De acties in de andere banen zijn gecomprimeerd en anoniem weergegeven.

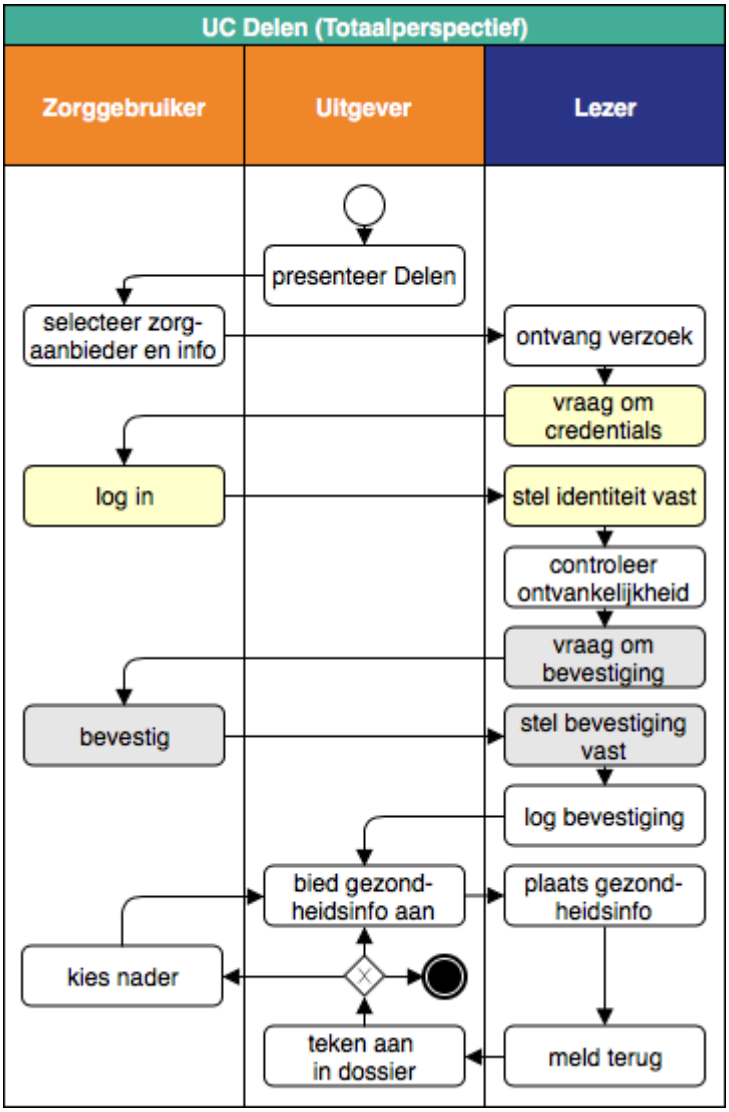
Tot slot bespreken we de uitzonderingen op de happy flow. Daarbij werken we alleen vanuit het totaalperspectief.

Totaalperspectief (happy flow)

Toelichting

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

- De *Uitgever* presenteert aan de *Zorggebruiker* de mogelijkheid om te delen.
- De *Zorggebruiker* kiest expliciet de zorgaanbieder waarbij hij de informatie wenst te verzamelen en de te delen informatie. Daarvoor kunnen desgewenst de *Gegevensdienstnamen* worden gebruikt uit de *Gegevensdienstnamenlijst*. Het verzoek gaat naar de passende *Lezer*.
- De *Lezer* laat de *Zorggebruiker* zich authenticeren.
- Als dat slaagt, controleert de *Lezer* alvast of de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* wenst te ontvangen. Daarvoor is het in elk geval nodig dat de *Zorgaanbieder* een behandelrelatie heeft met de *Persoon*.
- Zo ja, dan vraagt de *Lezer* aan de *Zorggebruiker* of hij de wens bevestigt de informatie te laten verstrekken aan de *Zorgaanbieder*.
- De *Lezer* logt die bevestiging en laat de *Uitgever* weten of de die geslaagd is.
- Zo ja, dan kan de *Uitgever* de gezondheidsinformatie plaatsen bij de *Lezer*.
- Mocht de *Gegevensdienst* waartoe de *Zorggebruiker* heeft geautoriseerd uit meerdere *Transacties* bestaan, plaatst de *Uitgever* daarna mogelijk opnieuw bij de *Lezer* voor de nog resterende *Transacties*, eventueel na nieuwe gebruikersinteractie.
- De Uitgever tekent bij de informatie ook de meta-informatie aan die wordt bedoeld in verantwoordelijkheid 20 van de Processen- en Informatielaag.

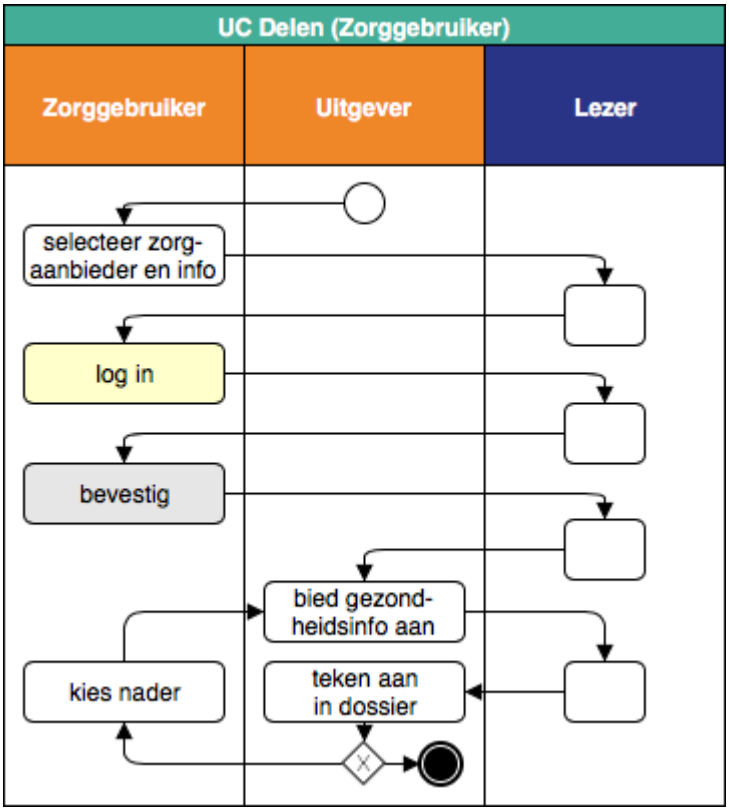


De vraag die aan de *Zorggebruiker* gesteld moet worden in de stap "bevestig" staat op de pagina Bevestigingsverklaring. Op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen is omschreven hoe de variabelen in deze verklaring gevuld worden.

Perspectief van de *Zorggebruiker* (happy flow)

Toelichting

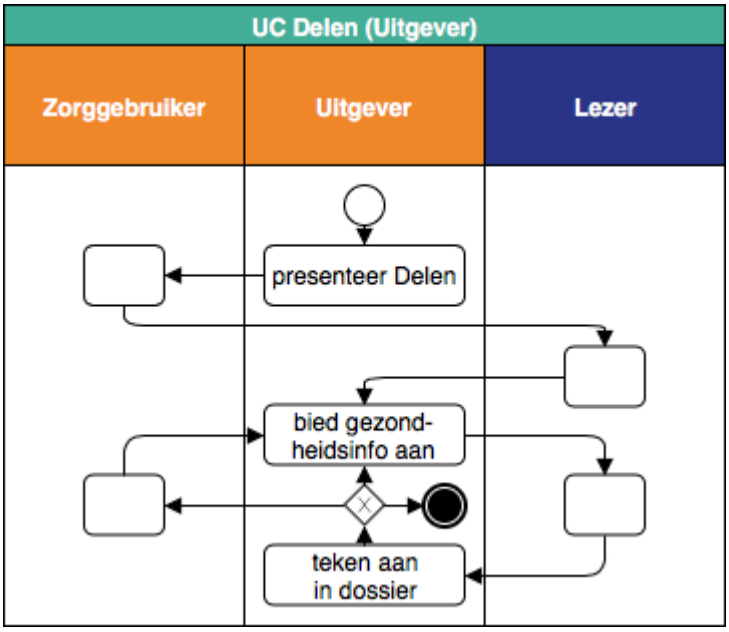
De *Zorggebruiker* moet om te beginnen drie stappen doorlopen: selectie van zorgaanbieder en informatie, inloggen en bevestigen. Eventueel kiest hij daarna voor nadere informatie om te laten plaatsen.



Perspectief van de *Uitgever* (happy flow)

Toelichting

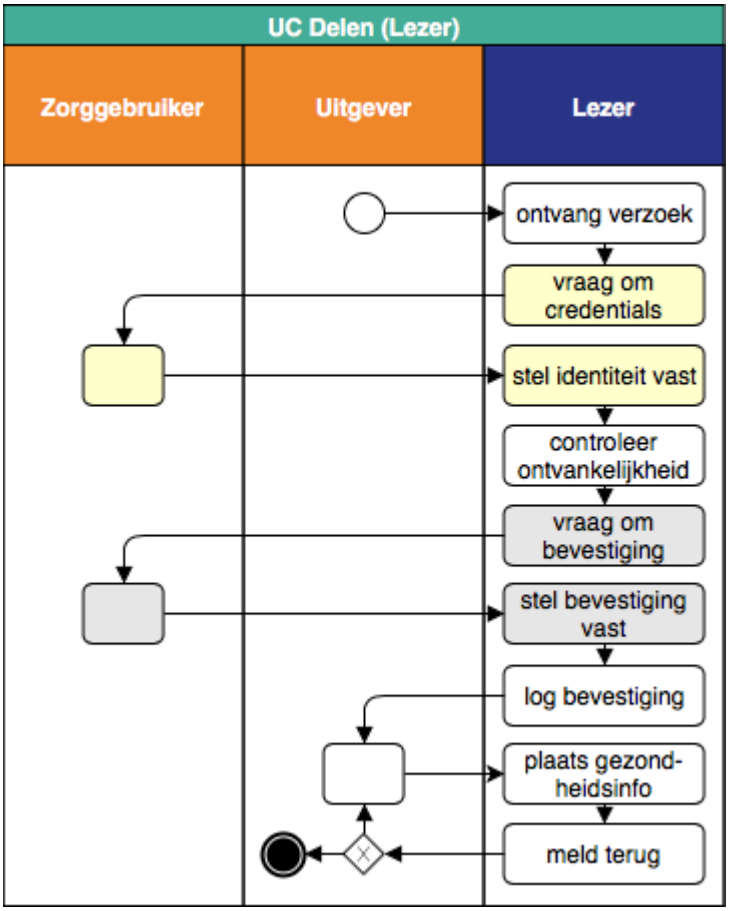
De *Uitgever* start de use case door aan de *Zorggebruiker* de mogelijkheid tot delen te presenteren. Van de *Lezer* krijgt hij na enige tijd het bericht dat de wens daartoe door Zorggebruiker is bevestigd, waarna hij de gezondheidsinformatie aanbiedt aan de *Lezer*. De reactie daarop tekent hij aan in het *Dossier*.



Perspectief van de *Lezer* (happy flow)

Toelichting

De *Lezer* regisseert, na ontvangst van het verzoek tot delen, de authenticatie en de bevestiging. Als die geslaagd zijn logt hij de bevestiging. Uiteindelijk krijgt hij van de *Uitgever* de gezondheidsinformatie aangeboden ter plaatsing bij de *Zorgaanbieder*. De *Lezer* meldt het resultaat daarvan terug.



Uitzonderingen (Totaalperspectief)

Toelichting

In onderstaande tabel staan de uitzonderingssituaties beschreven. Alle worden door de *Lezer* ontdekt. In deze release 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. Om te voorkomen dat de *Uitgever* 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 *Uitgever*.

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

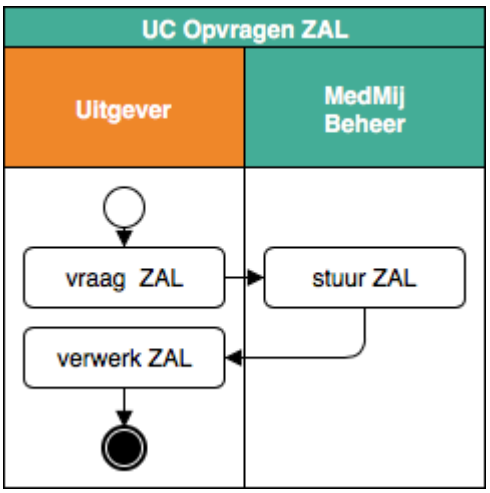
In deze versie van het MedMij afsprakenstelsel controleert de ontvankelijkheidstoets minimaal twee voorwaarden: het bestaan van een behandelrelatie die als grondslag kan dienen voor het delen en de controle of de Zorggebruiker minimaal zestien jaar oud is. Er kunnen echter ook andere redenen voor niet-ontvankelijkheid zijn, zoals technische. 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 beschikbaarheidstoets worden opgevat. Wanneer een toekomstige release van het MedMij

afsprakenstelsel wel zulke toestemmingen of machtigingen omvat, zal de leeftijdstoets gescheiden moeten worden van de ontvankelijkheidstoets.

nr.	uitzondering	actie	vervolg
UC Delen 1	*Lezer* vindt het ontvangen verzoek ongeldig.	*Lezer* informeert *Uitgever* over deze uitzondering. *Uitgever* informeert daarop *Zorggebruiker* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Delen 2	*Lezer* kan de identiteit van de *Zorggebruiker* niet vaststellen.	*Lezer* informeert *Uitgever* dat verzamelen niet toegelaten wordt.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Delen 3	*Lezer* stelt vast dat betreffende informatie van *Persoon* bij *Zorgaanbieder* niet welkom is. Hiervan is in elk geval sprake indien hetzij: • er geen behandelrelatie is als grondslag voor het verzamelen; • *Zorggebruiker* nog geen zestien jaar oud is.		
UC Delen 4	De bevestigingsvraag wordt ontkennend beantwoord.		
UC Delen 5	*Lezer* kan het antwoord op de bevestigingsvraag niet vaststellen.	*Lezer* informeert *Uitgever* over deze uitzondering. *Uitgever* informeert daarop *Zorggebruiker* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Delen 6	*Uitgever* kan, zelfs na bevestiging, de gezondheidsinformatie alsnog niet plaatsen bij *Lezer*.	*Uitgever* informeert daarop *Zorggebruiker* hierover, met opgave van oorzaak.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

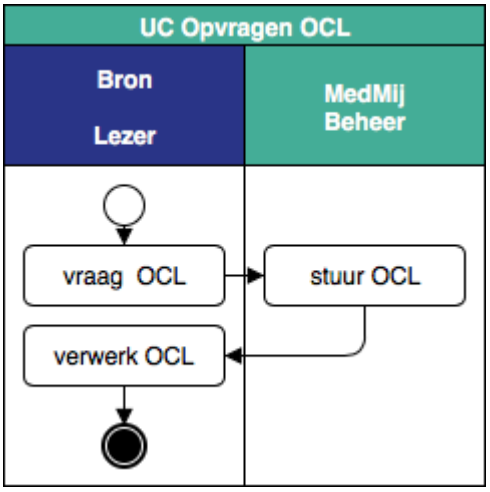
UC Opvragen ZAL

Stroomdiagram



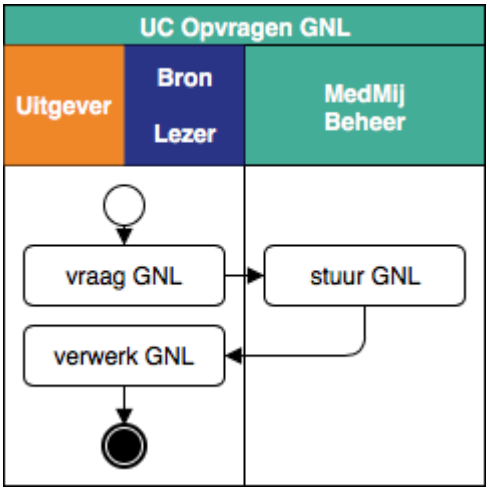
UC Opvragen OCL

Stroomdiagram

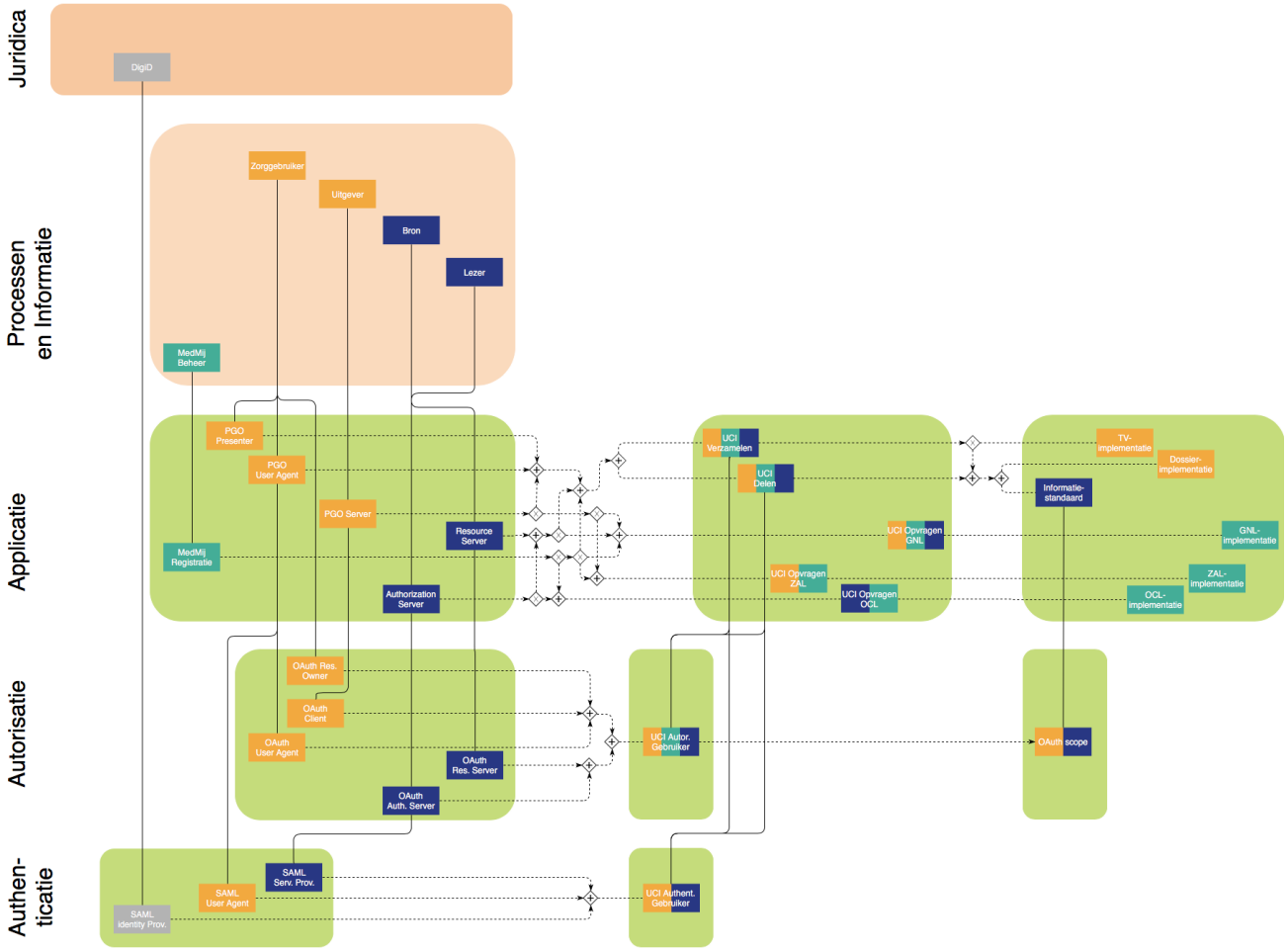


UC Opvragen GNL

Stroomdiagram



Applicatie



Toelichting

Voor een overzicht over alle lagen van de architectuur, en voor een toelichting van de betekenis van de symbolen en lijntjes, zie de overzichtspagina.

De afkorting:

- *TV* staat voor *Toestemmingsverklaring;*
- *ZAL* staat voor *Zorgaanbiederslijst;*
- *OCL* staat voor *OAuth Client List*;
- *GNL* staat voor *Gegevensdienstnamenlijst*.

Rollen

1. *Uitgever* biedt aan *Zorggebruiker,* in het kader van de toepasselijke *Dienstverleningsovereenkomst*, een geautomatiseerd systeem ter gebruik, hier genoemd: *PGO Server*.

2. *Zorggebruiker* gebruikt twee geautomatiseerd rollen voor toegang tot *PGO Server*: *PGO Presenter* voor de gebruikerstoegang en *PGO User Agent* voor de toegang door *PGO Server*.
3. *Bron* biedt, en *Lezer* biedt, een geautomatiseerde dienst, voor het namens zorgaanbieders uitwisselen van gezondheidsinformatie met *PGO Server*, bestaande uit: *Authorization Server* en *Resource Server*.
4. *MedMij Beheer* ontsluit ten behoeve van alle betrokkenen een geautomatiseerde dienst, hier genoemd: *MedMij Registratie*.
5. Ten behoeve van het authenticeren van *Zorggebruiker*, zal de betrokken *Authorization Server* (in deze release van het MedMij Afsprakenstelsel) gebruikmaken van *DigiD* als *SAML Identity provider*, volgens het SAML 2.0 koppelvlak van DigiD, waarbij:
    1. de SAML-rol van *User Agent* wordt verzorgd door de *PGO User Agent*;
    2. de SAML-rol van *Service Provider* wordt verzorgd door de *Authorization Server*;
    3. de SAML-rol van *Identity Provider* dus wordt verzorgd door *DigiD*.
6. Ten behoeve van het autoriseren van *PGO Server* voor toegang tot *Resource Server*, in het kader van de functies *UC Verzamelen* en *UC Delen*, zullen de betrokken *PGO User Agent*, *PGO Server, Authorization Server* en *Resource Server* gebruik maken van OAuth 2.0, waarbij als grant type gebruik wordt gemaakt van Authorization Code en waarbij:
    1. de rol van *OAuth User Agent* wordt verzorgd door de *PGO User Agent*;
    2. de rol van *OAuth Client* wordt verzorgd door de *PGO Server*;
    3. de rol van *OAuth Resource Server* wordt verzorgd door de *Resource Server*;
    4. de rol van *OAuth Authorization Server* wordt verzorgd door de *Authorization Server.*
7. Als *MedMij-verkeer* is gedefinieerd: al het gegevensverkeer in het kader van enige use case-implementatie op deze laag of op de Netwerk-laag, onmiddellijk tussen twee verschillende van de vier volgende soorten rollen, namelijk:

    - ten eerste *PGO Server*,
    - ten tweede *PGO 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 *OAuth*-rollen,
    - van deze rollen telkens uitgesloten zijn de door hen eventueel verzorgde respectievelijke *SAML*-rollen, en
    - in deze rollen, met betrekking tot de use case-implementaties op de Netwerk-laag, telkens inbegrepen zijn de Netwerk-rollen waarop zij functioneren.
8. Al het *MedMij-verkeer*, voor zover daarin de *PGO User Agent*:

    - betrokken is, heet *frontchannel-verkeer*;
    - niet betrokken is, vormt het *backchannel-verkeer*.

Toelichting

Hier worden de functionele rollen vertaald naar rollen op applicatieniveau. In het persoonsdomein zijn drie rollen onderscheiden: de *PGO Presenter*, *PGO User Agent* en de *PGO Server*. Dat is nodig om de verbinding te kunnen leggen met authenticatierollen volgens OAuth. *PGO Presenter* en *PGO User Agent* zijn alle front-end-rollen voor de PGO Server, en kunnen bijvoorbeeld allebei in een browser zijn geïmplementeerd, maar voor een goede binding aan de *OAuth*- en *SAML*-rollen en voor een goede beveiligingsmaatregelen is het nodig deze twee rollen te scheiden. Zoals ook elders in het MedMij Afsprakenstelsel gaat het hier om rollen, om setjes verantwoordelijkheden dus, niet om implementatiecomponenten.

In het zorgaanbiedersdomein is zo'n scheiding niet nodig. Waar een *Persoon* zelf operationeel betrokken wordt in het informatieverkeer — namelijk om zich te laten identificeren en authenticeren,

en het verkeer te laten autoriseren — laat de *Zorgaanbieder* 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).

In lijn met keuzes op de Proces- en Informatielaag, treden deze servers op namens alle eventuele achterliggende systemen in het zorgaanbiedersdomein, 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).

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. Op deze laag onderscheiden we bij deze toegang twee rollen : de rol *PGO Presenter* die zorgt voor gebruikerstoegang, en de rol *PGO User Agent* die zorgt voor toegang voor de *PGO Server*. Het is die laatste rol die verbonden wordt met de rollen *OAuth User Agent* en *SAML User Agent*.

De rollen *Authorization Server* en *Resource Server* werken in het huidige MedMij-afsprakenstelsel samen in eenzelfde synchrone sessie. Hun onderlinge relatie is een proceskoppeling. Dat wil zeggen, zij worden georkestreerd onder de hoede van één procesgang, niet door middel van een meerzijdige choreografie.

Het MedMij Afsprakenstelsel staat toe dat deze twee rollen in één gezamenlijke implementatie worden ondergebracht. Dat is expliciet toegestaan door de OAuth-specificatie, past bij het feit dat er geen separate autorisatievoorzieningen zijn en is efficiënt, omdat het het complexe informatieverkeer voorkomt dat anders tussen de twee gescheiden rollen zou moeten plaatsvinden. Maar, het is ook mogelijk de twee rollen gescheiden te implementeren, zolang hun onderlinge proceskoppeling gehandhaafd blijft en de beschreven beveiligingsmaatregelen getroffen worden.

De standaarden OAuth 2.0 en SAML 2.0 hebben verschillende doelen: OAuth voor autorisatie en SAML voor authenticatie. Dat zorgt er onder andere voor dat de rolstructuur anders is. In OAuth is er een gebruiker (*Resource Owner*) die via zijn browser of app (*User Agent*) aan de ene applicatie (*Client*) toegang verleent aan een andere (*Resource Server*), welke laatste zich daarvoor laat bijstaan door een *Authorization Server*. In SAML is er een gebruiker die via een browser of app (*User Agent*) inlogt bij een dienst (*Service Provider*), die zich daarvoor laat bijstaan door een *Identity Provider*.

Toch zitten er belangrijke overeenkomsten tussen de manieren waarop ze werken.

- Beide gaan ervan uit dat de eindgebruiker zich aandient via een betrekkelijk onveilig kanaal (de *User Agent*, het "front-channel"), terwijl er ook gevoeliger informatie moet worden uitgewisseld ("back-channel"), dat niet via dit kanaal verloopt.
- Bij beide moet de *User Agent* aan de hand worden genomen en heen- en teruggestuurd (redirect). Bij OAuth is dat van de *Client* naar de *Authorization Server* en terug. Bij SAML is dat van de *Service Provider* naar de *Identity Provider* en terug.
- Bij beide krijgt de dienstverlener (bij OAuth de *Authorization Provider* en bij SAML de *Service Provider*) niet onmiddellijk de gewenste informatie (bij OAuth het access token en bij SAML de gebruikersidentiteit, bij DigiD het BSN), maar via een ophaalbewijs (bij OAuth de authorization code, bij SAML het artefact). Het ophaalbewijs gaat voorlangs (via de *User Agent*), waarna achterlangs met het ophaalbewijs de gewenste informatie wordt opgehaald.

In artikel 7 wordt het *MedMij-verkeer* afgebakend, met het oog op de Netwerk-laag. Al het *MedMij-verkeer* is over domeingrenzen. Bovendien maakt noch eventueel verkeer tussen *PGO Presenter* en *PGO User Agent*, noch eventueel verkeer tussen *Authorization Server* en *Resource Server* deel uit van *MedMij-verkeer*. SAML-verkeer is uitgesloten, omdat het MedMij Afsprakenstelsel geen eisen kan opleggen aan Digid. Deze afbakening is bovendien de opmaat voor artikel 8. Het daarin gemaakte onderscheid tussen frontchannel- en backchannelverkeer is nodig voor het formuleren van verantwoordelijkheden over adressering (zie Gegevens en performance in UCI Verzamelen en UCI Delen) en beveiliging (zie Netwerk). In artikel 7 moet ermee rekening gehouden worden dat er ook een use case-implementatie is op de Netwerk-laag: *UCI Opvragen Whitelist*.

Verantwoordelijkheden

Toelichting

De verantwoordelijkheden op deze laag en die op de processen- en informatielaag hebben een vergelijkbare opbouw. Ze zijn geordend in hoofdstukjes en secties als volgt:

- Dossier en toestemmingen
  - Use cases
  - Gegevensdiensten
  - Authenticatie
  - Autorisatie
- Lijsten
  - Zorgaanbiederslijst
  - OAuth Client List
  - Gegevensdienstnamenlijst
- Beveiliging

Van vijf van de zes use cases (zie de laag Processen en Informatie) wordt op deze (Applicatie)laag een use case-implementatie (UCI) voorgeschreven. Het gaat om:

use case-implementatie	Stroomdiagram
UCI Verzamelen	met
UCI Delen	met
UCI Opvragen ZAL	met
UCI Opvragen OCL	met
UCI Opvragen GNL	met

Dossier en toestemmingen

Use cases

1a. Bovengenoemde rollen implementeren de use case *UC Verzamelen* met de use case-implementatie *UCI Verzamelen*. Zij gebruiken hiertoe het betreffende stroomdiagram. De gehele procesgang wordt synchroon uitgevoerd.

1b. Bovengenoemde rollen implementeren de use case *UC Delen* met de use case-implementatie *UCI Delen* . Zij gebruiken hiertoe het betreffende stroomdiagram. De gehele procesgang wordt synchroon uitgevoerd.

> **Toelichting**
>
> In deze release van het MedMij Afsprakenstelsel zijn de use cases *UC Verzamelen* (eenmalige verzameling) en *UC Delen* (eenmalig delen) de enige waarin gezondheidsinformatie wordt gedeeld. Omdat de verzameling en deling eenmalig zijn, kunnen autorisatie en authenticatie nog verweven zijn in de betreffende flows. De gebruikersbeleving wordt het best bediend door de gehele procesgang synchroon te houden.

Gegevensdiensten

2. Voor zover een *Uitgever* de use case *UC Verzamelen* of *UC Delen* bij een *Bron* voor een zekere *Gegevensdienst* aanbiedt aan een *Zorggebruiker* zullen de *PGO Server* van die *Uitgever* en de *Authorization Server* en *Resource Server* van die *Bron*, respectievelijk *Lezer,* deze use case implementeren en daarvoor de standaarden gebruiken die voor die soort *Gegevensdienst* in de *Catalogus* wordt voorgeschreven.

> **Toelichting**
>
> Zo wordt geborgd dat voor de verschillende soorten informatie de juiste MedMij-informatiestandaarden worden gebruikt.

Authenticatie

3. Tijdens de use case-implementaties *UCI Verzamelen* en *UCI Delen* laat de *Authorization Server,* ten behoeve van zijn rol in deze use case-implementaties, en in zijn SAML-rol als *Service Provider*, onmiddellijk na de start van de OAuth-flow en voordat hij de *Zorggebruiker* om OAuth-autorisatie vraagt, de *Zorggebruiker* authenticeren door DigiD, volgens het SAML 2.0 koppelvlak van DigiD.

> **Toelichting**
>
> Conform stroomdiagram onder 1. De zorgaanbieder in het Zorgaanbieders- en dus BSN-domein is verplicht bij het verstrekken van gegevens vanuit een gezondheidsdossier de identiteit van de persoon te verifiëren aan de hand van het BSN. Uit het Juridisch kader volgt vooralsnog gebruik van DigiD voor dit doel.

Autorisatie

4. Tijdens de use case-implementaties *UCI Verzamelen* en *UCI Delen* zet de *Authorization Server*, onmiddellijk na de authenticatie van de *Zorggebruiker* zoals bedoeld onder 3, de OAuth-autorisatie voort, volgens de standaard OAuth 2.0.

> **Toelichting**
>
> Conform wettelijke verplichting geeft *Zorggebruiker*, in de *UC Verzamelen*, actief toestemming aan de *Zorgaanbieder.* In de *UC Delen* is deze verplichting niet aan de orde, maar vindt op dit moment evengoed een bevestiging door de *Zorggebruiker* plaats. Op de *PGO Client* wordt een venster

getoond waarin de *Zorggebruiker* deze toestemming, respectievelijk bevestiging, kan geven. Aangezien in de *PGO Client* niet met BSN gewerkt mag worden, moet er een vervangende identificatie van de zorggebruiker gebruikt worden. Zie regel 5.

5. Voor zover er in het verkeer tussen *PGO Server* en *Resource Server* in de use case-implementaties *UCI Verzamelen* en *UCI Delen* sprake is, in de stuurgegevens, van een gegevenselement dat tot de identiteit van de *Zorggebruiker* herleid kan worden, gebruiken zij daarvoor niets anders dan de OAuth-gegevens die zij in hun respectievelijke *OAuth Client* en *OAuth Resource Server* moeten uitwisselen. *PGO Server*, *Authorization Server* en *Resource Server* treffen goed beveiligde voorzieningen waarmee zij hieruit waar nodig zelf de identiteit van de *Zorggebruiker* kunnen vaststellen. Voor zover in onder 2 genoemde *Gegevensdiensten* sprake is van een informatie-element dat het BSN bevat, zal deze niet worden gebruikt of leeg blijven.

Toelichting

Met het oog op het borgen van de privacy en het zo eenvoudig mogelijk houden van de architectuur, wordt in deze release van het afsprakenstelsel ervoor gekozen de identifier voor de *Zorggebruiker* onderweg zo betekenisloos mogelijk te houden. Alle betekenis wordt er ter weerszijden aan verbonden door raadpleging van interne registraties. Omdat de *PGO Server, Authorization Server* en *Resource Server* samen een OAuth-flow afhandelen, beschikken zij (na authenticatie van de *Zorggebruiker*) over tokens die de identiteit van de *Zorggebruiker* vertegenwoordigen, namelijk (eerst) de authorization code en (later) het access token. Buiten deze hoeft en zal er geen identificerende gegevenselementen in het verkeer worden opgenomen. Het FHIR-gegevenselement *PatientID* wordt, in elk geval in deze release van het MedMij Afsprakenstelsel, *niet* gebruikt.

6. Van de vier soorten authorization grants die OAuth 2.0 biedt, beperken de OAuth-rollen zich tot Authorization Code.

Toelichting

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.

7. De *OAuth Client* en *OAuth Resource Server* zullen slechts tokens van het type Bearer Token uitwisselen, conform RFC6750.

Toelichting

De OAuth-standaard laat het (access) token type vrij. Token types verschillen in het vertrouwen waarmee de *Resource Server* aan de *Client* de gevraagde resources kan prijsgeven als laatstgenoemde het access token aan eerstgenoemde overlegt. Bij de eenvoudigste vorm (Bearer Token) geeft de *Resource Server* eenvoudigweg aan elke *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 *Client* aan wie het uitgedeeld was. Andere token types kunnen daarom vragen om meer garanties, zoals een identiteit van de *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 *Client* en *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. Zie hiervoor verantwoordelijkheden 26, 27 en 28.

8. 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 bepaald is door de op te vragen *Gegevensdienst*.

Toelichting

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 opvraging.

9. 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.

Toelichting

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 *Verzamelen* synchroon uitgevoerd (zie onder 1). De 900 seconden moeten dan voldoende zijn voor de Client om het access token aan de *Authorization Server* aan te bieden. Een refresh token is dan niet nodig.

10. De *OAuth Authorization Server* genereert authorization codes en access tokens volgens UUID. Daarbij wordt slechts gebruik gemaakt van UUID Version 4 en van cryptografisch veilige random number generators. Met betrekking tot zowel authorization codes als access tokens, draagt de *OAuth Authorization Server* ervoor zorg dat nooit twee dezelfde geldige door haar uitgebrachte daarvan in omloop zijn.

Toelichting

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 onderweg betekenisloos is en alleen betekenis krijgt door confrontatie met lokale en goed beschermde administraties. Ook moeten deze niet geraden kunnen worden en mag door vergelijking van meerdere codes/tokens niet doorschemeren hoe zij gegenereerd worden. Bovendien maakt MedMij bij voorkeur gebruik van standaarden voor dergelijke identifiers. UUID Version 4 biedt de gewenste betekenisloosheid onderweg, omdat de gehele identifier willekeurig wordt gegenereerd. De tweede eis, uniciteit, is ook erg belangrijk, maar de door UUID nagestreefde *globale* uniciteit, dat wil zeggen, uniciteit over alle lokale contexten heen, is niet nodig. In het MedMij Afsprakenstelsel worden authorization codes en access tokens alleen uitgedeeld door een specifieke Authorization Server en een specifieke geldigheidsduur. Alleen binnen die contexten hoeft de authorization code, respectievelijk het acces token, uniek te zijn. UUID Version 4 zelf biedt geen garantie op uniciteit: zoals in een groep van 23 mensen de kans al 50% is dat er twee op dezelfde datum jarig zijn, kunnen twee willekeurige identifiers toch hetzelfde zijn. Dit kan echter door de Authorization Server worden gedetecteerd door administraties bij te houden van de door haar uitgegeven en nog geldige authorization codes, respectievelijk access tokens. Mocht een nieuw gegenereerde identifier daarin voorkomen, dan moet er een nieuwe gegenereerd worden.

Noch in de authorization code, noch in het access token wordt betekenisvolle informatie opgenomen. Dat zorgt er ook voor dat er een minimale afhankelijkheid wordt gecreëerd tussen de dienstverleners

in het persoonsdomein enerzijds en die in het zorgaanbiedersdomein anderzijds, zodat principes P1 en P7 maximaal wordt nageleefd en interne complexiteit en implementatiekeuzes in het zorgaanbiedersdomein niet doorschemeren in, of invloed uitoefenen op, de implementatie in het persoonsdomein. Deze eis van betekenisloosheid geldt zelfs als de in de authorization code of het access token opgenomen informatie versleuteld zou zijn en zo ontoegankelijk gemaakt voor interpretatie onderweg, of zelfs voor interpretatie door de PGO Server (zodat de PGO Server een onwetende tussenschakel zou worden in het verkeer tussen componenten in het zorgaanbiedersdomein). Dit zou namelijk intern verkeer in het zorgaanbiedersdomein onnodig gevoelig maken voor compromittering in het persoonsdomein. Zulke compromittering zou bovendien moeilijk te ontdekken en te pareren zijn in het zorgaanbiedersdomein, 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 PGO Server.

Het formaat van UUIDs wordt textueel vaak opgeschreven in 32 hexadecimalen, hier en daar gescheiden door streepjes, als volgt:

`xxxxxxxx-xxxx-Mxxx-Nxxx-xxxxxxxxxxxx`

Hierbij worden de vier bits van `M` gebruikt voor het UUID-versienummer (in het MedMij Afsprakenstelsel dus: 4) en de eerste twee bits van `N` voor het zogenoemde variantnummer (altijd 1 in de betreffende UUID-RFC). Daarmee zien in het MedMij Afsprakenstelsel zowel de authorization code als het acces token eruit als:

`xxxxxxxx-xxxx-4xxx-Nxxx-xxxxxxxxxxxx`, met `N` = `10bb` (in bits) en alle `b` en `x` random. Let wel, met random wordt niet bedoeld dat er geen eisen aan worden gesteld, maar juist dat eraan de eis wordt gesteld dat de waarden willekeurig worden gegenereerd.

11. De *OAuth Client* biedt een zekere authorization code maximaal eenmaal aan aan de *Authorization Server* ter verkrijging van een access token. De *Authorization Server* voert een authorization code af, wanneer het eenmaal is aangeboden ter verkrijging voor een access token.

Toelichting

Dit is een maatregel tegen beveiligingsrisico 4.4.1 uit RFC 6819. 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.

12. De *OAuth Authorization Server* draagt alleen een access token over aan een *OAuth Client* als de daartoe aangeboden authorization code aan diezelfde *OAuth Client* is afgegeven.

Toelichting

Dit is een maatregel tegen beveiligingsrisico's 4.4.1.3, 4.4.1.5 en 4.4.1.7 uit RFC 6819. Hiervoor moet de *Authorization Server* dus bijhouden aan welke *Clients* hij de authorization codes uitdeelt. Dit betekent dat het access token alleen mag worden uitgereikt via een redirect URI waarbij de hostname gelijk is aan de hostname van de *OAuth Client* voor wie de bijbehorende authorization code bedoeld was.

13. De *OAuth Client* en *OAuth Authorization Server* gebruiken voor al hun onderlinge verkeer PKIoverheid-certificaten, en wel servercertificaten, ten behoeve van de authenticatie van de andere server in een uitwisseling.

Toelichting

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

14. De *OAuth Client* biedt, al dan niet via de *OAuth User Agent*, aan de *OAuth Authorization Servers* slechts redirect URI's aan die volledig (full) zijn én verwijzen naar een `https`-beschermd endpoint. *OAuth Authorization Servers* redirecten niet naar een URI die niet aan deze eisen voldoet.

Toelichting

Dit is een maatregel tegen beveiligingsrisico's 4.1.5, 4.2.4, 4.4.1.1, 4.4.1.5 en 4.4.1.6 in RFC 6819. Zie bovendien de tweede toelichting onder 14.

15. Het OAuth-client type van de *OAuth Client* is confidential.

Toelichting

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 *Authorization Server* afdoende mate van vertrouwelijkheid van zijn credentials bieden, de tweede 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 *Clients* ten behoeve van hun betrouwbaarheid jegens *Authorization Servers*. We verwachten dat een groot deel van de implementaties van de Oauth *Client* (van de *PGO Server* dus) deze vertrouwelijkheid sowieso kunnen bieden, omdat ze de architectuur hebben van wat de OAuth-specificatie web application noemt. Andersoortige *PGO Server*-architecturen, zoals die van een app, blijven nog steeds mogelijk, maar daarvan zal worden gevraagd dat zij al het verkeer van OAuth client credentials in de achtergrond op een server zullen afhandelen, niet op het user device.

Lijsten

Zorgaanbiederslijst

16. *MedMij Beheer* en elke *PGO Server* implementeren de use case *UC Opvragen ZAL* met de use case-implementatie *UCI Opvragen ZAL*. Zij gebruiken hiertoe het betreffende stroomdiagram.

17. *PGO Servers* betrekken minstens elke vijftien minuten (900 seconden) de meest recente *Zorgaanbiederslijst* van *MedMij Registratie*.

18. *Dienstverlener persoon* valideert elke nieuw verkregen *Zorgaanbiederslijst* tegen het XML-schema van de *Zorgaanbiederslijst*. Dit XML-schema is een technische implementatie van het MedMij-metamodel.

OAuth Client List

19. *MedMij Registratie* en *Authorization Server* implementeren de use case *UC Opvragen OCL* met de use case-implementatie *UCI Opvragen OCL*. Zij gebruiken hiervoor het betreffende stroomdiagram.

20. *Authorization Server* betrekt minstens elke vijftien minuten (900 seconden) de meest recente *OAuth Client List* van *MedMij Registratie*.

21. *Authorization Server* valideert elke nieuwe verkregen *OAuth Client List* tegen het XML-schema van de *OAuth Client List*. Dit XML-schema is een technische implementatie van het MedMij-metamodel.

> Omdat op de *OAuth Client List* de hostname van een *(PGO) Node* wordt gebruikt om een *OAuth Client* te identificeren, stelt de netwerklaag als eis dat eenzelfde *OAuth Client* altijd op dezelfde *PGO Node* draait.

Gegevensdienstnamenlijst

22. *MedMij Registratie* en *PGO Server* implementeren de use case *UC Opvragen GNL* met de use case-implementatie *UCI Opvragen GNL*. Zij gebruiken hiervoor het betreffende stroomdiagram.

23. *PGO Server* betrekt minstens elke vijftien minuten (900 seconden) de meest recente *GNL-implementatie* van *MedMij Registratie*.

24. *PGO Server* valideert elke nieuwe verkregen *GNL-implementatie* tegen het XML-schema van de GNL. Dit XML-schema is een technische implementatie van het MedMij-metamodel.

Beveiliging

25. In het gegevensverkeer dat zich voltrekt in het kader van *UCI Verzamelen*, *UCI Delen*, *UCI Opvragen ZAL*, *UCI Opvragen OCL* en *UCI Opvragen GNL*, maken deze gebruik van de functies *Versleuteling*, *Server Authentication* en *Server Authorization*, volgens het bepaalde op de Netwerk-laag.

26. De *OAuth Client* realiseert de volgende beveiligingsmaatregelen, conform RFC6819:

beveiligingsmaatregel	paragraaf in RFC6819	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

27. De *PGO Server* realiseert de volgende beveiligingsmaatregelen, conform RFC6819:

beveiligingsmaatregel	paragraaf in RFC6819	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

28. De *OAuth Authorization Server* realiseert de volgende beveiligingsmaatregelen, conform RFC6819:

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

Toelichting

Voor het opstellen van verantwoordelijkheden 26,27 en 28 is gebruik gemaakt 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. Zie hiervoor verantwoordelijkheid 7 op deze laag.

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

- bedreiging 4.1.1: Obtaining Client Secrets, omdat authenticatie van OAuth Clients in MedMij werkt op basis van PKI-servercertificaten, niet op basis van client secrets;
- 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 4.4.1.1: 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. Deze betreffen bijvoorbeeld het gebruik van TLS (Netwerk-laag), Digid (Applicatie-laag) en UUID (Applicatie-laag) en het beperken van de scope en de geldigheidsduur van authorization codes en access tokens (Applicatie-laag);
- maatregelen die weliswaar door RFC6819 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 *PGO Server*, *OAuth Client* of *OAuth Authorization Server*.

Met bovenstaande verantwoordelijkheden 26, 27 en 28 is die laatste groep van maatregelen ook onderdeel van het MedMij Afsprakenstelsel.

29. *OAuth Clients*, *Authorization Server* en *OAuth Resource Server* implementeren de op deze respectievelijke rollen toepasselijke beveiligingsmaatregelen, volgens paragaaf 5.3 van RFC6750.

Toelichting

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.

UCI Verzamelen

Toelichting

In de platen hieronder staat het stroomdiagram van de use case-implementatie *Verzamelen*, in vier perspectieven:

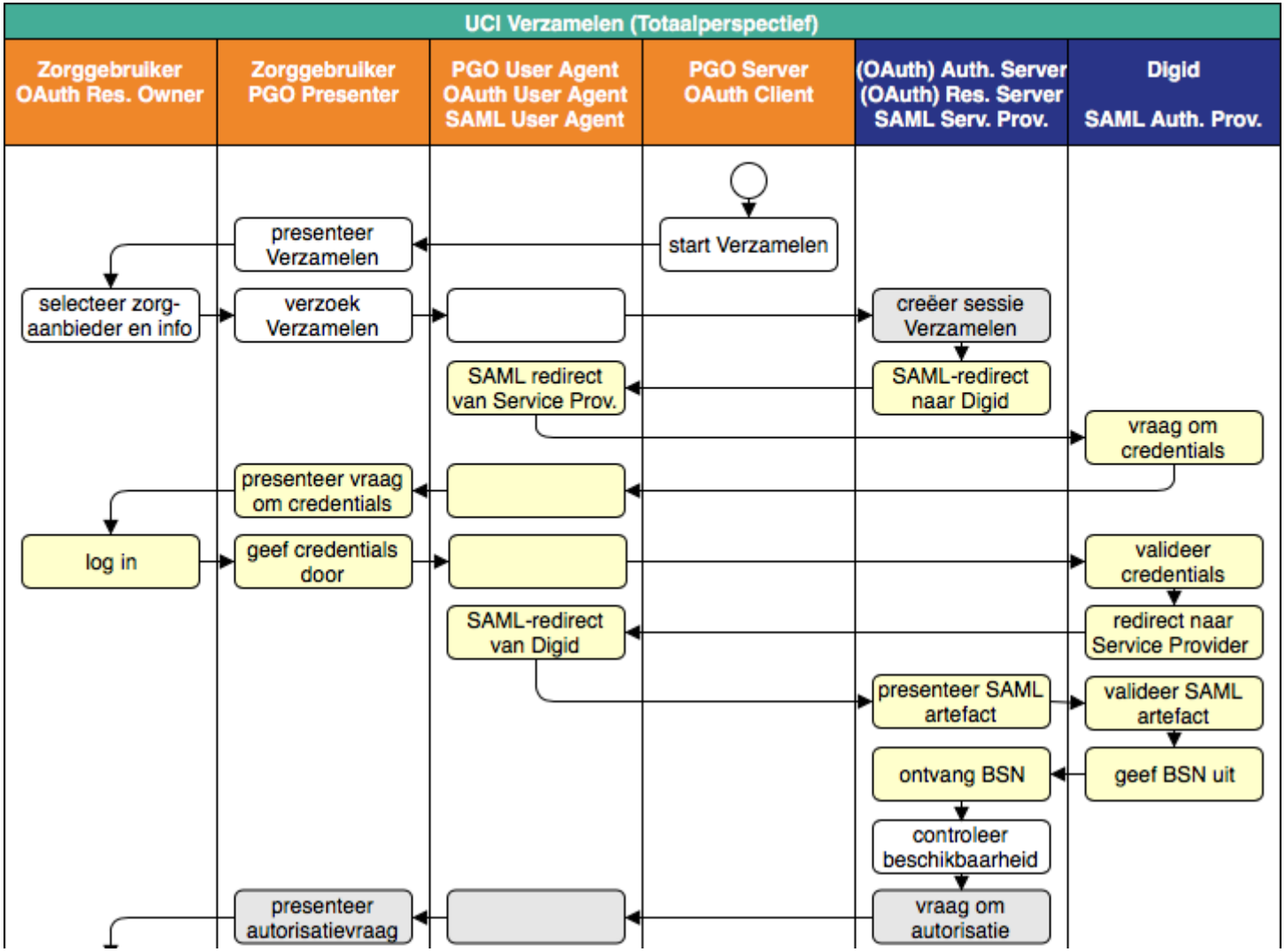
- het totaalperspectief, met zowel de happy flow als de uitzonderingen;
- het perspectief van de *PGO Server* (= *OAuth Client*), die onder de hoede van de *Dienstverlener Persoon* valt. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Verzamelen;*
- het perspectief van de (*OAuth) Authorization Server/(OAuth) Resource Server/SAML Service Provider*, die onder de hoede van de *Dienstverlener Zorgaanbieder* valt. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Verzamelen;*
- het perspectief van de *Zorggebruiker* (= *OAuth Resource Owner*).

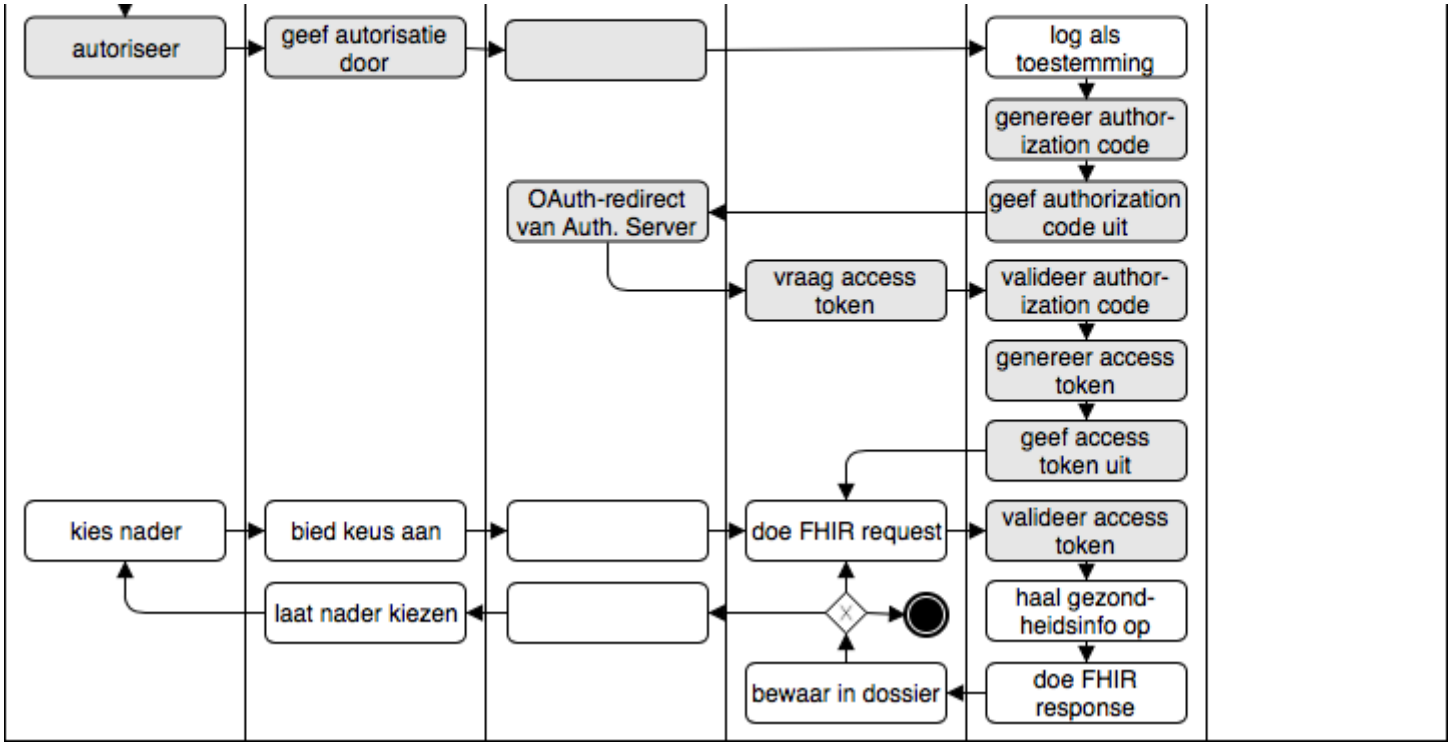
De stroomdiagrammen tonen alleen de situatie waarin alle acties slagen tot en met het uiteindelijke verzamelen van de gezondheidsinformatie (de zogenaamde happy flow). De drie oranje banen horen, conform de MedMij-huisstijl tot het Persoonsdomein, de twee blauwe tot het Zorgaanbiedersdomein. Menige actie in de stroomdiagrammen is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow volgens OAuth 2; de zachtgeel gekleurde acties vormen samen de authenticatieflow volgens DigiD/SAML. 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. In de stroomdiagrammen voor de specifieke perspectieven hebben alleen de acties in de bij dat perspectief horende baan namen. De acties in de andere banen zijn gecomprimeerd en anoniem weergegeven.

Verantwoordelijkheden inzake de gegevens die omgaan in deze use case-implementatie zijn, samen met die van UCI Delen, opgenomen in een aparte pagina.

Totaalperspectief

Happy flow


UCI Verzamelen (Totaalperspectief)
Zorggebruiker OAuth Res. Owner
Zorggebruiker PGO Presenter
PGO User Agent OAuth User Agent SAML User Agent
PGO Server OAuth Client
(OAuth) Auth. Server (OAuth) Res. Server SAML Serv. Prov.
Digid SAML Auth. Prov.
start Verzamelen
presenteer Verzamelen
selecteer zorg-aanbieder en info
verzoek Verzamelen
creëer sessie Verzamelen
SAML-redirect naar Digid
SAML redirect van Service Prov.
vraag om credentials
presenteer vraag om credentials
log in
geef credentials door
valideer credentials
redirect naar Service Provider
SAML-redirect van Digid
presenteer SAML artefact
valideer SAML artefact
ontvang BSN
geef BSN uit
controleer beschikbaarheid
presenteer autorisatievraag
vraag om autorisatie



Toelichting

De flow kent de volgende stappen:

1. De *PGO Server* start de flow door in de *PGO Presenter* van de *Zorggebruiker* de mogelijkheid te presenteren om een bepaalde *Gegevensdienst* bij een zekere *Zorgaanbieder* te verzamelen. Het gaat altijd om precies één *Gegevensdienst* (één scope, in OAuth-termen). Uit de *Zorgaanbiederslijst* weet de *PGO Server* welke *Gegevensdiensten* voor een *Zorgaanbieder* beschikbaar zijn. Desgewenst worden de *Gegevensdienstnamen* uit de *Gegevensdienstnamenlijst* gebruikt.

2. De *Zorggebruiker* maakt expliciet zijn selectie en laat de *OAuth User Agent* een verzamel-verzoek sturen naar de *Authorization Server*. Het adres van het authorization endpoint komt uit de *ZAL*. De redirect URI geeft aan waarnaartoe de *Authorization Server* de *OAuth 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. Dan start de *Authorization Server* (nu in de rol van *SAML Service Provider*) de SAML-flow door de browser naar *DigiD* te redirecten, onder meegeven van een redirect URI, die aangeeft waarnaartoe *DigiD* straks de *OAuth User Agent* moet terugsturen, na het inloggen van de *Zorggebruiker*.
5. DigiD vraagt van de *Zorggebruiker* via zijn *User Agent* om inloggegevens.
6. Wanneer deze juist zijn, redirect *DigiD* de *OAuth User Agent* terug naar de *Authorization Server*, onder meegeven van een ophaalbewijs: het SAML-artefact.
7. Met dit ophaalbewijs haalt de *Authorization Server* rechtstreeks bij *DigiD* het BSN op.
8. De *Authorization Server* controleert alvast of de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft. Daarvan maakt deel uit dat de *Persoon* daarvoor meerderjarig of minstens 16 jaar oud moet zijn.
9. Zo ja, dan presenteert de *Authorization Server* via de *PGO Presenter* aan *Zorggebruiker* de vraag of laatstgenoemde hem toestaat de gevraagde persoonlijke gezondheidsinformatie aan de *PGO Server* (als *OAuth Client*) te sturen. Onder het flow-diagram staat gespecificeerd welke informatie, waarvandaan, de *OAuth Authorization Server* verwerkt in de aan *Zorggebruiker* voor te leggen autorisatievraag.
10. 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 *PGO Server*. De *Authorization Server* stuurt daarbij de local state-informatie mee die hij in de eerste stap van de *PGO Server* heeft gekregen. Laatstgenoemde herkent daaraan het verzoek waarmee hij de authorization code moet associëren.
11. De *PGO 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.
12. Met dit ophaalbewijs wendt de *PGO Server* zich weer tot de *Authorization Server*, maar nu zonder tussenkomst van de *OAuth User Agent*, voor een access token.
13. Daarop genereert de *Authorization Server* een access token en stuurt deze naar de *PGO Server*.
14. Nu is de *PGO Server* gereed om het verzoek om de gezondheidsinformatie naar de *Resource Server* te sturen. 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.
15. De *Resource Server* controleert of het ontvangen token recht geeft op de gevraagde resources, haalt deze (al dan niet) bij achterliggende bronnen op en verstuurt ze in een FHIR-response naar de *PGO Server*.
16. Deze bewaart de ontvangen gezondheidsinformatie in het persoonlijke dossier. Mocht de *Gegevensdienst* waartoe de *Zorggebruiker* heeft geautoriseerd uit meerdere *Transacties* bestaan, bevraagt de *PGO Server* de *Resource Server* daarna mogelijk opnieuw voor de nog resterende *Transacties*, eventueel na nieuwe gebruikersinteractie. Zolang het access token geldig is, kan dat.

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

Uitzonderingen

Toelichting

In onderstaande tabel staan de uitzonderingssituaties beschreven. Zij kunnen gezien worden als de implementatie-tegenhangers van de uitzonderingen van de use case Verzamelen. Alle uitzonderingen worden door de *Authorization Server* of de *Resource 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. Om te voorkomen dat de *PGO Server* 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 *PGO Server*.

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.

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Vervolg
UCI Verzamelen 1	UC Verzamelen 1	*Authorization Server* vindt het ontvangen verzoek ongeldig.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert *Zorggebruiker* daarover.	conform OAuth 2.0-specificatie, par. 4.1.2.1, error code `invalid_request`, met in de error description de oorzaak	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Verzamelen 2	UC Verzamelen 2	*Authorization Server* kan de identiteit van de *Zorggebruiker* niet vaststellen.	*Authorization Server* informeert *PGO Server* over deze uitzondering.	conform OAuth 2.0-specificatie, par. 4.1.2.1, error code `access denied`, met in de error description "`Access denied.`"	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Verzamelen 3	UC Verzamelen 3	*Authorization Server* stelt vast dat van *Persoon* bij *Zorgaanbieder* geen gezondheidsinformatie voor die *Gegevensdienst* beschikbaar is.			

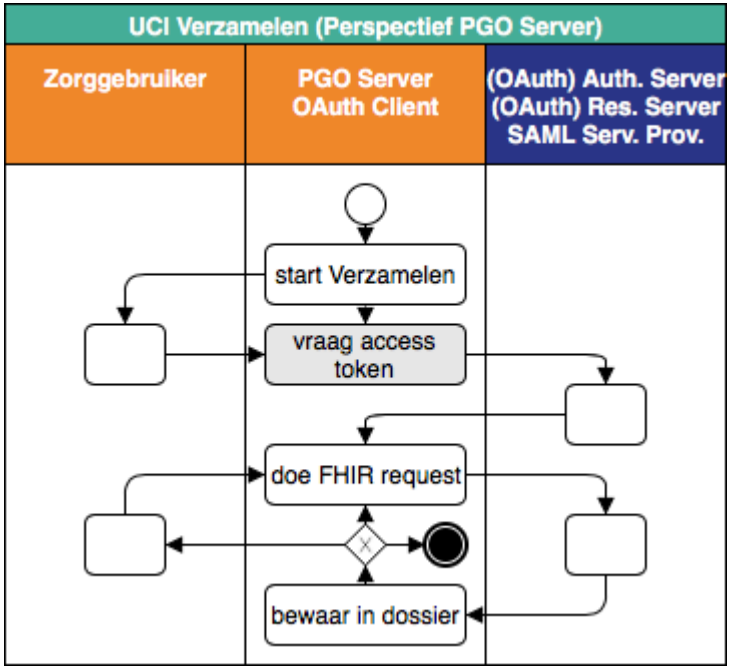
UCI Verzamelen 4	UC Verzamelen 4	De autorisatievraag wordt ontkennend beantwoord.			
UCI Verzamelen 5	UC Verzamelen 5	*Authorization Server* kan de autorisatie niet vaststellen.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform OAuth 2.0-specificatie, par. 4.1.2.1, error code `access denied`, met in de error description "`Authorization failed.`"	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Verzamelen 6	UC Verzamelen 6	De validatie van de authorization code door *Authorization Server* faalt.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform OAuth 2.0-specificatie, par. 5.2, error code `invalid_grant`	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Verzamelen 7	UC Verzamelen 6	De validatie van het access token door *Resource Server* faalt.	*Resource Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform FHIR-specificatie, in de FHIR-response, issue type security/suppressed	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Verzamelen 8	UC Verzamelen 5	*Resource Server* kan de gevraagde informatie niet ophalen bij achterliggende systemen.	*Resource Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform FHIR-specificatie, in de FHIR-response, issue type processing/incomplete	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

Specifieke perspectieven

Perspectief PGO Server (happy flow)

Toelichting

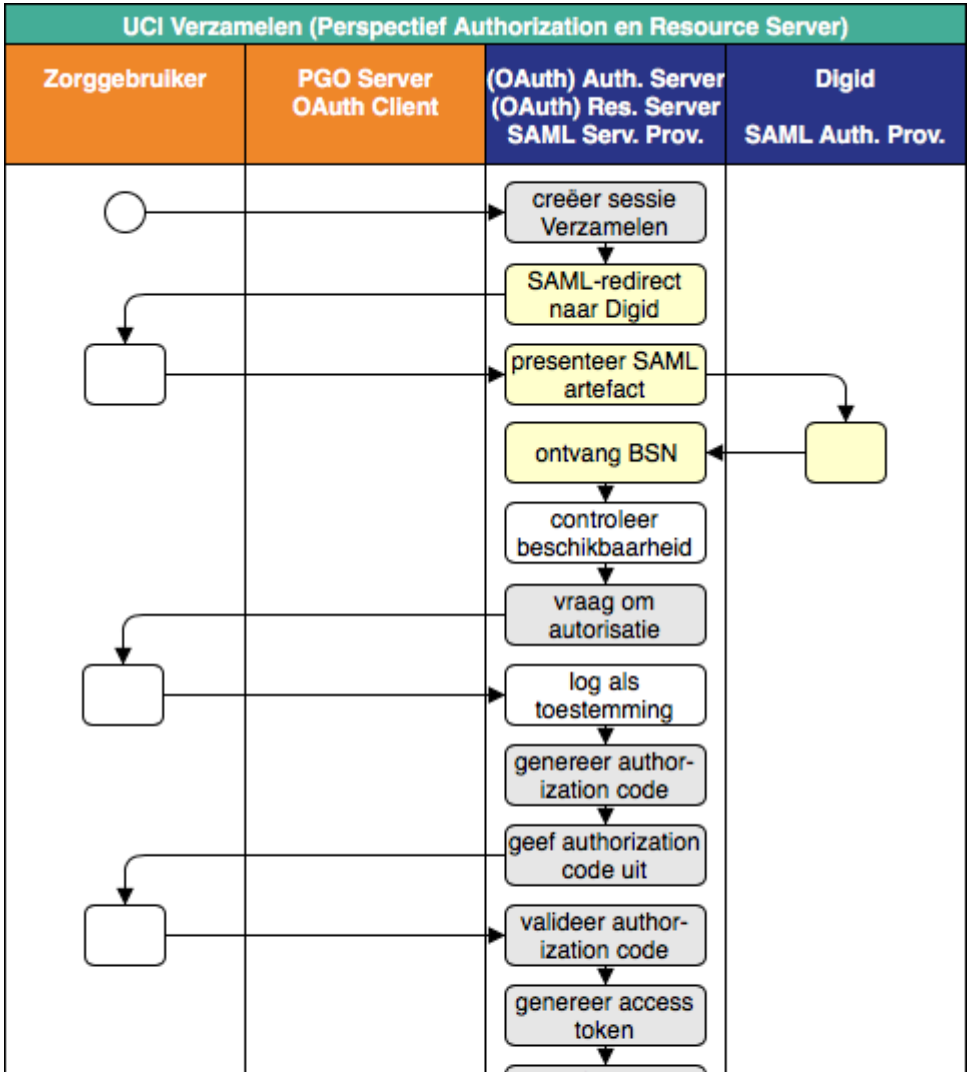
Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *PGO Server*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *PGO Server*, kortgesloten zijn. *Zorggebruiker* is "verborgen achter de browser" en *DigiD* "achter de *Authorization Server*".

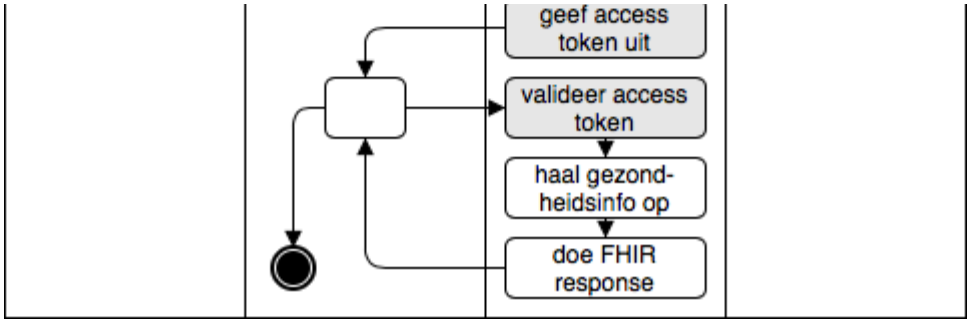


Perspectief Authorization Server/Resource Server (happy flow)

Toelichting

Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *Authorization/Resource Server*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *PGO Server*, kortgesloten zijn. *Zorggebruiker* is "verborgen achter de browser".

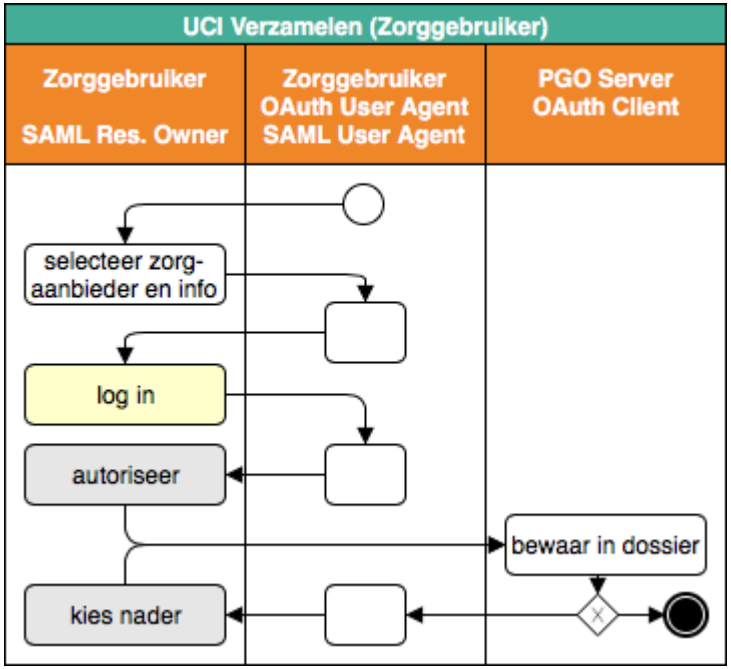

UCI Verzamelen (Perspectief Authorization en Resource Server)
Zorggebruiker
PGO Server
OAuth Client
(OAuth) Auth. Server
(OAuth) Res. Server
SAML Serv. Prov.
Digid
SAML Auth. Prov.
creëer sessie Verzamelen
SAML-redirect naar Digid
presenteer SAML artefact
ontvang BSN
controleer beschikbaarheid
vraag om autorisatie
log als toestemming
genereer author-ization code
geef authorization code uit
valideer author-ization code
genereer access token



Perspectief Zorggebruiker (happy flow)

Toelichting

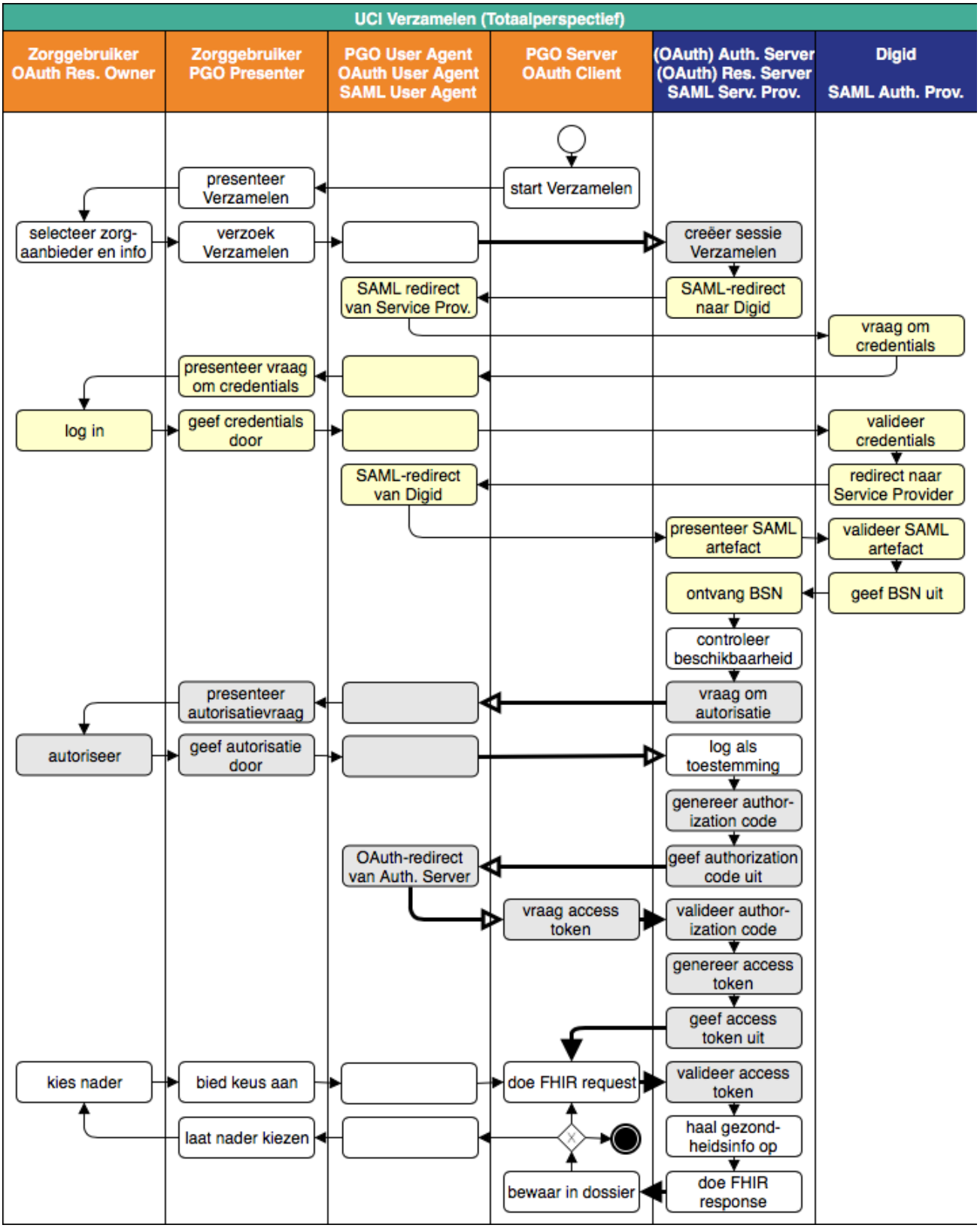
Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *Zorggebruiker*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *Zorggebruiker*, kortgesloten zijn. Vrijwel alles is "verborgen achter de browser". We hebben alleen de laatste stap van *PGO Server* zichtbaar gehouden, omdat het bewaren van de verzamelde gezondheidsinformatie betekenis heeft voor de *Zorggebruiker*. Waarschijnlijk zal de *PGO Server* de *Zorggebruiker* laten weten dat het verzamelen geslaagd is, maar dat is niet verplicht.


UCI Verzamelen (Zorggebruiker)
Zorggebruiker
SAML Res. Owner
Zorggebruiker
OAuth User Agent
SAML User Agent
PGO Server
OAuth Client
selecteer zorg-aanbieder en info
log in
autoriseer
bewaar in dossier
kies nader

Frontchannel en backchannel

Toelichting

In onderstaand stroomschema van UCI Verzamelen 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.


UCI Verzamelen (Totaalperspectief)
Zorggebruiker OAuth Res. Owner
Zorggebruiker PGO Presenter
PGO User Agent OAuth User Agent SAML User Agent
PGO Server OAuth Client
(OAuth) Auth. Server (OAuth) Res. Server SAML Serv. Prov.
Digid SAML Auth. Prov.
start Verzamelen
presenteer Verzamelen
selecteer zorg-aanbieder en info
verzoek Verzamelen
creëer sessie Verzamelen
SAML redirect van Service Prov.
SAML-redirect naar Digid
vraag om credentials
presenteer vraag om credentials
log in
geef credentials door
valideer credentials
SAML-redirect van Digid
redirect naar Service Provider
presenteer SAML artefact
valideer SAML artefact
ontvang BSN
geef BSN uit
controleer beschikbaarheid
presenteer autorisatievraag
vraag om autorisatie
autoriseer
geef autorisatie door
log als toestemming
genereer author-ization code
OAuth-redirect van Auth. Server
geef authorization code uit
vraag access token
valideer author-ization code
genereer access token
geef access token uit
kies nader
bied keus aan
doe FHIR request
valideer access token
laat nader kiezen
haal gezond-heidsinfo op
bewaar in dossier
doe FHIR response

UCI Delen

Toelichting

In de platen hieronder staat het stroomdiagram van de use case-implementatie *Delen*, in vier perspectieven:

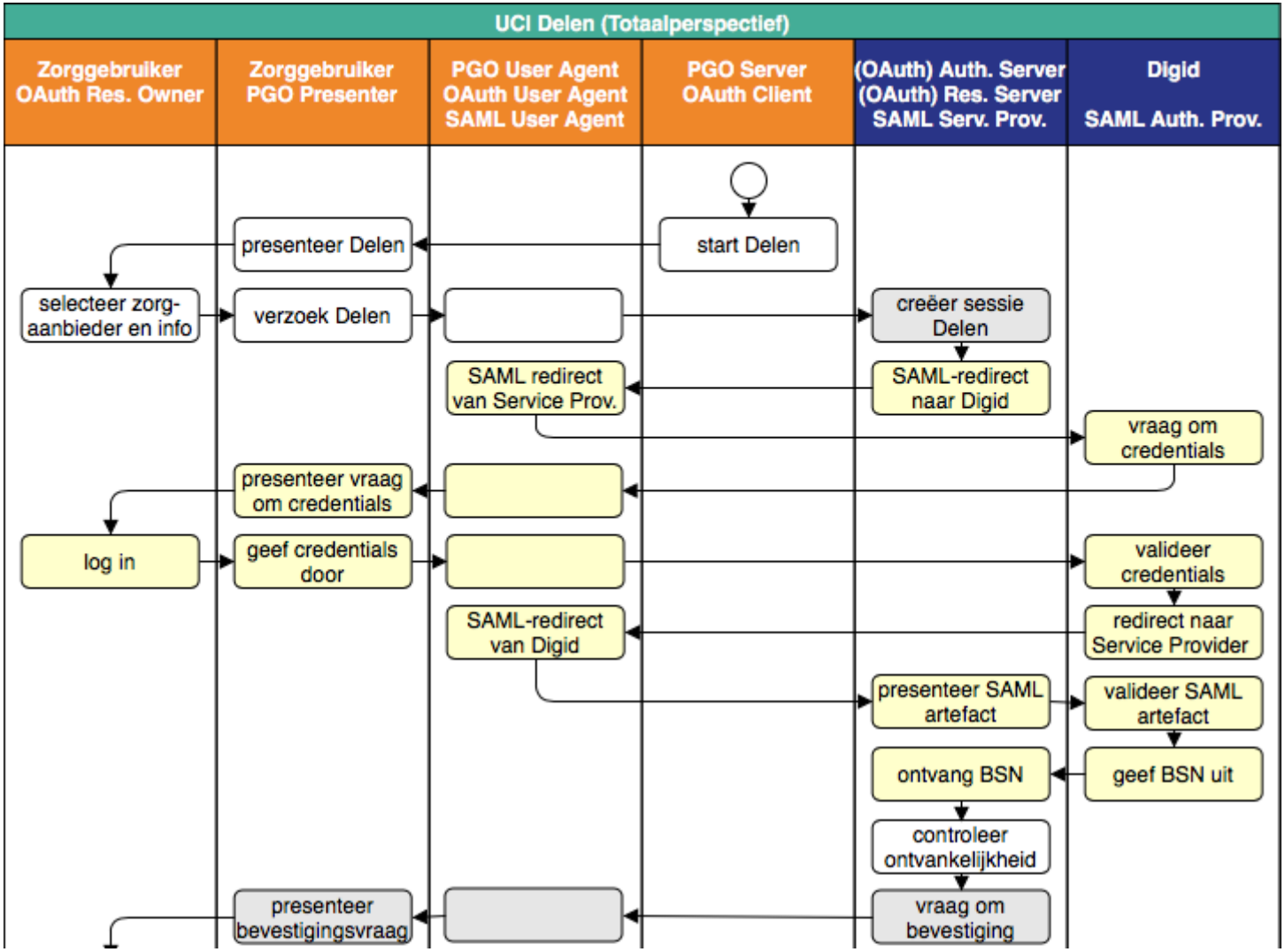
- het totaalperspectief, met zowel de happy flow als de uitzonderingen;
- het perspectief van de *PGO Server* (= *OAuth Client*), die onder de hoede van de *Dienstverlener Persoon* valt. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Delen;*
- het perspectief van de (*OAuth) Authorization Server/(OAuth) Resource Server/SAML Service Provider*, die onder de hoede van de *Dienstverlener Zorgaanbieder* valt. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Delen;*
- het perspectief van de *Zorggebruiker* (= *OAuth Resource Owner*).

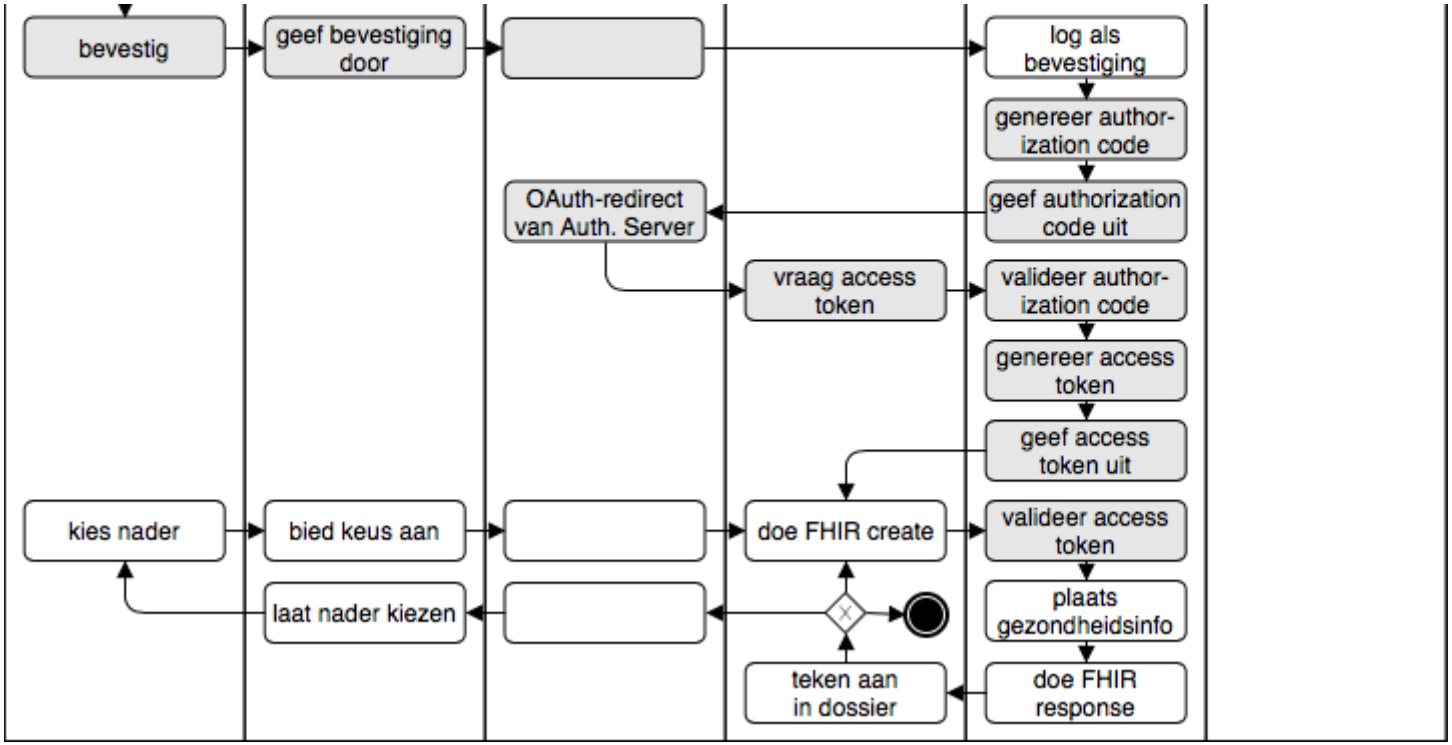
De stroomdiagrammen tonen alleen de situatie waarin alle acties slagen tot en met het uiteindelijke delen van de gezondheidsinformatie (de zogenaamde happy flow). De drie oranje banen horen, conform de MedMij-huisstijl tot het Persoonsdomein, de twee blauwe tot het Zorgaanbiedersdomein. Menige actie in de stroomdiagrammen is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow volgens OAuth 2; de zachtgeel gekleurde acties vormen samen de authenticatieflow volgens DigiD/SAML. 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. In de stroomdiagrammen voor de specifieke perspectieven hebben alleen de acties in de bij dat perspectief horende baan namen. De acties in de andere banen zijn gecomprimeerd en anoniem weergegeven.

Verantwoordelijkheden inzake de gegevens die omgaan in deze use case-implementatie zijn, samen met die van UCI Verzamelen, opgenomen in een aparte pagina.

Totaalperspectief

Happy flow


UCI Delen (Totaalperspectief)
Zorggebruiker OAuth Res. Owner
Zorggebruiker PGO Presenter
PGO User Agent OAuth User Agent SAML User Agent
PGO Server OAuth Client
(OAuth) Auth. Server (OAuth) Res. Server SAML Serv. Prov.
Digid SAML Auth. Prov.
start Delen
presenteer Delen
selecteer zorg-aanbieder en info
verzoek Delen
creëer sessie Delen
SAML-redirect naar Digid
SAML redirect van Service Prov.
vraag om credentials
presenteer vraag om credentials
log in
geef credentials door
valideer credentials
redirect naar Service Provider
SAML-redirect van Digid
presenteer SAML artefact
valideer SAML artefact
ontvang BSN
geef BSN uit
controleer ontvankelijkheid
vraag om bevestiging
presenteer bevestigingsvraag



Toelichting

De flow kent de volgende stappen:

1. De *PGO Server* start de flow door in de *PGO Presenter* van de *Zorggebruiker* de mogelijkheid te presenteren om een bepaalde *Gegevensdienst* met een zekere *Zorgaanbieder* te delen. Het gaat altijd om precies één *Gegevensdienst* (één scope, in OAuth-termen). Uit de *Zorgaanbiederslijst* weet de *PGO Server* welke *Gegevensdiensten* met een *Zorgaanbieder* beschikbaar zijn. Desgewenst worden de *Gegevensdienstnamen* uit de *Gegevensdienstnamenlijst* gebruikt.

2. De *Zorggebruiker* maakt expliciet zijn selectie en laat de *OAuth User Agent* een deel-verzoek sturen naar de *Authorization Server*. Het adres van het authorization endpoint komt uit de *ZAL*. De redirect URI geeft aan waarnaartoe de *Authorization Server* de *OAuth 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. Dan start de *Authorization Server* (nu in de rol van *SAML Service Provider*) de SAML-flow door de *OAuth User Agent* naar *DigiD* te redirecten, onder meegeven van een redirect URI, die aangeeft waarnaartoe *DigiD* straks de *OAuth User Agent* moet terugsturen, na het inloggen van de *Zorggebruiker*.
5. DigiD vraagt van de *Zorggebruiker* via zijn *User Agent* om inloggegevens.
6. Wanneer deze juist zijn, redirect *DigiD* de *OAuth User Agent* terug naar de *Authorization Server*, onder meegeven van een ophaalbewijs: het SAML-artefact.
7. Met dit ophaalbewijs haalt de *Authorization Server* rechtstreeks bij *DigiD* het BSN op.
8. De *Authorization Server* controleert alvast of de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt ontvankelijk is voor gezondheidsinformatie van die *Persoon*. Daarvan maakt deel uit dat de *Persoon* daarvoor meerderjarig of minstens 16 jaar oud moet zijn.
9. Zo ja, dan presenteert de *Authorization Server* via de *PGO Presenter* aan *Zorggebruiker* de vraag of laatstgenoemde bevestigt de gevraagde persoonlijke gezondheidsinformatie door de *PGO Server* (als *OAuth Client*) te laten aanbieden. Onder het stroomdiagram staat gespecificeerd welke informatie, waarvandaan, de *OAuth Authorization Server* verwerkt in de aan *Zorggebruiker* voor te leggen bevestigingsvraag.
10. 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 *PGO Server*. De *Authorization Server* stuurt daarbij de local state-informatie mee die hij in de eerste stap van de *PGO Server* heeft gekregen. Laatstgenoemde herkent daaraan het verzoek waarmee hij de authorization code moet associëren.
11. De *PGO 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.
12. Met dit ophaalbewijs wendt de *PGO Server* zich weer tot de *Authorization Server*, maar nu zonder tussenkomst van de *OAuth User Agent*, voor een access token.
13. Daarop genereert de *Authorization Server* een access token en stuurt deze naar de *PGO Server*.
14. Nu is de *PGO Server* gereed om de gezondheidsinformatie aan de *Resource Server* aan te bieden. 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.
15. 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 *PGO Server*.
16. Deze maakt hierover een aantekeningen bij de aangeboden gezondheidsinformatie in het persoonlijke dossier. Mocht de *Gegevensdienst* waartoe de *Zorggebruiker* heeft geautoriseerd uit meerdere *Transacties* bestaan, plaatst de *PGO Server* daarna mogelijk opnieuw bij de *Resource Server* voor de nog resterende *Transacties*, eventueel na nieuwe gebruikersinteractie. Zolang het access token geldig is, kan dat.

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

Uitzonderingen

Toelichting

In onderstaande tabel staan de uitzonderingssituaties beschreven. Zij kunnen gezien worden als de implementatie-tegenhangers van de uitzonderingen van de use case Delen. Alle uitzonderingen worden door de *Authorization Server* of de *Resource 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. Om te voorkomen dat de *PGO Server* 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 *PGO Server*.

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.

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Vervolg
UCI Delen 1	UC Delen 1	*Authorization Server* vindt het ontvangen verzoek ongeldig.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server*informeert *Zorggebruiker* daarover.	conform OAuth 2.0-specificatie, par. 4.1.2.1, error code `invalid_request`, met in de error description de oorzaak	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Delen 2	UC Delen 2	*Authorization Server* kan de identiteit van de *Zorggebruiker* niet vaststellen.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform OAuth 2.0-specificatie, par. 4.1.2.1, error code `access denied`, met in de error description "`Access denied.`"	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Delen 3	UC Delen 3	*Authorization Server* stelt vast dat *Zorgaanbieder* inzake deze *Gegevensdienst* niet ontvankelijk is voor gezondheidsinformatie van *Persoon*.			

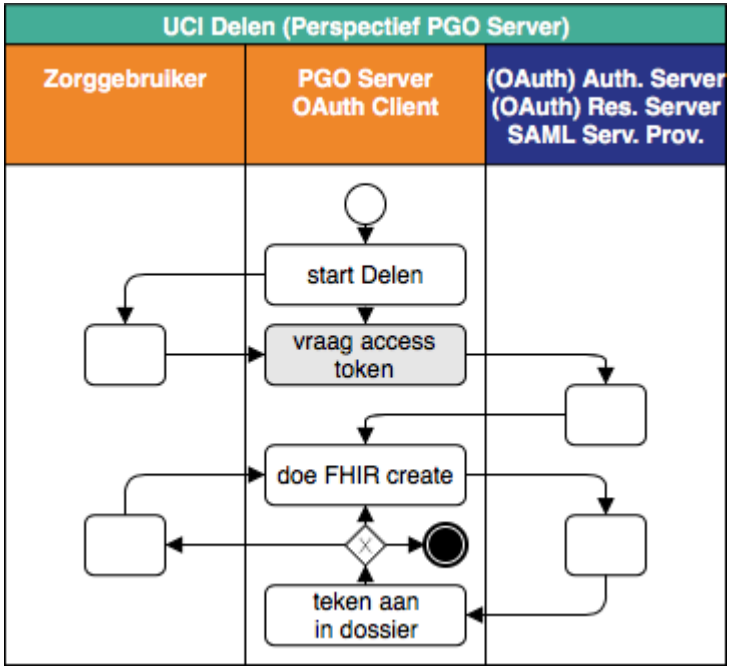
UCI Delen 4	UC Delen 4	De bevestigingvraag wordt ontkennend beantwoord.			
UCI Delen 5	UC Delen 5	*Authorization Server* kan de autorisatie niet vaststellen.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform OAuth 2.0-specificatie, par. 4.1.2.1, error code `access denied`, met in de error description "`Authorization failed.`"	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Delen 6	UC Delen 6	De validatie van de authorization code door *Authorization Server* faalt.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform OAuth 2.0-specificatie, par. 5.2, error code `invalid_grant`	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Delen 7	UC Delen 6	De validatie van het access token door *Resource Server* faalt.	*Resource Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform FHIR-specificatie, in de FHIR-response, issue type security/suppressed	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Delen 8	UC Delen 5	*Resource Server* kan de gevraagde informatie niet plaatsen bij achterliggende systemen.	*Resource Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform FHIR-specificatie, in de FHIR-response, issue type processing/incomplete	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

Specifieke perspectieven

Perspectief PGO Server (happy flow)

Toelichting

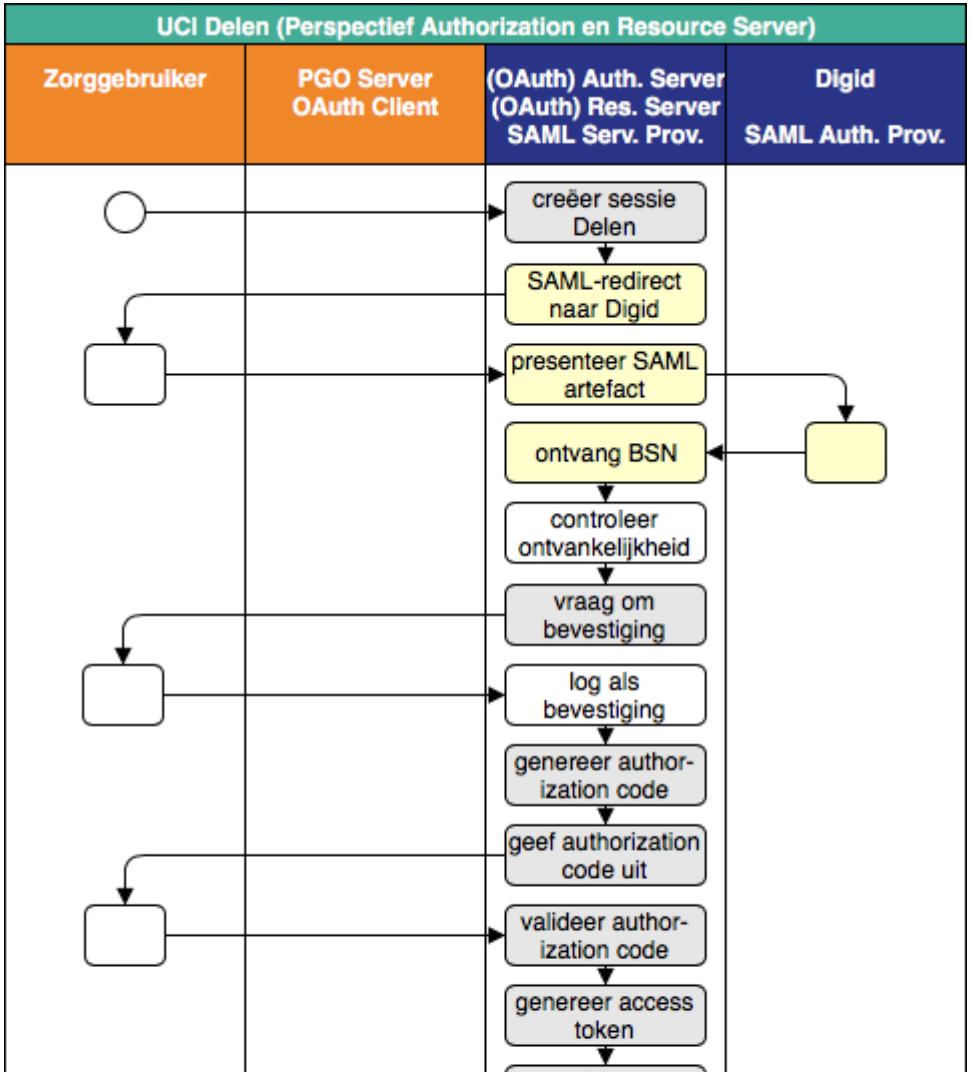
Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *PGO Server*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *PGO Server*, kortgesloten zijn. *Zorggebruiker* is "verborgen achter de browser" en *DigiD* "achter de *Authorization Server*".

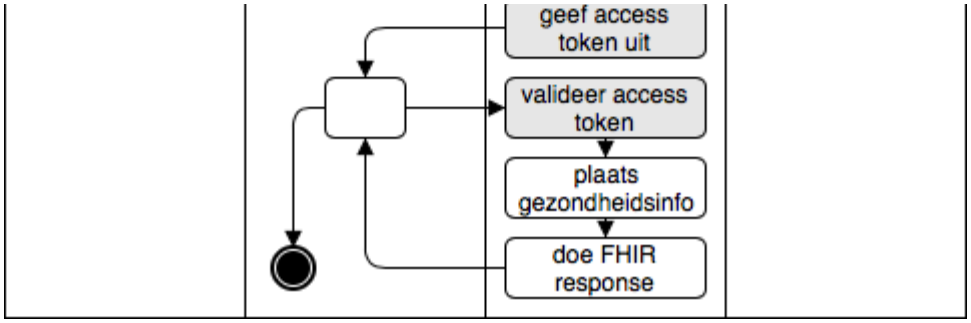


Perspectief Authorization Server/Resource Server (happy flow)

Toelichting

Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *Authorization/Resource Server*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *PGO Server*, kortgesloten zijn. *Zorggebruiker* is "verborgen achter de browser".

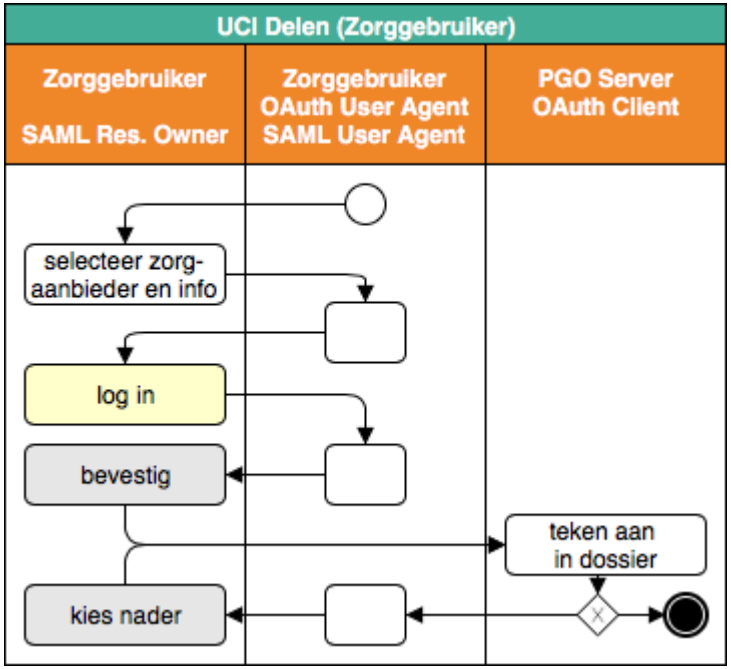

UCI Delen (Perspectief Authorization en Resource Server)
Zorggebruiker
PGO Server
OAuth Client
(OAuth) Auth. Server
(OAuth) Res. Server
SAML Serv. Prov.
Digid
SAML Auth. Prov.
creëer sessie Delen
SAML-redirect naar Digid
presenteer SAML artefact
ontvang BSN
controleer ontvankelijkheid
vraag om bevestiging
log als bevestiging
genereer author-ization code
geef authorization code uit
valideer author-ization code
genereer access token



Perspectief Zorggebruiker (happy flow)

Toelichting

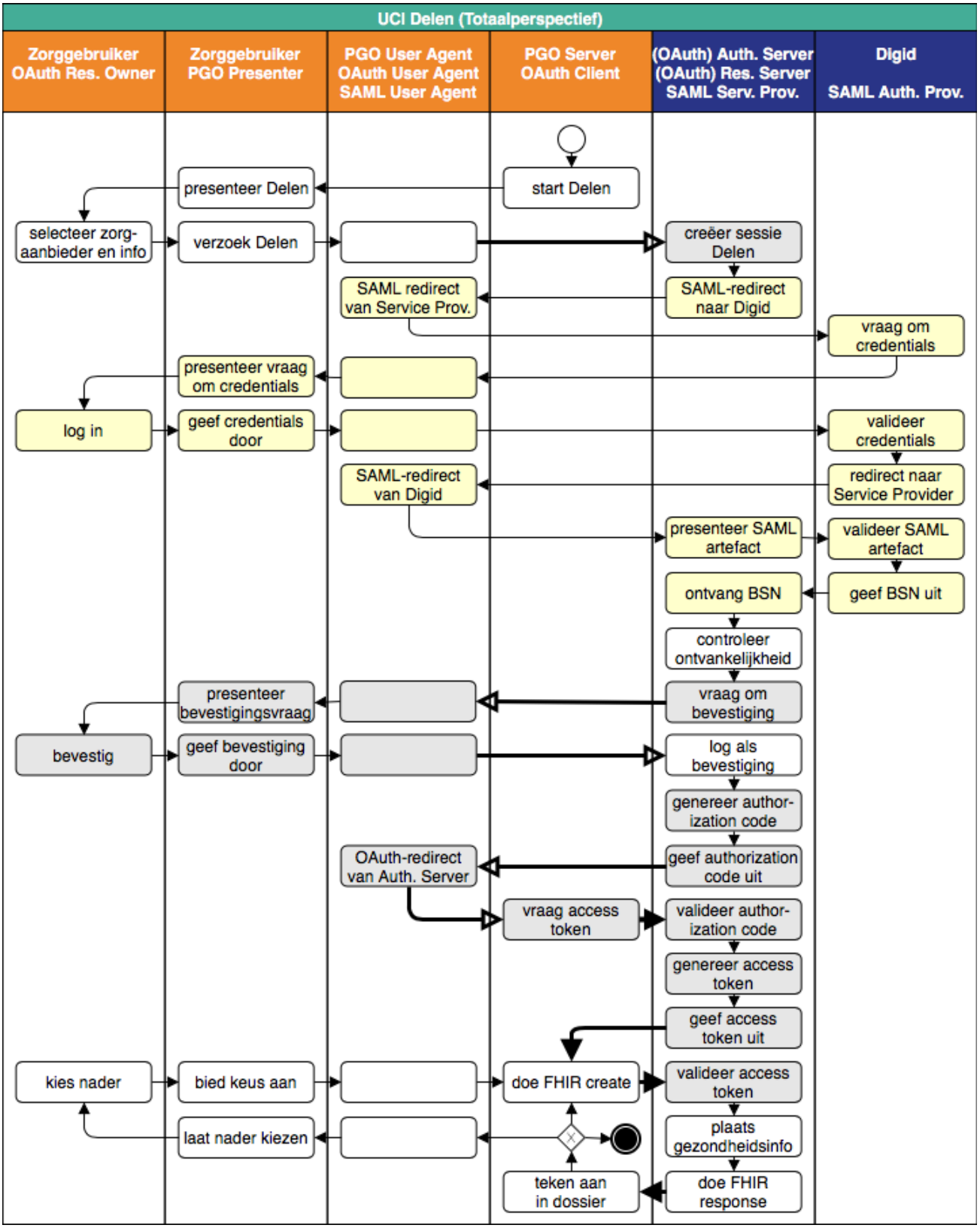
Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *Zorggebruiker*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *Zorggebruiker*, kortgesloten zijn. Vrijwel alles is "verborgen achter de browser". We hebben alleen de laatste stap van *PGO Server* zichtbaar gehouden, omdat het markeren van de gedeelde gezondheidsinformatie betekenis heeft voor de *Zorggebruiker*. Waarschijnlijk zal de *PGO Server* de *Zorggebruiker* laten weten dat het delen geslaagd is, maar dat is niet verplicht.


UCI Delen (Zorggebruiker)
Zorggebruiker
SAML Res. Owner
Zorggebruiker
OAuth User Agent
SAML User Agent
PGO Server
OAuth Client
selecteer zorg-
aanbieder en info
log in
bevestig
teken aan
in dossier
kies nader

Frontchannel en backchannel

Toelichting

In onderstaand stroomschema van UCI Delen 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.

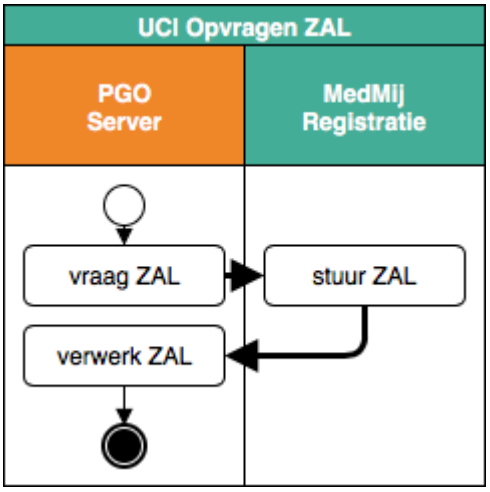

UCI Delen (Totaalperspectief)
Zorggebruiker OAuth Res. Owner
Zorggebruiker PGO Presenter
PGO User Agent OAuth User Agent SAML User Agent
PGO Server OAuth Client
(OAuth) Auth. Server (OAuth) Res. Server SAML Serv. Prov.
Digid SAML Auth. Prov.
start Delen
presenteer Delen
selecteer zorg-aanbieder en info
verzoek Delen
creëer sessie Delen
SAML-redirect naar Digid
SAML redirect van Service Prov.
vraag om credentials
presenteer vraag om credentials
log in
geef credentials door
valideer credentials
redirect naar Service Provider
SAML-redirect van Digid
presenteer SAML artefact
valideer SAML artefact
ontvang BSN
geef BSN uit
controleer ontvankelijkheid
presenteer bevestigingsvraag
vraag om bevestiging
bevestig
geef bevestiging door
log als bevestiging
genereer author-ization code
OAuth-redirect van Auth. Server
geef authorization code uit
vraag access token
valideer author-ization code
genereer access token
geef access token uit
kies nader
bied keus aan
doe FHIR create
valideer access token
laat nader kiezen
plaats gezondheidsinfo
teken aan in dossier
doe FHIR response

UCI Opvragen ZAL

Stroomdiagram

Toelichting

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

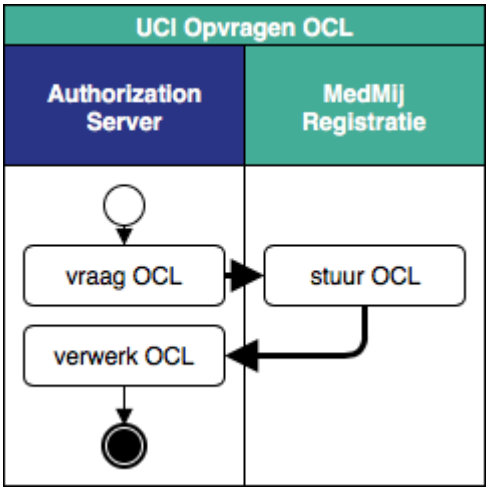


UCI Opvragen OCL

Stroomdiagram

Toelichting

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

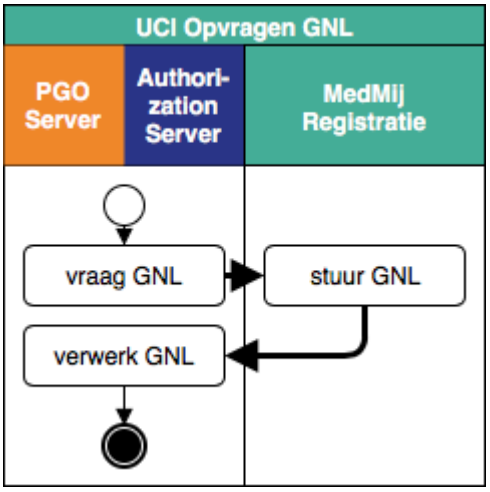


UCI Opvragen GNL

Stroomdiagram

Toelichting

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



Gegevens en performance in UCI Verzamelen en UCI Delen

Toelichting

De UCI Verzamelen en UCI Delen zijn analoog van opzet. Voor de gegevens die omgaan in beide use case-implementaties betekent dat, dat zij grotendeels identiek zijn. Anticiperend op een even analoge evolutie in toekomstige releases van het MedMij afsprakenstelsel, zijn de verantwoordelijkheden over de gegevens en performance in beide use case-implementaties daarom in deze pagina bij elkaar geplaatst.

Toestemmingsverklaring en bevestigingsverklaring

1a. De vraag die aan de *Zorggebruiker* gesteld moet worden in de stap "autoriseer" in UCI Verzamelen staat gespecificeerd op de pagina Toestemmingsverklaring. Daarbij geldt dat:

- de gebruikersvriendelijke weergave van de identiteit van de *Zorgaanbieder* (`NaamZorgaanbieder`) wordt bepaald door de betreffende *Dienstverlener Zorgaanbieder*, in haar dienstverleningsrelatie met de betreffende *Zorgaanbieder*;
- 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 *Gegevensdienstnaam* die bij de betreffende *Gegevensdienst* in de *Gegevensdienstnamenlijst* is opgenomen;
- de gebruikersvriendelijke weergave van de identiteit van de *Uitgever* (`NaamLeverancierPGO`) wordt betrokken uit de *OAuth Client List*, op basis van de `redirect_uri` (van OAuth) die in stap 1 is verkregen.

1b. De vraag die aan de *Zorggebruiker* gesteld moet worden in de stap "bevestig" in UCI Delen staat gespecificeerd op de pagina Bevestigingsverklaring. Daarbij geldt dat:

- de gebruikersvriendelijke weergave van de identiteit van de *Zorgaanbieder* (`NaamZorgaanbieder`) wordt bepaald door de betreffende *Dienstverlener Zorgaanbieder*, in haar dienstverleningsrelatie met de betreffende *Zorgaanbieder*;
- 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 *Gegevensdienstnaam* die bij de betreffende *Gegevensdienst* in de *Gegevensdienstnamenlijst* is opgenomen;
- de gebruikersvriendelijke weergave van de identiteit van de *Uitgever* (`NaamLeverancierPGO`) wordt betrokken uit de *OAuth Client List*, op basis van de `redirect_uri` (van OAuth) die in stap 1 is verkregen.

Toelichting

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

Adressering en parameters

Toelichting

Op vier momenten in de flow van UCI Verzamelen, en die van UCI Delen, adresseren OAuth-rollen elkaar, op basis van een URI. Onderstaande tabel geeft een overzicht van die vier momenten. De adresbepaler is de OAuth-rol die de URI bepaalt (hier altijd de *OAuth Client*), de gebruiker de OAuth-rol die het bepaalde adres toepast. Wanneer de adresgebruiker de *OAuth User Agent* is, is de gebruiker dus niet de bepaler en verloopt het betreffende verkeer via de zogenoemde front-channel. In de andere twee gevallen is de *OAuth Client* bepaler en gebruiker en verloopt het verkeer via de zogenoemde back-channel.

gebruiksmoment	adresbepaler	adresgebruiker	geadresseerde	parameters
authorization request (stap 1)	*OAuth Client* (stap 1)	*OAuth User Agent*	*Authorization Endpoint* van de *OAuth Authorization Server*	• `response_type` • `client_id` • `redirect_uri` • `scope` • `state`
OAuth redirect (stap 10)	*OAuth Client* (stap 1)	*OAuth User Agent*	*OAuth Client*	
access token request (stap 12)	*OAuth Client* (stap 12)	*OAuth Client*	*Token Endpoint* van de *OAuth Authorization Server*	• `grant_type` • `code` • **geen** client_id • `redirect_uri`
FHIR request (stap 14)	*OAuth Client* (stap 14)	*OAuth Client*	*Resource Endpoint* van de *OAuth Resource Server*	

In de nu volgende 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, maar inzake poortnummers maken de verantwoordelijkheden een onderscheid tussen front- en back-channel.

2. De *OAuth Client* stelt conform RFC 3986 de URI samen waarmee hij zichzelf, de *OAuth Authorization Server* of de *OAuth Resource Server* adresseert, volgens het patroon `scheme://host[:port] 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 `/`.

> **Toelichting**
>
> 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, RFC 1123 en het feit dat de hostname een zogeheten fully-qualified domain name is. Het laatste segment is het zogeheten top-level domain.

3. Ingeval de adresgebruiker *OAuth User Agent* is,

- is het gebruik van het voor `https` bedoelde poortnummer verplicht dat is opgenomen in de Service Name and Transport Protocol Port Number Registry van IANA;
- en, ingeval de geadresseerde het *Authorization Endpoint* van de *OAuth Authorization Server* is, betrekt de *OAuth Client* (als adres-bepaler) de URI, inclusief `host` en `path`, uit de *Zorgaanbiederslijst* , op basis van de van toepassing zijnde *Zorgaanbieder* en *Gegevensdienst.*

4. Ingeval de adresgebruiker de *OAuth Client* is, betrekt de *OAuth Client* (als adres-bepaler) de URI, inclusief `host`, `path` en eventueel `port`, uit de *Zorgaanbiederslijst*, op basis van de van toepassing zijnde *Zorgaanbieder* en hetzij *Gegevensdienst* (wanneer geadresseerde *OAuth Authorization Server* is) of *Systeemrol* (wanneer geadresseerde *OAuth Resource Server* is).

> **Toelichting**
>
> Andere elementen van de algemene URI-syntax, zoals `user`, `password`, `query` en `fragment`, zijn afwezig in de adressen. Met de eis dat `host` noch `path` op een `/` mag eindigen, wordt mogelijk gemaakt dat de URI, vooral in het vierde van de genoemde momenten, wordt aangevuld met informatiestandaard-specifieke URL-eindstukken, zonder dat de grens met het generieke MedMij-beginstuk onherkenbaar wordt.

5. Voor één *OAuth Authorization Server* zijn de hostnames in de adressen voor zijn *Authorization Endpoint* en zijn *Token Endpoint* identiek.

> **Toelichting**
>
> Deze verantwoordelijkheid is opgenomen met het oog op de afbeelding, op de Netwerk-laag, van één *Authorization Server* op één *ZA Node*. Het *Resource Endpoint* mag wel met een andere hostname geadresseerd worden, omdat de *Resource Server* een andere rol is.

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

parameter	vulling	toelichting
`response_type`	letterlijke waarde `code`	Dit is het gevolg van verantwoordelijkheid 6 op de Applicatielaag.
`client_id`	dezelfde hostname van de *OAuth Client* die ook in de *OAuth Clientlist* is opgenomen	

`redirect_uri`	zodanig dat de erin opgenomen hostname gelijk is aan de `client_id` en er geen poortnummer is opgenomen	Zie verantwoordelijkheid 3 hierboven.
`scope`	verplicht en enkelvoudig, met het *GegevensdienstId* van de betreffende *Gegevensdienst* uit de *Gegevensdienstnamen*	
`state`	conform sectie 4.1.1. van RFC 6749	Hiermee geeft de *OAuth Client* informatie mee aan de *OAuth Authorization Server*, waaraan eerstgenoemde later, bij de redirect, kan afleiden bij welk verzoek de authorization code hoort. Deze informatie is verder betekenisloos voor de *OAuth Authorization Server.*

7. De parameters in de access token request worden als volgt gevuld:

parameter	vulling	toelichting
`grant_type`	letterlijke waarde `authorization_code`	Dit is het gevolg van verantwoordelijkheid 6 op de Applicatielaag.
`code`	conform verantwoordelijkheid 11 op de Applicatielaag	Zie de toelichting bij verantwoordelijkheid 11 op de Applicatielaag.
`client_id`	**niet gebruikt**	Deze is niet nodig, want door verantwoordelijkheid 13 op de Applicatielaag wordt geborgd dat het access token alleen wordt verstrekt aan de *OAuth Client* aan wie de *OAuth Resource Owner* toestemming heeft verleend.
`redirect_uri`	dezelfde waarde als in de voorafgaande authorization request	

Performance

7. Na ontvangst van een access token request, in *UCI Verzamelen* of *UCI Delen*, zal de *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 *PGO Server*. Dit gedrag van de *Authorization Server* is gedurende minimaal 99,5% van de tijd beschikbaar.

8. Na ontvangst van een FHIR request, in *UCI Verzamelen* of *UCI Delen*, zal de *Resource Server*, indien in antwoord daarop een FHIR response dient te worden gedaan, na maximaal zestig (60) seconden dit FHIR response ter beschikking stellen aan de *PGO Server*. Dit gedrag van de *Resource Server* is gedurende minimaal 98,5% van de tijd beschikbaar.

Gegevens en performance inzake opvragen lijsten

Toelichting

Op enkele punten zijn er overeenkomsten tussen de verantwoordelijkheden inzake *UCI Opvragen ZAL*, *UCI Opvragen OCL* en *UCI Opvragen GNL* (Applicatie-laag) en *UCI Opvragen Whitelist* (Netwerk-laag). Deze verantwoordelijkheden zijn in deze pagina ondergebracht.

1. *MedMij Registratie* (in *UCI Opvragen ZAL*, *UCI Opvragen OCL* en *UCI Opvragen GNL*) en *MedMij Stelselnode* (*UCI Opvragen Whitelist*) worden geadresseerd met de hostname `PLACEHOLDER`. In:

- *UCI Opvragen ZAL* wordt *MedMij Registratie* geadresseerd op `PLACEHOLDER`;
- *UCI Opvragen OCL* wordt *MedMij Registratie* geadresseerd op `PLACEHOLDER`;
- *UCI Opvragen GNL* wordt *MedMij Registratie* geadresseerd op `PLACEHOLDER`;
- *UCI Opvragen Whitelist* wordt *MedMij Stelselnode* geadresseerd op `PLACEHOLDER`.

Toelichting

Dit zijn placeholders. *MedMij Registratie* en de *MedMij Stelselnode* is in deze versie van het MedMij Afsprakenstelsel nog niet live.

2. Het aandeel van *MedMij Registratie* in elk van de use case-implementaties *UCI Opvragen ZAL*, *UCI Opvragen OCL* en *UCI Opvragen GNL* en van *MedMij Stelselnode* in *UCI 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 (4800 minuten) verstrijken voordat het weer beschikbaar is.

3. *MedMij Beheer* brengt, in geval van zo'n incident, *Uitgevers*, *Bronnen* en *Lezers* op de hoogte van het optreden van het incident en van de verwachte down-time. *MedMij Beheer* brengt partijen op de hoogte van gepland onderhoud dat leidt tot tijdelijke onbeschikbaarheid.

XML-bestanden voor lijsten

Toelichting

De XML-bestanden waarmee MedMij Beheer de *Zorgaanbiederslijst*, de *Whitelist*, de *OAuth Client List* en de *Gegevensdienstnamenlijst* ontsluit voldoen aan enkele eisen, zodat PGO Server, Authorization Server en MedMijNode 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`.

2. Bij een wijziging in een lijst die tot hernieuwde publicatie leidt, wordt het volgnummer van de lijst met één opgehoogd.

Toelichting

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.

Toelichting

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.

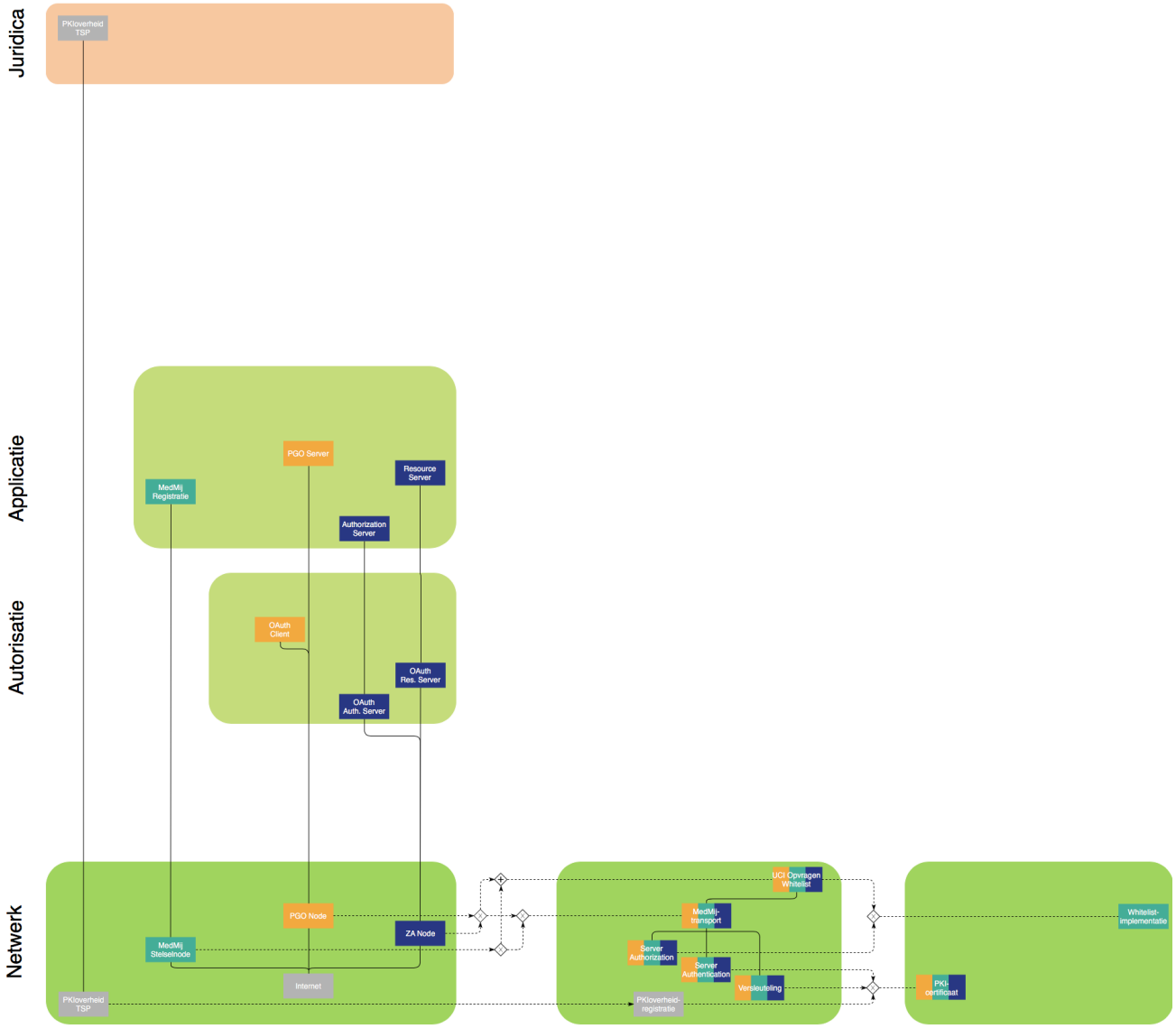
4. De in verantwoordelijkheid 1 bedoelde XML-bestanden:

- 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.

Toelichting

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.

Netwerk



Toelichting

Op deze laag worden de rollen (*Nodes*) op het MedMij-netwerk bepaald en voorzien van verantwoordelijkheden op het gebied van versleuteling, authenticatie van *Nodes* en autorisatie van *Nodes*. Met dat laatste wordt bedoeld dat er steeds opnieuw moet worden vastgesteld dat een Nodes gerechtigd is zich te bewegen op het MedMij-netwerk. Voor versleuteling en authenticatie worden PKI-certificaten gebruikt.

Autorisatie zou op grofweg twee manieren in het MedMij Afsprakenstelsel kunnen worden opgenomen:

- via diezelfde PKI-certificaten, waarin aan de domeinnaam van de houder van het certificaat gezien kan worden of het om een *MedMij Node* gaat, door daarvan te eisen dat die domeinnaam de vorm `<dienstverlener>.medmij.nl` heeft;
- via een door MedMij-zelf beheerde lijst van geautoriseerde *MedMij Nodes* (een whitelist).

De voordelen van de eerste optie zouden zijn dat:

- er zo maximaal gebruik wordt gemaakt van afspraken die ook voor andere doeleinden al nodig zijn, namelijk het gebruik van PKI-certificaten;
- zo de mate van operationele centrale betrokkenheid van de Stichting MedMij wordt geminimaliseerd, en dus de kosten en risico's daarvan. In de whitelist-optie zou Stichting MedMij zelf een lijst moeten gaan beheren en ontsluiten naar alle servers om het operationele verkeer mogelijk te maken. In de eerste optie is alleen een name service nodig voor de `medmij.nl`-domeinnamen. Dat laatste is een goed gestandaardiseerde, goed begrepen en goed uit te besteden service, die lagere kosten, lagere risico's en minder afhankelijkheid voor de deelnemers met zich mee zal brengen;
- MedMij zich zo maximaal houdt aan haar architectuurprincipe P6: MedMij spreekt alleen af wat nodig is.

Toch is voor de tweede optie gekozen, omdat de voor de eerste optie benodigde controle over de hostnames en de certificaten alleen met ongewenste bijeffecten gepaard zou gaan. De volgende opties zijn daarbij verkend:

- De MedMij-beheerorganisatie wordt **Registration Authority (RA)** in PKIoverheid, jegens alle betrokken Certificate Authorities (CA's). PKIoverheid kent echter die mogelijkheid niet.
- De MedMij-beheerorganisatie geeft een **domeinverklaring** af, zodat deelnemers zelf een subdomein onder .medmij.nl kunnen aanvragen bij een CA. Daarmee heeft de beheerorganisatie wel invloed op de uitgifte van een certificaat, maar laten intrekken is niet mogelijk, tenzij er sprake is van misbruik. Er is immers geen juridische relatie tussen de eigenaar van het domein (de beheerorganisatie) en de CA.
- Analoog aan de wijze waarop door sommigen beroepsgebonden certificaten worden uitgegeven, is een **maatwerk-certificeringsdienst** denkbaar. In de voorwaarden van het product (geldend vanaf de aanvraag van het certificaat) wordt dan expliciet geregeld dat wanneer de inschrijving in een extern register wegvalt, het certificaat door de CA wordt ingetrokken. Dat vereist dat de registerhouder (beheerorganisatie) wijzigingen doorgeeft aan alle CA's. Dit is economisch pas interessant bij een aanzienlijke hoeveelheid certificaathouders, waarvan in MedMij voorlopig geen sprake zal zijn.
- MedMij zou een **eigen PKI-omgeving** kunnen inrichten (afwijkend van PKIOverheid). Dit is niet verder verkend, vanwege de complexiteit en verantwoordelijkheid die op de schouders van de beheerorganisatie zou rusten.
- De Stichting MedMij zou zelf **houder** kunnen zijn van alle certificaten, waarbij deelnemers gemandateerd worden voor beheerstaken rond hun eigen subset van certificaten. De Stichting kan certificaten intrekken. Identificatie van de dienstverlener naar de gebruiker is niet mogelijk, want de certificaten staan op naam van Stichting MedMij.
- Er zou een **custom field** gebruikt kunnen worden in certificaten. De MedMij Beheerorganisatie zou de controle kunnen krijgen over de wijze waarop met dit veld wordt omgegaan. Dit vereist waarschijnlijk afspraken met alle CA's. Dit geeft controle op het uitgeven van certificaten, maar geeft de beheerorganisatie geen mogelijkheden het certificaat te laten intrekken.

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, met PKIoverheid-certificaat	altijd		
identificatie op basis van ...	`redirect_uri` of *Zorgaanbiederslijst*		PKIoverheid-certificaat
authenticatie, op basis van PKIoverheid-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	tijdens de TLS-handshake

Rollen

1. In het *MedMij-netwerk* functioneert:

- elke *PGO Server*, met inbegrip van zijn *OAuth*-rol, op één of meerdere *PGO Nodes*. Voor frontchannel-verkeer gebruikt elke *PGO Server* één *PGO Node*, en wel met een hostname die voor die *PGO Server* voorkomt op de *OAuth Clientlist*.
- elke *Authorization Server*, met inbegrip van zijn *OAuth*-rol, op één *ZA Node*;
- elke *Resource Server*, met inbegrip van zijn *OAuth*-rol, op één *ZA Node*;
- precies één *MedMij Stelselnode*, waarop *MedMij Registratie* functioneert.

2. Op één:

- *PGO Node* functioneert één *PGO Server*;
- *ZA Node* kunnen meer dan één *Authorization Server* en/of meer dan één *Resource Server* functioneren.

3. Een of meerdere *PKIoverheid TSP*'s treden op als *PKIoverheid TSP*.

Toelichting

De getalsverhouding tussen *Servers* en *Nodes* is gespiegeld tussen het persoonsdomein (één-op-meer) en het zorgaanbiedersdomein (meer-op-één). Dat komt doordat er twee lijsten aan de orde zijn die in in tegengestelde richting een vertaling maken: de *OAuth Clientlist* vertaalt **van** hostnames, de *Zorgaanbiederslijst* juist **naar** hostnames. Om deze vertalingen te kunnen laten slagen moet er bij elke *PGO Node* één *PGO Server* horen, en (andersom) bij één *Authorization Server* of één *Resource Server* dus één *ZA Node*.

Het is dus mogelijk voor een *PGO Server* om verschillende certificaten te hanteren voor frontchannel- en backchannel-verkeer, zolang op de *OAuth Clientlist* maar de hostname in het certificaat voor frontchannelverkeer voorkomt die tevens voorkomt in de redirect URI inzake OAuth. Want laatstgenoemde wordt gebruikt door de Authorization Server ten behoeve van de toestemmingsvraag (in UCI Verzamelen) en de bevestigingsvraag (in UCI Delen).

Zie tevens verantwoordelijkheid 5 op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.

Er is precies één *MedMij Stelselnode* in het *MedMij-netwerk*. Zonder die *MedMij Stelselnode* is er geen *MedMij-netwerk*.

In lijn met keuzes op de Proces- en Informatielaag, treden in het zorgaanbiedersdomein alleen de *ZA Nodes* op in het *MedMij-netwerk*. Dat wil zeggen dat bijvoorbeeld achterliggende xIS'en niet over het *MedMij-netwerk* communiceren met de *ZA Node*. Dat verkeer is verborgen achter de *ZA Node*. Alle daarvoor benodigde routering wordt afgehandeld door de server-implementaties en speelt zich buiten het zicht van het MedMij Afsprakenstelsel af.

Verantwoordelijkheden

TLS en certificaten

1. Al het verkeer over het *MedMij-netwerk* is beveiligd met Transport Layer Security (TLS). Er wordt enkel gebruik gemaakt van TLS-versies en -algoritmen die door het NCSC zijn geclassificeerd als "goed".

2. Om zich te kunnen authenticeren en autoriseren op het *MedMij-netwerk*, waar en zoals het MedMij Afsprakenstelsel dat vereist, kunnen elke *PGO Node*, elke *ZA Node* en de *MedMij Stelselnode*, in het kader van het TLS-verkeer zoals bedoeld in verantwoordelijkheid 1, een PKIoverheid-certificaat overleggen, en wel een server-certificaat van een *PKIoverheid TSP*.

3. Alle certificaathouders verbinden zich aan de op hen toepasselijke eisen van het PKIoverheid-stelsel. Een organisatie mag meerdere certificaten hebben.

Toelichting

Het MedMij Afsprakenstelsel bouwt 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 van PKIoverheid.

Functie *Versleuteling*

4. Op het *MedMij-netwerk* wordt al het verkeer versleuteld volgens TLS, zoals bedoeld in verantwoordelijkheid 1.

Functie *Server Authentication*

5. Tijdens de handshake van TLS, zoals bedoeld in verantwoordelijkheid 1, 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.

Toelichting

Bij backchannel-verkeer vindt dus twee-wegauthenticatie plaats, bij frontchannel-verkeer een-wegauthenticatie.

6. *ZA Node, PGO Node en MedMij Stelselnode* valideren tijdens de TLS-handshake aan het begin van een TLS-sessie of het een PKIoverheid-certificaat is en controleren, bij de *Certification Authority,* op basis van OCSP, of het ontvangen certificaat geldig is. In geval van het falen van één van deze controles, of het uitblijven van een controleresultaat, wordt het certificaat niet geaccepteerd en de TLS-sessie niet gestart.

Functie *Server Authorization*

Verspreiding van de *Whitelist*

7. De *MedMij Stelselnode* biedt aan *PGO Node* en *ZA Node* een use case-implementatie (*UCI Opvragen Whitelist*) om de actuele versie van die *Whitelist* op te vragen. Betrokken rollen gebruiken hiervoor het betreffende stroomdiagram.

8. Het aandeel van de *MedMij Stelselnode* in *UCI 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 use case, maximaal acht uren (4800 minuten) verstrijken voordat het weer beschikbaar is.

9. *PGO Nodes* en *ZA Nodes* betrekken minstens elke vijftien minuten (900 seconden) de meest recente *Whitelist* van *MedMij Stelselnode*.

10. De *MedMij Stelselnode* heeft de hostname PLACEHOLDER. De *MedMij Stelselnode* staat niet op de *Whitelist*, maar wordt er voor de controle tegen de *Whitelist* wel geacht op te staan.

> **Toelichting**
>
> Door op deze manier de *MedMij Stelselnode* te autoriseren voor MedMij-verkeer wordt ervoor gezorgd dat ook in foutsituaties of bootstrap-situaties een *PGO Node* of *ZA Node* de *MedMij Stelselnode* kan aanspreken om een *Whitelist* op te halen.

11. *PGO Nodes en ZA Nodes* valideren elke nieuw verkregen *Whitelist* tegen het XML-schema van de Whitelist. Dit XML-schema is een technische implementatie van het MedMij-metamodel.

12. Ten behoeve van de technische beveiliging van het gegevensverkeer dat zich voltrekt in het kader van *UCI Opvragen Whitelist* maakt deze gebruik van *Versleuteling*, *Server Authentication* en *Server Authorization* , volgens het bepaalde op deze Netwerk-laag.

Gebruik van de whitelist

13. *ZA Node, PGO Node en MedMij Stelselnode* 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.

> **Toelichting**
>
> In geval van frontchannel-verkeer vindt er geen Server Authorization plaats.

14. De *Node* die

- de TLS-client zou worden voert de in verantwoordelijkheid 13 bedoelde controle tegen de *Whitelist* uit voorafgaand aan de start van de TLS-handshake. Indien die controle niet kan worden uitgevoerd, of een negatief resultaat oplevert, wordt de TLS-handshake niet gestart.
- de TLS-server is, voert de in verantwoordelijkheid 13 bedoelde controle tegen de *Whitelist* uit tijdens de TLS-handshake, en wel onmiddellijk voorafgaand aan de voorziene verzending van de `Finished message`. Indien die controle niet kan worden uitgevoerd, of een negatief resultaat oplevert, wordt in plaats van de `Finished message` de uitzondering `access_denied` verzonden. In dit geval slaagt de controle tegen de *Whitelist* dan en slechts dan als op de *Whitelist* tenminste een van de volgende namen uit het de door de TLS-client aangeboden certificaat voorkomen: de `Common Name` of een van de eventuele `Subject Alternative Names`.

Toelichting

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 de TLS-handshake, aan de hand van het certificaat dat hij, conform verantwoordelijkheid 1b, 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.

Wanneer de *Whitelist* wordt geraadpleegd gedurende de TLS-handshake, vraagt dat in de implementatie van de TLS-handshake mogelijk een extra stap ten opzichte van sommige standaard-implementaties. Daarom zijn alternatieven overwogen voor de *Whitelist*-controle in geval van inkomend verkeer. Eén alternatief is om de *Whitelist*-controle te laten plaatsvinden na afloop van een (succesvolle) TLS-handshake, maar dat introduceert een beveiligingsrisico, omdat na een succesvolle TLS-handshake ook al inhoudelijk gegevensverkeer kan plaatsvinden, mogelijk dus on-geautoriseerd. Bovendien zou deze variant een MedMij-specifiek autorisatieprotocol introduceren, terwijl de internationale en open TLS-standaard, door middel van de foutmelding `access_denied`, deze functionaliteit al biedt. Een andere overweging zou nog zijn de *Whitelist*-controle te verplaatsen naar de Applicatie-laag, maar dat zou weinig mogelijkheden bieden tot hergebruik en tot extra complexiteit leiden in zowel implementatie als onderhoud van het MedMij Afsprakenstelsel.

De foutmelding `access_denied` wordt besproken in sectie 7.2.2 van de TLS-specificatie.

15. Indien een *Whitelist*-controle, in het kader van verantwoordelijkheid 14, niet kan worden uitgevoerd, of een negatief resultaat oplevert, breekt dit de voortgang af van de uitvoering van de use case-implementatie en wordt deze uitzondering behandeld als ware het de eerstvolgende inhoudelijke uitzondering conform de tabellen met uitzonderingen op UCI Verzamelen, respectievelijk UCI Delen, met dien verstande dat de betrokken Applicatie-rollen elkaar hiervan niet op de hoogte stellen.

Toelichting

Zo krijgt een uitzondering op Netwerk-niveau ook betekenis op Applicatie-niveau. Omdat het niet slagen van de *Whitelist*-controle duidt op een niet te vertrouwen tegenpartij, wordt deze daarvan niet op de hoogte gesteld.

Domain Name System

16. Elke *Dienstverlener Persoon*, elke *Dienstverlener Zorgaanbieder* en *MedMij Beheer* dragen ervoor zorg, in zijn rol als DNS Server, of cliënt daarvan, in het publieke Domain Name System, inzake de hostnames van de *MedMij Nodes*, respectievelijk *MedMij Stelselnode*, waarvoor hij verantwoordelijk is, dat de name records behorende bij die hostname zijn ondertekend volgens DNSSEC.

17. De *MedMij Stelselnode* en elke *MedMij 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.

Toelichting

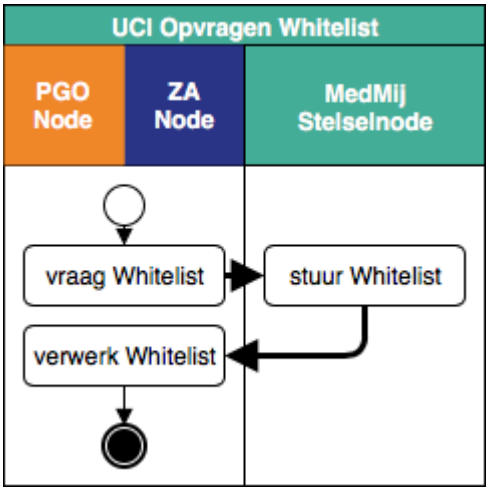
Het gebruik van DNSSEC (RFC 4033, RFC 4034, RFC 4035) vermindert de kwetsbaarheid van het Domain Name System voor bijvoorbeeld DNS spoofing.

UCI Opvragen Whitelist

Stroomdiagram

Toelichting

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



Metamodel

Toelichting

Het metamodel ordent kernbegrippen uit het MedMij Afsprakenstelsel. Het is een logisch gegevensmodel, in de vorm van een UML-klassediagram. Het metamodel is primair gericht op het samenhangend beschrijven van begrippen en relaties die worden gebruikt in een aantal registers, catalogi en lijsten. Vier daarvan worden door MedMij Beheer gepubliceerd voor operationeel gebruik door Dienstverleners:

- de *Zorgaanbiederslijst*, waarmee de *OAuth Client* de 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*, waarmee de de *OAuth Authorization Server* een gebruikersvriendelijke naam van de *OAuth Client* kan vinden om te gebruiken in de toestemmingsverklaring danwel de bevestigingsverklaring;
- de *Gegevensdienstnamenlijst*, waaraan de *OAuth Client* kan zien welke *Gegevensdienstnamen* de *Gegevensdiensten* hebben die op enig moment beschikbaar zijn op het MedMij-netwerk.

Twee andere zijn niet voor operationeel gebruik door de *Dienstverleners*, namelijk:

- het *Deelnemersregister*;
- het *Register van Informatiestandaarden*.

Het metamodel is in een bepaalde stijl opgezet. Er wordt vooral gebruik gemaakt van associatieklassen. Het voordeel daarvan is dat op deze manier het logische metamodel zo aanpasbaar en uitbreidbaar mogelijk blijft. Veel voorkomende constructies, zoals attributen, associatie en specialisatie zijn allemaal implementaties van associatieklassen. Implementatie willen we echter aan 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. De bestaansafhankelijkheid op klasse-niveau is kwalitatief.

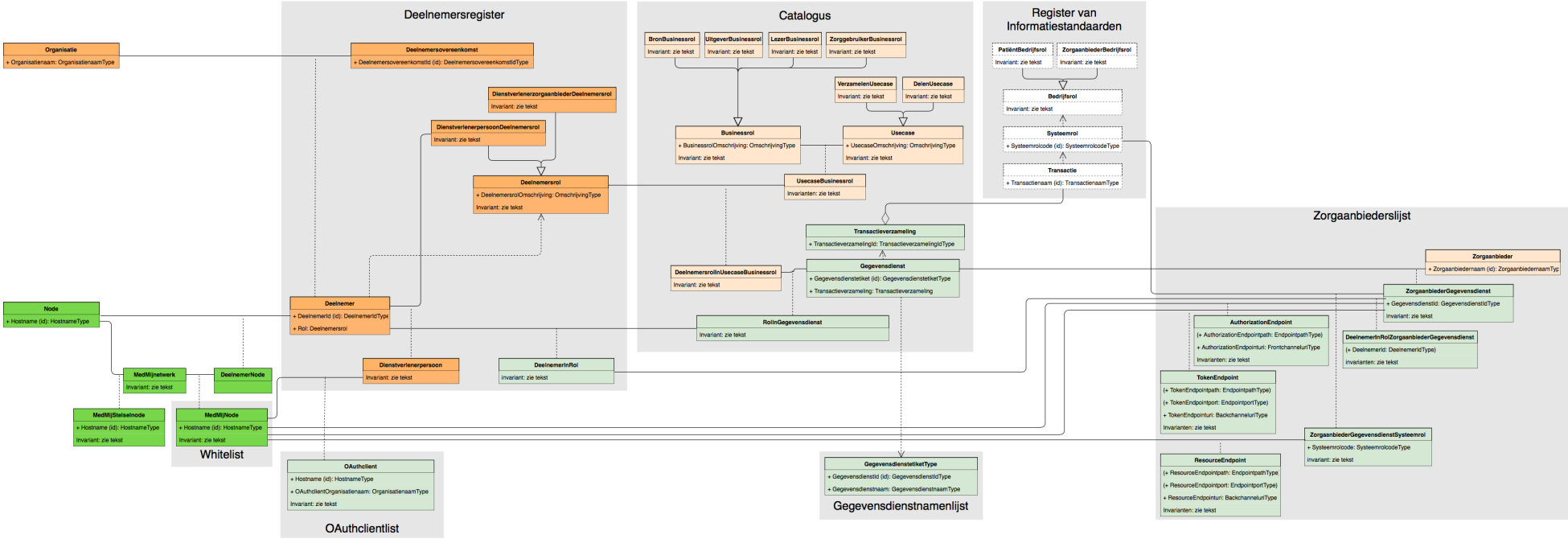
Op enkele punten is afgeweken van deze modelleerstijl, door gebruik van:

- de uses-relatie;
- de containment-relatie;
- de objectgeoriënteerde specialisatie, namelijk waar we een opsommende definitie geven van *Businessrol*, *Usecase* en *Bedrijfsrol*;
- attributen, voor identificatie, omschrijving of vererving (zie onder).

In alle gevallen zouden ook associatieklassen gebruikt kunnen worden, maar zou dat de presentatie van het model onnodig compliceren.

De namen van de klassen, de typen 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 *Gegevensdienstnamenlijst* staat kortweg als een uitsnede getekend uit de verzamelde *Gegevensdiensten* in de *Catalogus*. Hiermee wil het *Metamodel* aangeven dat de *Gegevensdienstnamenlijst* dezelfde populatie kent als de *Gegevensdiensten* in de *Catalogus*, maar daarvan steeds slechts twee van de drie attributen bevat.



Toelichting

In het *Deelnemersregister* houdt de MedMij-beheerorganisatie 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. 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 (*OAuthclientOrganisatienaam*), om gebruikt te worden in de toestemmingsverklaring.

De *Catalogus* is het portfolio van *Businessrollen, Usecases* en *Gegevensdiensten* die in deze release van het MedMij Afsprakenstelsel voorhanden zijn en beschrijft daarnaast:

- de wijze waarop de *Businessrollen* in de *Usecases* betrokken zijn en welke van die combinaties door welke *Deelnemersrollen* gespeeld kunnen worden;
- welke van die combinaties samen kunnen voorkomen met welke *Gegevensdiensten*;
- welke verzamelingen van *Transacties* (uit het Register van Informatiestandaarden) horen bij een *Gegevensdienst*.

Zo biedt de *Catalogus* aan het *Deelnemersregister* ook de klasse (*RolInGegevensdienst*) waarmee laatstgenoemde kan bijhouden welke *Deelnemers* welke *RolInGegevensdienst* aanbieden. Waar zij dat doen, ontstaat een *DeelnemerInRol*.

De klassen in het *Register van Informatiestandaarden*, inclusief hun namen, moeten begrepen worden in de zin waarin Nictiz ze gebruikt in het kader van de Informatiestandaarden die voor gebruik binnen MedMij zijn toegelaten. Daarom zijn de randen van deze klassen gestippeld. Een *Bedrijfsrol*, waarvan er twee zijn (*PatiëntBedrijfsrol* en *ZorgaanbiederBedrijfsrol*), wordt aangenomen door een *Systeemrol*, die op haar beurt gebruikt wordt door een *Transactie*. Bij elke *Transactie* hoort een *Informatiestandaard. Transacties* worden gegroepeerd in *Transactieverzamelingen* die een *Gegevensdienst* vormen. Een actueel voorbeeld van een *Transactieverzameling* is de *Transactie* die een overzicht van beschikbare PDF-documenten ophaalt in combinatie met een *Transactie* die een PDF-document uit dat overzicht ophaalt. *Gegevensdiensten* worden als geheel aan Zorggebruikers aangeboden en die gebruikers zullen deze ook ineens autoriseren.

Helemaal rechts in het model wordt het verband gelegd met de *Zorgaanbieder*, in de door MedMij Beheer beheerde en ontsloten *Zorgaanbiederslijst*. Wanneer een *Zorgaanbieder* een zekere *Gegevensdienst* aanbiedt, hoort daarbij een *ZorgaanbiederGegevensdienst*. Deze klasse kan worden gebruikt om *Zorggebruikers* te informeren over wie van de *Zorgaanbieders* welke *Gegevensdiensten* aanbieden. Binnen een *Gegevensdienst* zijn bovendien één of meerdere *Systeemrollen* aan de orde. Deze relatie is vervat in de klasse *ZorgaanbiederGegevensdienstSysteemrol*.

Bij een *ZorgaanbiederGegevensdienst* hoort één *AuthorizationEndpoint* en één *TokenEndpoint*, en bij een *ZorgaanbiederGegevensdienstSysteemrol* één *ResourceEndpoint*. Bij alle drie soorten endpoints administreert de *Zorgaanbiederslijst* bovendien componenten van het technische adres (URI) waarmee zij geadresseerd worden, namelijk:

- het *Endpointpath*, dat wil zeggen, een eerste stuk van het path in de URI;

- de *Endpointport*, dat wil zeggen, het (optionele) poortnummer dat gebruikt wordt in het verkeer via de back-channel. Dit is niet aan de orde bij het *AuthorizationEndpoint*, omdat deze via het front-channel wordt aangesproken en daarvoor dus de standaard IANA-poort voor `https` verplicht is.

Deze onderdelen worden samen met de Hostname van de betreffende MedMijNode samengesteld tot een URI die geldt als het adres van het respectievelijke endpoint. De eisen aan al deze componenten en de wijzen van samenstellen tot de URI's staat beschreven op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.

In de *Zorgaanbiederslijst* administreert de beheerder ook welke *DeelnemerInRol* hoort bij een zekere *ZorgaanbiederGegevensdienst*. 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. Deze is slechts voor beheersdoeleinden bedoeld en wordt niet in de *Zorgaanbiederslijst* ontsloten naar *Uitgevers*.

Invarianten, dat wil zeggen, beperkingen die te allen tijden aan de orde zijn, staan onderaan in een separate tabel opgenomen. Enkele van die invarianten zijn slechts bedoeld om attributen te vererven van generiekere naar specifiekere klassen, zodat zij in het bereik van een zeker register of catalogus komen. De meeste zijn echter conceptueel, dat wil zeggen, onafhankelijk van de implementatie van registers en catalogi. Dit verschil staat in de tabel van invarianten aangegeven.

In de *Zorgaanbiederslijst* komen attributen voor die tussen haakjes zijn genoteerd. Daarmee wordt bedoeld dat zij weliswaar worden geadministreerd in de *Zorgaanbiederslijst*, maar niet worden ontsloten. Dat is niet nodig, omdat in de ontsloten variant de URI's al zijn samengesteld, zodat de *OAuth Client* dat niet meer hoeft te doen en daarmee ook geen fouten meer kan maken. De samenstelling van de URI's uit haar componenten is een verantwoordelijkheid van MedMij Beheer.

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. Alleen bij de Nictiz-klassen in het *Register van Informatiestandaarden* hebben we dit achterwege gelaten.

Uit dit metamodel wordt duidelijk hoe in het MedMij 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* en *Transacties* met *Systeemrollen* zoals opgenomen in de *Catalogus* en het *Register van Informatiestandaarden*;

- Elke *Zorgaanbieder* kent bij elke *Gegevensdienst* maximaal één *AuthorizationEndpoint* en maximaal één *TokenEndpoint* (namelijk als deze door één van zijn *Dienstverleners Zorgaanbieder* wordt aangeboden) en bij elke *Systeemrol* binnen een *Gegevensdienst*maximaal één *ResourceEndpoint*. De endpoints hebben elk een URI als technisch adres.

De *Authorization Server* herkent bij de authorization request (zie UCI Verzamelen en UCI Delen) de aangesproken *Zorgaanbieder* aan het *Authorization Endpoint*, zodat verschillende *Zorgaanbieders* niet hetzelfde *Authorization Endpoint* mogen hebben. Net zo herkent de *Resource Server* bij de resource request (zie UCI Verzamelen en UCI Delen) de aangesproken *Zorgaanbieder* aan het *Resource Endpoint*, zodat verschillende *Zorgaanbieders* niet hetzelfde *Resource Endpoint* mogen hebben. Bij het *Token Endpoint* hoeft een dergelijke eis niet gesteld te worden, omdat de *Authorization Server* bij het access token request (zie UCI Verzamelen en UCI Delen) geen specifieke *Zorgaanbieder* hoeft te herkennen.

Invarianten

Het klassediagram hierboven definieert de (bestaan)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. Daarop is, met het oog op informatiebeveiliging, één uitzondering: bij ontvangst van een *Zorgaanbiederslijst*, *Whitelist, OAuthclientlist* of *Gegevensdienstnamenlijst* wordt de ontvanger geacht deze te valideren jegens het toepasselijke XML-schema.

Betreft instanties van klasse ...	Invariant	Bedrijfsregel voor beheer van ...	Validatie door ontvanger lijst	Toelichting	Aard
AuthorizationEndpoint	Elke *AuthorizationEndpointuri* is samengesteld conform de adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen, uit: • *AuthorizationEndpoint.MedMijNode.Hostname* • *AuthorizationEndPoint. AuthorizationEndpointpath*	*Zorgaanbiederslijst*	XML-schema *Zorgaanbiederslijst* (syntax van de URI)	Zie de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.	lokale afhankelijkheid
AuthorizationEndpoint	Elke *AuthorizationEndpoint* hoort bij exact één *Zorgaanbieder*.	*Zorgaanbiederslijst*	n.v.t.	Zo kan de *OAuth Authorization Server* aan het	getalsverhouding

				Authorization-Endpoint de *Zorgaanbieder* herkennen.	
Bedrijfsrol	Elke *Bedrijfsrol* is hetzij *PatiëntBedrijfsrol* of *ZorgaanbiedersBedrijfsrol.*	*Register van Informatiestandaarden*	n.v.t.	Dit is een uitsluitende opsomming.	opsomming
BronBusinessrol	Er is precies één instantie hiervan.	*Deelnemersregister*	n.v.t.	Dit is een atoom van het model.	getalsverhouding
Businessrol	Elke *BusinessRol* is hetzij *BronRol*, hetzij *UitgeverRol*, hetzij *LezerRol*, hetzij *ZorggebruikerBusinessrol*.	*Catalogus*	n.v.t.	Dit is een uitsluitende opsomming.	opsomming
DeelnemerInRol	*DeelnemerInRol.Deelnemer.Deelnemersrol* en *DeelnemerInRol.RollnGegevensdienst. DeelnemersrolInUsecaseBusinessrol. Deelnemersrol* zijn identiek.	*Deelnemersregister*	n.v.t.	De betreffende *Deelnemer* kan zich alleen aanmelden voor rollen die hem door de *Catalogus* geboden worden.	niet-lokale afhankelijkheid
DeelnemerInRolZorgaanbiederGegevensdienst	*DeelnemerInRolZorgaanbiederGegevensdienst. ZorgaanbiederGegevensdienst.Gegevensdienst = DeelnemerInRolZorgaanbiederGegevensdienst. DeelnemerInRol.RollnGegevensdienst. Gegevensdienst*	*Zorgaanbiederslijst*	n.v.t.	Een *Deelnemer* kan alleen gezag doen gelden over de opname, in de *Zorgaanbiederslijst*, van een *Gegevensdienst* bij een *Zorgaanbieder*, als die *Deelnemer* ook voor die *Gegevensdienst* is toegelaten in MedMij.	niet-lokale afhankelijkheid
DeelnemerInRolZorgaanbiederGegevensdienst	*DeelnemerInRolZorgaanbiederGegevensdienst. DeelnemerId = DeelnemerInRolZorgaanbiederGegevensdienst. DeelnemerInRol. Deelnemer.DeelnemerId*	*Zorgaanbiederslijst*	n.v.t.	Zo weet de beheerder van de *Zorgaanbiederslijst* namens welke *Deelnemer* een *Zorgaanbiedergegevensdienst* mag worden gecreëerd, gewijzigd of verwijderd.	vererving
Deelnemerpersoon	Er bestaat hooguit één instantie hiervan bij één *Deelnemer*, en precies één als de *Deelnemersrol* van laatstgenoemde *DienstverlenerpersoonDeelnemersrol* is.	*Deelnemersregister*	n.v.t.	Een Deelnemer heet een *Dienstverlenerpersoon* dan en slechts dan als hij de toepasselijke rol speelt.	getalsverhouding
Deelnemersrol	Elke *Deelnemersrol* is hetzij *DienstverlenerpersoonDeelnemersrol*, hetzij *DienstverlenerzorgaanbiederDeelnemersrol*.	*Deelnemersregister*	n.v.t.	Dit is een uitsluitende opsomming.	opsomming

DeelnemersrolInUsecaseBusinessrol	Als (*DeelnemersrolinUsecaseBusinessrol.* *UsecaseBusinessrol.Businessrol =* *BronBusinessrol* en *DeelnemersrolinUsecaseBusinessrol.* *UsecaseBusinessrol.Usecase =* *VerzamelenUsecase*) dan *DeelnemersrolinUsecaseBusinessrol.* *Deelnemersrol =* *DienstverlenerzorgaanbiederBusinessrol*.	*Catalogus*	n.v.t.	De *Bron* (Processen-en Informatielaag) in *UC Verzamelen* wordt gespeeld door de *Dienstverlener Zorgaanbieder*.	rolbinding
DeelnemersrolInUsecaseBusinessrol	Als (*DeelnemersrolinUsecaseBusinessrol.* *UsecaseBusinessrol.Businessrol =* *UitgeverBusinessrol* en (*DeelnemersrolinUsecaseBusinessrol.* *UsecaseBusinessrol.Usecase =* *VerzamelenUsecase* of *DeelnemersrolinUsecaseBusinessrol.* *UsecaseBusinessrol.Usecase = DelenUsecase*)) dan *DeelnemersrolinUsecaseBusinessrol.* *Deelnemersrol =* *DienstverlenerpersoonBusinessrol*.	*Catalogus*	n.v.t.	De *Uitgever* (Processen- en Informatielaag) in zowel *UC Verzamelen* als *UC Delen* wordt gespeeld door de *Dienstverlener Persoon*.	rolbinding
DeelnemersrolInUsecaseBusinessrol	Als (*DeelnemersrolinUsecaseBusinessrol.* *UsecaseBusinessrol.Businessrol =* *LezerBusinessrol* en *DeelnemersrolinUsecaseBusinessrol.* *UsecaseBusinessrol.Usecase = DelenUsecase*) dan *DeelnemersrolinUsecaseBusinessrol.* *Deelnemersrol =* *DienstverlenerzorgaanbiederBusinessrol*.	*Catalogus*	n.v.t.	De *Lezer* (Processen-en Informatielaag) in *UC Delen* wordt gespeeld door de *Dienstverlener Zorgaanbieder*.	rolbinding
DelenUsecase	Er is precies één instantie hiervan.	*Catalogus*	n.v.t.	Dit is een atoom van het model.	getalsverhouding

DienstverlenerpersoonDeelnemersrol	Er is precies één instantie hiervan.	*Deelnemersregister*	n.v.t.	Dit is een atoom van het model.	getalsverhouding
DienstverlenerzorgaanbiederDeelnemersrol	Er is precies één instantie hiervan.	*Deelnemersregister*	n.v.t.	Dit is een atoom van het model.	getalsverhouding
Gegevensdienst	Er zijn nul of meer *Gegevensdiensten*.	*Catalogus*	XML-schema *Gegevensdienstnamenlijst*	De *Gegevensdienstnamenlijst* kan leeg zijn.	getalsverhouding
LezerBusinessrol	Er is precies één instantie hiervan.	*Catalogus*	n.v.t.	Dit is een atoom van het model.	getalsverhouding
MedMijnetwerk	Er is precies één instantie hiervan.	*Whitelist*	n.v.t.	Dit is een atoom van het model.	getalsverhouding
MedMijNode	*MedMijNode.Hostname = MedMijNode. DeelnemerNode.Node.Hostname*	*Whitelist*	n.v.t.	Zo erft de *MedMijNode* de *Hostname* van de *Node* die het is.	vererving
MedMijStelselNode	Er is precies één instantie hiervan.	*Whitelist*	n.v.t.	Zonder *MedMijStelselnode* geen *MedMijNetwerk* en geen *Whitelist*.	getalsverhouding
MedMijStelselNode	*MedMijStelselNode.Hostname = MedMijStelseNode.Node.Hostname*	*Whitelist*	n.v.t.	Zo erft de *MedMijStelselNode*, van de *Node* die het is, de *Hostname*.	vererving
OAuthclient	*OAuthclient.OAuthclientOrganisatienaam = OAuthclient. MedMijNode.DeelnemerNode. Deelnemer.Organisatie.Organisatienaam*	*OAuthclientlist*	n.v.t.	Zo erft de *OAuthclientlist* de (*OAuthclient)Organisatienamen* van de *Organisaties*.	vererving
OAuthclient	*OAuthclient.Hostname = OAuthclient. MedMijNode.Hostname*.	*OAuthclientlist*	n.v.t.	Zo erft de *OAuthclientlist* de *Hostnames* van de *Nodes*.	vererving
OAuthclientlist	Er is precies één instantie hiervan.	*OAuthclientlist*	n.v.t.	Dit is een atoom van het model.	getalsverhouding
OAuthclientlist	De *OAuthclientlist* bevat nul of meer *OAuthclients*.	*OAuthclientlist*	XML-schema *OAuthclientlist*	In de starttoestand is de *OAuthclientlist* leeg.	getalsverhouding
PatiëntBedrijfsrol	Er is precies één instantie hiervan.	*Register van Informatiestandaarden*	n.v.t.	Dit is een atoom van het model.	getalsverhouding
ResourceEndpoint		*Zorgaanbiederslijst*		Zie de pagina Gegevens en	lokale

	De *ResourceEndpointuri* is samengesteld conform de adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen, uit: • *ResourceEndpoint.MedMijNode.Hostname* • *ResourceEndpoint.ResourceEndpointport* • *ResourceEndPoint.ResourceEndpointpath*		XML-schema *Zorgaanbiederslijst* (syntax van de URI)	performance in UCI Verzamelen en UCI Delen.	afhankelijkheid
ResourceEndpoint	Elk *ResourceEndpoint* hoort bij precies één *Zorgaanbieder*.	*Zorgaanbiederslijst*	n.v.t.	Zo kan de *OAuth Resource Server* aan het *ResourceEndpoint* de *Zorgaanbieder* herkennen.	getalsverhouding
RolInGegevensdienst	Als *RolInGegevensdienst. DeelnemersrolinUsecaseBusinessrol. Deelnemersrol = DienstverlenerpersoonDeelnemersrol*, dan geldt voor alle *RolInGegevensdienst. Gegevensdienst.TransactieVerzameling. Transactie t: t.Systeemrol.Bedrijfsrol. PatiëntBedrijfsrol*.	*Catalogus*	n.v.t.	Dit koppelt de MedMij-rol *Dienstverlener Persoon* aan de Nictiz-rol *Patiënt*.	rolbinding
RolInGegevensdienst	Als *RolInGegevensdienst. DeelnemersrolinUsecaseBusinessrol. Deelnemersrol = DienstverlenerzorgaanbiederDeelnemersrol*, dan geldt voor alle *RolInGegevensdienst. Gegevensdienst.TransactieVerzameling. Transactie t: t.Systeemrol.Bedrijfsrol. ZorgaanbiederBedrijfsrol*.	*Catalogus*	n.v.t.	Dit koppelt de MedMij-rol *Dienstverlener Zorgaanbieder* aan de Nictiz-rol *Zorgaanbieder*.	rolbinding
TokenEndpoint	De *TokenEndpointuri* is samengesteld conform de adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen, uit: • *TokenEndpoint.MedMijNode.Hostname* • *TokenEndpoint.TokenEndpointport* • *TokenEndpoint.TokenEndpointpath*	*Zorgaanbiederslijst*	XML-schema *Zorgaanbiederslijst* (syntax van de URI)	Zie de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.	lokale afhankelijkheid
UitgeverBusinessrol	Er is precies één instantie hiervan.	*Catalogus*	n.v.t.	Dit is een atoom van het	getalsverhouding

				model.	
Usecase	Elke *UseCase* is hetzij *VerzamelenUsecase* of *DelenUsecase*.	*Catalogus*	n.v.t.	Dit is een uitsluitende opsomming. In deze release zijn er twee.	opsomming
UsecaseBusinessrol	Als *UseCaseBusinessrol.Usecase = VerzamelenUsecase* dan *UseCaseBusinessrol. Businessrol = BronBusinessrol* of *UseCaseBusinessrol.Businessrol = UitgeverBusinessrol* en Als *UseCaseBusinessrol.Usecase = DelenUsecase* dan *UseCaseBusinessrol. Businessrol = LezerBusinessrol* of *UseCaseBusinessrol.Businessrol = UitgeverBusinessrol*	*Catalogus*	n.v.t.	Dit is een uitsluitende opsomming (tabel) van de toegestane combinaties van *Businessrollen* en *Usecases*.	opsomming
VerzamelenUsecase	Er is precies één instantie hiervan.	*Catalogus*	n.v.t.	Dit is een atoom van het model.	getalsverhouding
Whitelist	Er is precies één instantie hiervan.	*Whitelist*	n.v.t.	Dit is een atoom van het model.	getalsverhouding
Whitelist	De *Whitelist* bevat nul of meer *MedMijNodes*.	*Whitelist*	XML-schema *Whitelist*	In de starttoestand staat op de *Whitelist* alleen de *MedMij Stelselnode* (zie aldaar), maar dat is geen *MedMijNode.*	getalsverhouding
ZorgaanbiedersBedrijfsrol	Er is precies één instantie hiervan.	*Register van Informatiestandaarden*	n.v.t.	Dit is een atoom van het model.	getalsverhouding
Zorgaanbieder	Elke *Zorgaanbieder* heeft minstens één *ZorgaanbiederGegevensdienst*	*Zorgaanbiederslijst*	n.v.t.	Anders is de opname van de *Zorgaanbieder* in de *Zorgaanbiederslijst* nutteloos.	getalsverhouding
Zorgaanbieder	Elke *Zorgaanbieder* heeft bij elke *Gegevensdienst* ten hoogste één *ZorgaanbiederGegevensdienst*.	*Zorgaanbiederslijst*	XML-schema *Zorgaanbiederslijst*	Zo kan de *OAuth Client* bij de combinatie van een *Zorgaanbieder* en een *Gegevensdienst* het *AuthorizationEndpoint* en	getalsverhouding

				TokenEndpoint vinden, in de *Zorgaanbiederslijst*.	
ZorgaanbiederGegevensdienst	Voor elke *ZorgaanbiederGegevensdienst. Gegevensdienst. TransactieVerzameling. Transactie.Systeemrol s* waarvoor geldt dat *s.Bedrijfsrol* = *ZorgaanbiederBedrijfsrol*, geldt dat er een *ZorgaanbiederGegevensdienstSysteemrol z* is zodat *z.Systeemrol* = s.	*Zorgaanbiederslijst*	n.v.t.	Als in de Catalogus een *Systeemrol* voor *Zorgaanbieders* hoort bij een namens een zekere *Zorgaanbieder* aangeboden *Gegevensdienst*, dan moet namens dezelfde *Zorgaanbieder* ook deze *Systeemrol* worden aangeboden.	niet-lokale afhankelijkheid
ZorgaanbiederGegevensdienst	Elke *ZorgaanbiederGegevensdienst* heeft precies één *AuthorizationEndpoint*.	*Zorgaanbiederslijst*	XML-schema *Zorgaanbiederslijst*	Zo kan de *OAuth Client* bij de combinatie van een *Zorgaanbieder* en een *Gegevensdienst* het *AuthorizationEndpoint* vinden, in de *Zorgaanbiederslijst*.	getalsverhouding
ZorgaanbiederGegevensdienst	Elke *ZorgaanbiederGegevensdienst* heeft precies één *TokenEndpoint*.	*Zorgaanbiederslijst*	XML-schema *Zorgaanbiederslijst*	Zo kan de *OAuth Client* bij de combinatie van een *Zorgaanbieder* en een *Gegevensdienst* het *TokenEndpoint* vinden, in de *Zorgaanbiederslijst*.	getalsverhouding
ZorgaanbiederGegevensdienst	*ZorgaanbiederGegevensdienst. GegevensdienstId* = *ZorgaanbiederGegevensdienst.Gegevensdienst .GegevensdienstId*	*Zorgaanbiederslijst*	n.v.t.	Zo erft de *Zorgaanbiederslijst* de *GegevensdienstId*'s van de *Catalogus*.	vererving
ZorgaanbiederGegevensdienst	Elke *ZorgaanbiederGegevensdienst* heeft precies één *DeelnemerInRolZorgaanbiederGegevensdienst*.	*Zorgaanbiederslijst*	n.v.t.	Zo is duidelijk welke *DeelnemerInRol* zorgt voor een *ZorgaanbiederGegevensdienst* .	getalsverhouding
ZorgaanbiederGegevensdienstSysteemrol	Elke combinatie van een *Zorgaanbieder Gegevensdienst* en een *Systeemrol* heeft ten hoogste één *ZorgaanbiederGegevensdienstSysteemrol*.	*Zorgaanbiederslijst*	XML-schema *Zorgaanbiederslijst*	Zo kan de *OAuth Client* bij de combinatie van een *Zorgaanbieder,* een *Gegevensdienst* en een Systeemrol het	getalsverhouding

				ResourceEndpoint vinden, in de *Zorgaanbiederslijst*.	
ZorgaanbiederGegevensdienstSysteemrol	*ZorgaanbiederGegevensdienstSysteemrol. Systeemrol.Bedrijfsrol = ZorgaanbiederBedrijfsrol*	*Zorgaanbiederslijst*	n.v.t.	*Zorgaanbieders* kunnen alleen *Systeemrollen* aanbieden die voor *Zorgaanbieders* bedoeld zijn.	niet-lokale afhankelijkheid
ZorgaanbiederGegevensdienstSysteemrol	Elke *ZorgaanbiederGegevensdienstSysteemrol* heeft precies één *ResourceEndpoint*.	*Zorgaanbiederslijst*	XML-schema *Zorgaanbiederslijst*	Zo kan de *OAuth Client* bij de combinatie van een *Zorgaanbieder,* een *Gegevensdienst* en een Systeemrol het *ResourceEndpoint* vinden, in de *Zorgaanbiederslijst*.	getalsverhouding
ZorgaanbiederGegevensdienstSysteemrol	*ZorgaanbiederGegevensdienstSysteemrol. Systeemrolcode = ZorgaanbiederGegevensdienstSysteemrol. Systeemrol.Systeemrolcode*	*Zorgaanbiederslijst*	n.v.t.	Zo erft de *Zorgaanbiederslijst* de *Systeemrolcodes* van het *Register van Informatiestandaarden*.	vererving
Zorgaanbiederslijst	Er is precies één instantie hiervan.	*Zorgaanbiederslijst*	n.v.t.	Dit is een atoom van het model.	getalsverhouding
Zorgaanbiederslijst	Deze bevat minstens nul *Zorgaanbieders*.	*Zorgaanbiederslijst*	XML-schema *Zorgaanbiederslijst*	In de starttoestand is de *Zorgaanbiederslijst* leeg.	getalsverhouding
ZorggebruikerBusinessrol	Er is precies één instantie hiervan.	*Register van Informatiestandaarden*	n.v.t.	Dit is een atoom van het model.	getalsverhouding

Stringtypes

Stringtype	Definitie	Validatie door ontvanger lijst
BackchanneluriType	Zie adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.	XML-schema *Zorgaanbiederslijst*
DeelnemerIdType	Kan hier ongespecificeerd blijven.	n.v.t.
DeelnemersovereenkomstIdType	Kan hier ongespecificeerd blijven.	n.v.t.
EndpointportType	Zie adresseringsverantwoordelijkheden op de pagina Gegevens en performance in	n.v.t.

	UCI Verzamelen en UCI Delen.	
EndpointpathType	Zie adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.	n.v.t.
FrontchanneluriType	Zie adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.	XML-schema *Zorgaanbiederslijst*
GegevensdienstIdType	String van minimaal één teken.	XML-schema *Zorgaanbiederslijst* XML-schema *Gegevensdienstnamenlijst*
GegevensdienstnaamType	String van minimaal drie en maximaal 50 tekens.	XML-schema *Gegevensdienstnamenlijst*
HostnameType	Zie adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.	XML-schema van *Whitelist*
OmschrijvingType	Kan hier ongespecificeerd blijven.	n.v.t.
OrganisatienaamType	String van minimaal drie en maximaal 50 tekens.	XML-schema van *OAuthclientlist*
SysteemrolcodeType	String van minimaal één teken.	XML-schema van *Zorgaanbiederslijst*
TransactienaamType	Kan hier ongespecificeerd blijven.	n.v.t.
TransactieverzamelingIdType	Kan hier ongespecificeerd blijven.	n.v.t.
ZorgaanbiedernaamType	Conform toepasselijk Zorgaanbiedersnamenbeleid.	regels 5, 6, 7 en 8 van toepasselijk Zorgaanbiedersnamenbeleid: XML-schema van *Zorgaanbiederslijst*

XML-schema's

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.

Overzicht

Lijst	Bestandsnaam	Release	Versie bestand
Zorgaanbiederslijst	MedMij_Zorgaanbiederslijst.xsd	2	2
Whitelist	MedMij_Whitelist.xsd	2	5
OAuthclientlist	MedMij_OAuthclientlist.xsd	2	2
Gegevensdienstnamenlijst	MedMij_Gegevensdienstnamenlijst.xsd	1	3

Alleen de hierboven genoemde bestanden, met de aangegeven release en versie, mogen worden gebruikt in deze release van het MedMij Afsprakenstelsel.

Voorbeeldbestanden (XML)

Van elke lijst is een voorbeeldbestand beschikbaar. Dit bestand maakt geen onderdeel uit van de formele specificaties van het MedMij Afsprakenstelsel.

Lijst	Bestandsnaam	Versie voorbeeldbestand	Behorend bij XML-schema van de lijst van uitgave
Zorgaanbiederslijst	MedMij_Zorgaanbiederslijst_example.xml	2	Release 2, versie 1
Whitelist	MedMij_Whitelist_example.xml	5	Release 2, versie 5
OAuthclientlist	MedMij_OAuthclientlist_example.xml	2	Release 2, versie 1
Gegevensdienstnamenlijst	MedMij_Gegevensdienstnamenlijst_example.xml	1	Release 1, versie 2

Toelichting

Van metamodel naar hiërarchisch model

De XML-schema's zijn gebaseerd op het metamodel. Een van de majeure verschillen tussen de structuur van het metamodel en die van XML-schema's is dat eerstgenoemde associatief is en XML-schema's hiërarchisch zijn. Een ontwerper van een XML-schema moet zich daarom afvragen hoe de (vrijere) associatieve structuur wordt ingeperkt tot een hiërarchie. In het MedMij Afsprakenstelsel zijn daarbij de volgende afwegingen gebruikt:

- Alle typen en elementen die worden gebruikt binnen een van de lijsten, zijn in het XML-schema van de betreffende lijst gedefinieerd. Met andere woorden, er is geen gebruik gemaakt van een basisschema. Hiermee wordt de afhankelijkheid tussen de XML-schema's beperkt, zodat het gemakkelijker is een aanpassing te doen in een van de schema's zonder dat de andere schema's gewijzigd worden. De definities moeten echter synchroon blijven met het metamodel; een aanpassing van het metamodel maakt aanpassing noodzakelijk van alle XML-schema's die door de wijziging geraakt worden.
- De namen van de XML-typen en XML-elementen zijn zoveel mogelijk identiek aan die in het metamodel, met één belangrijke uitzondering. Daar waar, in het XML-schema, een naam in de hiërarchische context onder een naam is komen te vallen waarmee eerstgenoemde naam zelf begon,

wordt dat begin in het XML-schema weggelaten. Dat gebeurt bijvoorbeeld in het XML-schema van de *Zorgaanbiederslijst* met de naam *ZorgaanbiederGegevensdienst*. Door de manier waarop er hiërarchie is aangebracht, valt die naam in het XML-schema namelijk hiërarchisch onder de naam *Zorgaanbieder*. Daarom volstaat in plaats van het langere *ZorgaanbiederGegevensdienst* ook het kortere *Gegevensdienst*.
- Voor een goede combinatie van (toekomstige) herbruikbaarheid en contextualisering van XML-typen en XML-elementen is het ontwerppatroon met de naam Venetian Blinds gebruikt.

Daarnaast is het metamodel 'statisch'; het geeft de ordening en regels aan die op enig en elk moment gelden in het MedMij afsprakenstelsel. De XML-bestanden voor de lijsten zijn specifieke momentopnames. 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 oudste 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.

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.

Taal- en technische keuzes

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]/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 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. De prefixes voor de namespaces worden zo kort mogelijk gehouden, zijn geheel in lowercase, omwille van de leesbaarheid van de XML-schema's, en hebben de waarde `wl`, `ocl`, `zal` of `gdnl`.

De XML-schema's gaan uit van XML 1.0 en XML Schema 1.0. 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 gebruikgemaakt 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 root element, voorafgegaan door de commentaartekst `<!--Root element-->`.
- De simpleTypes, voorafgegaan door de commentaartekst `<!--SimpleTypes-->`.
- De complexTypes, voorafgegaan door de commentaartekst `<!--ComplexTypes-->`.

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.

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, zorgaanbieders 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?
- Beleid: hoe gaat MedMij om met een aantal belangrijke besturingsthema's, waaronder change and release, toezicht en handhaving, etc.?
- Operationele processen: met welke processen krijgen deelnemers te maken en wat is hun rol hierin?

Rollen

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 zorgaanbieder. 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 zorgaanbieders, 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 zorgaanbieders, 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, zorgaanbieders, 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 zorgaanbieders 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 zorgaanbieders 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 zorgaanbieders 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 zorgaanbieders 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 zorgaanbieders 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 zorgaanbieders, 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 op termijn 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

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 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.

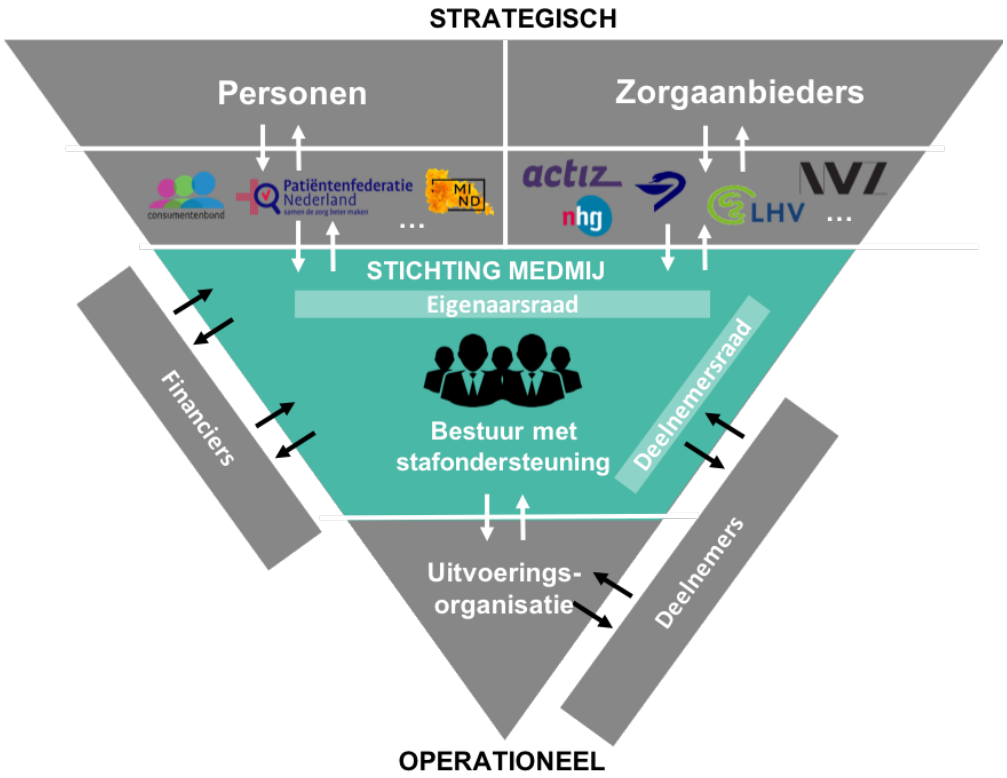
De inrichting van Stichting MedMij betekent niet dat geen hergebruik wordt gemaakt van bestaande beheerexpertise in de zorg en dat alle processen bij Stichting MedMij opnieuw worden ingericht. Een van de belangrijke uitgangspunten van het afsprakenstelsel is om zoveel mogelijk aan te sluiten bij bestaande, 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 zorgaanbieders 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 zorgaanbieders zijn grote, gedifferentieerde groepen en het is onpraktisch om zelf uit deze groepen leden voor eigenaarsraad te werven. De koepels van personen en zorgaanbieders 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 zorgaanbieders 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 zorgaanbieders 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. Werving van stafleden voor de stichting vindt pas eind 2018 plaats.

Beheerverantwoordelijkheden

In 2018 bestaat Programma MedMij nog naast Stichting MedMij en de uitvoeringsorganisatie. Niet alle beheerverantwoordelijkheden hoeven daarom gelijk te worden overgedragen. De volgende beheerverantwoordelijkheden worden in 2018 door de verschillende partijen ingevuld:

Stichting MedMij

- **Eindverantwoordelijkheid functioneren stelsel:** Het gehele beheertakenpakket dat hoort bij het in stand houden van een afsprakenstelsel vereist, net als in de beheersituatie op termijn, 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.

Programma MedMij

- **Visie/meerjarenplan:** Het stelsel zal mee moeten en willen ontwikkelen met de behoeften vanuit de twee grote belanghebbende partijen, de patiënten en de zorgaanbieders, 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.
- **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.
- **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. Voor 2018 is de financiering van het beheer ondertussen geregeld. Voor de financiering van het beheer vanaf 2019 moeten nog afspraken worden gemaakt.

- **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.
- **Communicatie richting eindgebruikers en ombudsfunctie:** 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. Het programma richt een loket in voor eindgebruikers.

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 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.
- **Handhaving bètaversieovereenkomst:** De uitvoeringsorganisatie ziet erop toe dat deelnemers zich houden aan de afspraken uit de bètaversieovereenkomst.
- **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.
- **Afhandelen klachten/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.

- **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.

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. Indien de situatie daarom vraagt, mag de beheerorganisatie na belangenafweging afwijken van het beleid.

Toetredingsbeleid

Het bestuur van Stichting MedMij besluit over toetreding van deelnemers. De uitvoeringsorganisatie bereidt, met input van de potentiële deelnemer, 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 deelnemer 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 deelnemer niet voldoet aan de eisen, dan wel er andere zwaarwegende motivaties zijn om een deelnemer niet toe te laten treden.

De uitvoeringsorganisatie toetst bij toetreding op de aanwezigheid van:

- De basale informatie over de potentiële deelnemer, zoals organisatie- en contactgegevens (o.a. van wettelijk vertegenwoordiger, servicedesks, servicemanager, technisch aanspreekpunt en verantwoordelijke privacy en informatiebeveiliging);
- Een door de potentiële deelnemer ingevulde en ondertekende Zelfverklaring integriteit;
- Een inschrijving in een handelsregister in de EU;
- Een bewijs van certificering conform NEN 7510 die aansluit bij het Normenkader informatiebeveiliging . Indien een deelnemer nog geen NEN 7510-certificering heeft (of deze is nog niet conform het Normenkader informatiebeveiliging), geldt het volgende:
    1. De deelnemer dient tijdens de toetreding een verklaring te overhandigen van zijn certificerende instelling (CI) waaruit blijkt dat (1) de opzet van alle maatregelen is getoetst, en (2) de opzet van de maatregelen conform het Normenkader informatiebeveiliging is;
    2. De deelnemer dient binnen 6 maanden na toetreding het NEN 7510-certificaat en bijbehorende VvT te overhandigen.

Tijdens het toetredingsproces dient de potentiële deelnemer voor minimaal één gegevensdienst succesvol de kwalificatie- en acceptatieprocedure te doorlopen (zie Gegevensdienstenbeleid en Kwalificatie- en acceptatiebeleid). Het toetredingsproces wordt afgerond met de ondertekening van de deelnemersovereenkomst door de potentiële deelnemer en Stichting MedMij. Na de toetreding levert de deelnemer de informatie aan voor de Whitelist, OAuthClientList en de Zorgaanbiederslijst, waaronder:

- De hostname van de vertrouwde MedMijNode(s) van de deelnemer;
- Voor de Dienstverlener zorgaanbieder per zorgaanbiedergegevensdienst-combinatie: zorgaanbiedersnaam, gegevensdienst en technische adressen;
- Voor de Dienstverlener persoon: de via de dienstverlener aangesloten OAuthclients met hun gebruiksvriendelijke namen.

De implementatie van de afspraken en het aanleveren van de juiste informatie is de verantwoordelijkheid van de deelnemer. Waar nodig en gepast kan de uitvoeringsorganisatie ondersteuning bieden door concrete problemen op te lossen, voorlichting te geven over het stelsel 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.

Herhaling toetsing bij verandering juridische status

Mocht de deelnemer na toetreding van juridische status veranderen, dan heeft Stichting MedMij het recht bovenstaande toetredingsprocedure opnieuw te laten doorlopen door de deelnemer (Deelnemersovereenkomsten, artikel 14.3).

Gegevensdienstenbeleid

Gegevensdiensten en de catalogus

Deelnemers bieden via MedMij gestandaardiseerde diensten voor gegevensuitwisseling aan, de zogeheten gegevensdiensten. Deze gegevensdiensten worden uitgewisseld via bijbehorende use cases uit de architectuur van het afsprakenstelsel. De gegevensdiensten die zijn toegestaan binnen MedMij worden opgenomen in de catalogus. Zolang nieuwe gegevensdiensten passen binnen de bestaande use cases, kunnen ze onafhankelijk van een release worden toegevoegd aan de catalogus. Mocht voor een gegevensdienst (een) nieuwe use case nodig zijn, dan dient eerst deze nieuwe use case te worden toegevoegd volgens het reguliere change- en releaseproces. Pas daarna kan ook deze nieuwe gegevensdienst worden toegevoegd aan de Catalogus.

Het Register van Informatiestandaarden

Een gegevensdienst bestaat uit een (verzameling) transactie(s) uit een informatiestandaard. Nictiz beheert voor MedMij het Register van Informatiestandaarden met daarin de informatiestandaarden die binnen MedMij gebruikt worden. Derde partijen kunnen informatiestandaarden indienen voor toepassing binnen MedMij. Zie www.medmij.nl voor het proces van toetreding en de bijbehorende eisen. Besluiten over toetreding van een informatiestandaard tot het register lopen via het bestuur van Stichting MedMij. Om de informatiestandaard ook te kunnen toepassen, worden Gegevensdiensten gedefinieerd die bestaan uit een verzameling transacties uit de informatiestandaard. De uitvoeringsorganisatie doet een voorstel voor de definitie van een of meer Gegevensdiensten (de naamgeving, de relatie met de use cases en de verzamelingen transacties). Het bestuur van de Stichting besluit over aanpassingen aan de catalogus.

Acceptatie op gegevensdiensten

Voordat een gegevensdienst in productie mag worden toegepast, tonen deelnemers aan de gegevensdienst op de juiste manier geïmplementeerd te hebben via de kwalificatie- en acceptatieprocedure (zie Kwalificatie- en acceptatiebeleid).

Overdracht van gegevensdiensten

Dienstverleners zorgaanbieder kunnen, op verzoek van de Zorgaanbieder, het aanbieden van een gegevensdienst van een andere Dienstverlener zorgaanbieder overnemen. Deze overnemende Dienstverlener zorgaanbieder moet in dat geval geaccepteerd zijn voor de gegevensdienst en bij de uitvoeringsorganisatie 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.

Uitfaseren van gegevensdiensten

Bij aanpassingen aan de informatiestandaard, worden voor MedMij een of meerdere nieuwe gegevensdiensten aangemaakt. Deelnemers die deze nieuwe gegevensdienst(en) willen aanbieden, doorlopen hiervoor eerst de kwalficatie- en acceptatieprocedure. Hoe lang de oude gegevensdienst(en), op basis van de vorige versie van de informatiestandaard, nog bruikbaar is/zijn, wordt besloten door het bestuur van Stichting MedMij. Bij dit besluit houdt het bestuur rekening met het perspectief van de deelnemers.

Kwalificatie- en acceptatiebeleid

Deelnemers bieden via het MedMij-netwerk gegevensdiensten aan (zie Gegevensdienstenbeleid). Om toe te zien op een goede implementatie van deze gegevensdiensten, lopen deelnemers voor deze gegevensdiensten een kwalificatie- en acceptatieprocedure door. Deelnemers tonen hiermee aan:

- De inhoud van de gegevensdienst te ondersteunen;
- De uitwisseling van de gegevensdienst te ondersteunen.

Deelnemers hebben een verantwoordelijke die toeziet op het succesvol doorlopen van de kwalificatie- en acceptatieprocedure en geeft de contactgegevens van deze verantwoordelijke door bij toetreding. Mocht deze verantwoordelijke wijzigen, dan geeft de deelnemer dit door aan de uitvoeringsorganisatie.

Ondersteuning inhoud gegevensdienst

Om te borgen dat de inhoud van een gegevensdienst goed wordt geïmplementeerd, dient een deelnemer een kwalificatie te halen op de transacties uit de bijbehorende informatiestandaard. Deze kwalificatie vindt plaats in een kwalificatieomgeving. Het streven is om de toets in deze opstelling met zo min mogelijk aanvullende inspanningen van de deelnemer te doen. Aanvullende technische inspanning blijft echter nodig. Deelnemers committeren zich via hun deelname aan het afsprakenstelsel aan deze inspanningen. Op de volgende pagina staat beschreven om welke inspanningen het gaat. De deelnemer kan zich voorbereiden op de kwalificatie in een testomgeving.

Ondersteuning uitwisseling gegevensdienst

Deelnemers laten bij de acceptatie zien een gegevensdienst in productie uit te kunnen wisselen. Een belangrijk onderdeel hierbij is het aantonen van de ondersteuning van de bijbehorende use case en de overige eisen in de Architectuur en technische specificaties. Indien een deelnemer bij de acceptatie van een andere gegevensdienst al heeft laten zien de use case en/of de overige eisen in de architectuur te ondersteunen, dan wordt hier bij de acceptatie rekening mee gehouden. Ook voor de acceptatie kan de deelnemer zich voorbereiden in een testomgeving.

Herkwalificatie en -acceptatie

Wijzigingen aan de Architectuur en technische specificaties, de Catalogus en de Informatiestandaarden kunnen aanleiding geven tot herkwalificatie en -acceptatie. Besluiten hierover vinden plaats onder verantwoordelijkheid van Stichting MedMij.

Bij wijzigingen in de afsprakenset, is het Change- en releasebeleid van toepassing. Herkwalificatie en -acceptatie behoren daarbij tot de mogelijkheden en zijn in dat geval onderdeel van de implementatieparagraaf bij de release.

Release 1.1 versie 0.8

Het beleid bij wijzigingen aan de Catalogus of de Informatiestandaarden wordt nader uitgewerkt in Release 1.1 versie 1.0.

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 de uitvoeringsorganisatie (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, de beheerorganisatie of zorgaanbieders terecht komen, dienen deelnemers ook de volgende rol in te vullen:

- Een servicedesk bestaande uit minimaal één persoon als dagelijks aanspreekpunt voor gebruikers.

Deelnemers maken bij de uitvoeringsorganisatie kenbaar hoe de servicedesks en de servicemanager te bereiken zijn. Deze contactgegevens worden, voor de eerste maal tijdens het toetredingsproces, geregistreerd en gepubliceerd in een online samenwerkingsplatform voor deelnemers en uitvoeringsorganisatie.

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 de uitvoeringsorganisatie het escalatiekanaal. Namens en samen met de escalerende partijen zal de uitvoeringsorganisatie 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.

Klachten- en geschillenbeleid

Een klacht is een uiting van ongenoegen, gericht aan Stichting MedMij of de uitvoeringsorganisatie over de dienstverlening van een deelnemer, de uitvoeringsorganisatie of de stichting. 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 deelnemer(s) en de uitvoeringsorganisatie;
3. 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 de uitvoeringsorganisatie (zie Samenwerkings- en escalatiebeleid). De klachten en geschillen moeten gerelateerd zijn aan het niet-nakomen van de afspraken/deelnemersovereenkomst door een deelnemer, de uitvoeringsorganisatie 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. De uitvoeringsorganisatie 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 de uitvoeringsorganisatie.

Nalevingsbeleid

Een goede naleving van het afsprakenstelsel is onontbeerlijk voor het vertrouwen in het stelsel. Zowel deelnemers, Stichting MedMij, de uitvoeringsorganisatie 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 partijen aan de afspraken blijven voldoen.

Signalen over het niet naleven van de afspraken door deelnemers komen via meerdere routes bij de beheerorganisatie binnen, waaronder bij:

- Een bemiddeling door de uitvoeringsorganisatie bij een escalatie in de samenwerking (zie Samenwerkings- en escalatiebeleid);
- Verzoeken tot handhaving, meldingen van misstanden of afwijkingen en klachten (Klachten- en geschillenbeleid);
- De (her)acceptatie van een deelnemer op een gegevensdienst (zie Kwalificatie- en acceptatiebeleid);
- 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);
- De hertoetsing vanwege een verandering in de juridische status (zie Toetredingsbeleid).

Het handhaven van de afspraken verloopt langs privaatrechtelijke lijnen. Bij signalering van niet-naleving worden daarom de volgende stappen doorlopen:

1. **Constatering en vastlegging.** De uitvoeringsorganisatie beschrijft zo concreet mogelijk welke verplichting van het MedMij Afsprakenstelsel het betreft, alsmede wat de concrete omstandigheden van het geval zijn;
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 de uitvoeringsorganisatie 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 de uitvoeringsorganisatie en/of 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 de uitvoeringsorganisatie onder verantwoordelijkheid van Stichting MedMij. Besluiten over opschorting of uitsluiting van deelname lopen via Stichting MedMij.

Stichting MedMij en de uitvoeringsorganisatie gaan 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 de Stichting 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 de stichting 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.

Change- en releasebeleid

Het MedMij Afsprakenstelsel is dynamisch van aard. 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. De uitvoeringsorganisatie 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). Jaarlijks stelt de uitvoeringsorganisatie samen met de verschillende belanghebbenden een releaseplanning op voor de doorontwikkeling van het afsprakenstelsel. Wijzigingen moeten passen binnen dit jaarplan en de releaseplanning. Het jaarplan en de releaseplanning moeten op hun beurt weer passen binnen de strategische kaders van Stichting MedMij. Het bestuur van Stichting MedMij stelt het jaarplan en de releaseplanning vast.

Totstandkoming releases

Release 1.1 versie 0.8

De ontwikkeling van het MedMij Afsprakenstelsel wordt momenteel nog projectmatig opgepakt. Daarbij gelden afwijkende afspraken.

Alle belanghebbenden, waaronder in ieder geval de deelnemers, gebruikers en de beheerorganisatie, 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. De uitvoeringsorganisatie doet een eerste beoordeling van ingediende RFC's door deze te toetsen aan de vigerende wet- en regelgeving, architectuur en grondslagen, strategische koers van MedMij, 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. De uitvoeringsorganisatie 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 controleren zij of de voorgestelde oplossing vrij en kosteloos voor de deelnemers te gebruiken is. Mochten belanghebbenden gedurende het change- en releaseproces actief bijdragen aan de uitwerking van een wijziging, dan dient de uitvoeringsorganisatie erop toe te zien dat Stichting MedMij over de juiste auteursrechten komt te beschikken om de documentatie te kunnen publiceren (zie ook 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 samenhangende set van RFC's. Per release wordt een implementatieparagraaf toegevoegd die uiteenzet op welke manier een release moet worden geïmplementeerd.

Verschillende typen releases

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:
    1. Wijzigingen die nodig zijn om een onmiddellijke dreiging voor de continuïteit van of het vertrouwen in het MedMij-afsprakenstelsel/-netwerk af te wenden;
    2. Verbeteringen waarvan de baten van spoedig doorvoeren significant groter zijn dan de implementatie-inspanningen, en die op breed draagvlak onder de deelnemers kan rekenen.

De aanduiding van releases is opgebouwd uit drie nummers, namelijk x.y.z. Hierbij staan de x en de y uit de combinatie voor de major releases (bijvoorbeeld 1.0) en de z voor de minor releases (bijvoorbeeld 1.0.3).

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 is bij een minor release niet noodzakelijk.

Implementatie releases

Zodra het besluit over een release van het afsprakenstelsel is genomen, moet de release worden ingevoerd. Nieuwe releases worden op gestructureerde wijze in het MedMij-netwerk geïmplementeerd. Per release wordt in overleg met de deelnemers en eigenaren bepaald welke aanpak de minste impact/verstoringen veroorzaakt. Ook wordt de afweging gemaakt of releases in productie naast elkaar kunnen bestaan en of deelnemers op enig moment meerdere releases moeten ondersteunen. De gekozen aanpak wordt gepland en volgens deze planning uitgevoerd. De uitvoeringsorganisatie 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 de uitvoeringsorganisatie 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).

MedMij hanteert een vaste cyclus voor releases van het afsprakenstelsel. In principe zijn er twee momenten in het jaar waarop deze geïmplementeerd moeten zijn: 1 juni en 1 december. Voor de implementatie van de release zijn de data in de implementatieplanning bij de release echter leidend. Afhankelijk van het soort release kan een implementatietermijn van toepassing zijn.

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. De uitvoeringsorganisatie en elke afzonderlijke deelnemer hebben een verantwoordelijke voor privacy en informatiebeveiliging in dienst (zie Normenkader informatiebeveiliging) en tussen deze verantwoordelijken is minimaal vier keer per jaar overleg. Hieromheen is een incidenten- en calamiteitenprocedure ingericht, zodat duidelijk is wat er van de verschillende partijen wordt verwacht in noodsituaties. Deelnemers zijn verantwoordelijk voor het doorgeven van de juiste contactpersoon en informeren de uitvoeringsorganisatie 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.

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.

Zorgaanbiedersnamenbeleid

Zorgaanbieders kunnen hun deelname en de manier waarop ze via MedMij te bereiken zijn aan personen kenbaar maken via een zorgaanbiedersnaam (zorgaanbiedersnaam@medmij). Het zorgaanbiedersnamenbeleid beschrijft hoe een zorgaanbieder een voor de persoon herkenbare naam kan kiezen, zonder in de toekomst de mogelijkheden van andere zorgaanbieders om een herkenbare naam te kiezen te veel te beperken.

Wie kiest de zorgaanbiedersnaam?

De zorgaanbieder bepaalt de gekozen naam en de Dienstverlener zorgaanbieder geeft deze naam door aan de uitvoeringsorganisatie. De uitvoeringsorganisatie stelt de naam in opdracht van Stichting MedMij vast. Het is de verantwoordelijkheid van de Dienstverlener zorgaanbieder om de Zorgaanbieder te informeren over de context en het doel van de naam binnen MedMij.

Waar moet de zorgaanbiedersnaam aan voldoen?

1. De naam moet gekoppeld zijn aan de naam die de zorgaanbieder 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 zorgaanbieders 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 50 karakters lang (exclusief `@medmij`);
7. De naam wordt geregistreerd in kleine letters;
8. De naam mag alleen bestaan uit karakters die voorkomen in het Nederlandse alfabet (bestaande uit zesentwintig letters). Diakrieten, speciale tekens (zoals spatie, koppelteken en punt) zijn dus niet toegestaan;
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.

OAuthclient-namenbeleid

Binnen de OAuth-flow wordt aan de Persoon toestemming gevraagd voor de gegevensuitwisseling tussen een Zorgaanbieder 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 zorgaanbieder 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 OAuth-naam?

De Dienstverlener persoon bepaalt de gekozen naam en geeft deze door aan de uitvoeringsorganisatie. De uitvoeringsorganisatie stelt de naam vast in opdracht van Stichting MedMij.

Waar moet de OAuth-naam aan voldoen?

1. De naam moet gelijk zijn aan de organisatienaam van de Dienstverlener persoon;
2. De naam dient zoveel mogelijk gelijk te zijn aan de naam zoals opgenomen in het handelsregister;
3. De naam is minimaal drie en maximaal 50 karakters lang;
4. De naam mag niet te herleiden zijn tot een persoon;
5. De naam mag in het verleden niet door een andere Dienstverlener persoon gebruikt zijn;
6. De naam mag het merk MedMij niet negatief beïnvloeden.

Operationele processen

Doel

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 voor (potentiële) deelnemers beschikbaar bij de uitvoeringsorganisatie.

Naast de use cases, 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. Het gaat om de volgende processen:

- Het toetredingsproces;
- Het uittredingsproces;
- Het incidenten- en calamiteitenproces;
- Registratieproces aanbod gegevensdiensten door deelnemer;
- De registratieprocessen voor de Zorgaanbiederslijst, Whitelist en OAuthclientlist;
- Het managementinformatieproces.

Toetredingsproces

- **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. Op welke manier deelnemers dit moeten doen, staat beschreven bij het Toetredingsbeleid;
  - 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.

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).
  - Uitvoeringsorganisatie voert de benodigde mutaties door in het deelnemersregister en de relevante lijsten.
- **Resultaat:** Deelnemer is uitgetreden uit het afsprakenstelsel.
- **Uitzonderingen:** -

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 uitvoeringsorganisatie constateert een incident/calamiteit.
- **Afspraken over het proces:**
  - In de nadere uitwerking van het proces bij de uitvoeringsorganisatie wordt gedefinieerd wat een incident en calamiteit is in het kader van MedMij. De procesafspraken hebben hier betrekking op;
  - Deelnemers en uitvoeringsorganisatie zijn verplicht elkaar te informeren over relevante kwetsbaarheden. Uitvoeringsorganisatie draagt zorg voor een centraal proces voor het signaleren en delen van nieuwe voor MedMij relevante kwetsbaarheden. In het proces zijn termijnen verbonden aan het oplossen van de kwetsbaarheden.
  - Deelnemers en uitvoeringsorganisatie 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 uitvoeringsorganisatie dienen zo spoedig mogelijk de benodigde acties uit te zetten om een incident of calamiteit op te lossen.
  - Uitvoeringsorganisatie 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 de uitvoeringsorganisatie hebben alle één persoon binnen de eigen organisatie aangewezen als eindverantwoordelijke en centraal contactpersoon voor informatiebeveiligingsincidenten en -calamiteiten (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 de uitvoeringsorganisatie (waar dit niet de wettelijke verplichting betreft);
- **Resultaat:** Incident en/of calamiteit is opgelost door de betrokkenen.
- **Uitzonderingen:** -

Registratieproces aanbod gegevensdiensten door deelnemer

- **Doel:** Het registratieproces aanbod gegevensdiensten door deelnemer heeft als doel de juiste informatie vast te leggen over het aanbod van gegevensdiensten door de deelnemer.
- **Initiatie:**
  - Deelnemer is geaccepteerd voor een gegevensdienst en mag deze aanbieden;
  - Deelnemer wil een gegevensdienst niet meer aanbieden;
  - Deelnemer mag een gegevensdienst niet meer aanbieden op grond van falende herkwalificatie of -acceptatie.
- **Afspraken over het proces:**
  - Uitvoeringsorganisatie 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:** De uitvoeringsorganisatie heeft het deelnemersregister en de overige relevante lijsten aangepast. De deelnemer wordt geïnformeerd over de doorgevoerde wijziging.
- **Uitzonderingen:** -

Registratieprocessen Zorgaanbiederslijst, Whitelist en OAuthclientlist

- **Doel:** De registratieprocessen voor de Zorgaanbiederslijst, 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 de uitvoeringsorganisatie om een entry in de Zorgaanbiederslijst, Whitelist of OAuthclientlist aan te maken, te wijzigen of te verwijderen.
  - Triggers voor wijzigingen zijn per lijst verschillend:
    - Zorgaanbiederslijst:

        - Deelnemer wil in het MedMij-netwerk kenbaar maken een gegevensdienst voor een zorgaanbieder aan te bieden;
        - Deelnemer wil in het MedMij-netwerk kenbaar maken een gegevensdienst voor een zorgaanbieder niet meer aan te bieden;
        - Deelnemer wil een endpoints bij een ZorgaanbiederGegevensdienst wijzigen.
    - Whitelist:
        - Deelnemer wil een node op het MedMij-netwerk gebruiken;
        - Deelnemer wil een van haar eigen nodes niet meer op het MedMij-netwerk gebruiken.
    - OAuthclientlist:
        - Dienstverlener persoon wil een OAuthclients toevoegen;
        - Dienstverlener persoon wil een OAuthclient verwijderen;
        - Dienstverlener persoon wil een gebruiksvriendelijke naam opgeven bij een eigen OAuthclient;
        - Dienstverlener persoon wil de gebruiksvriendelijke naam aanpassen bij een eigen OAuthclient.
- **Afspraken over het proces:**
    - Deelnemer is verantwoordelijk voor het aanleveren van mutaties voor de Zorgaanbiederslijst, WhiteList en OAuthclientlist.
    - Mutaties zijn gebonden aan de verantwoordelijkheden en regels zoals gespecificeerd in de Architectuur en technische specificaties, het Zorgaanbiedersnamenbeleid en OAuthclient-namenbeleid.
    - Uitvoeringsorganisatie neemt het verzoek in behandeling en is verantwoordelijk voor een check op integriteit.
    - Valide mutaties worden in 95 procent van de gevallen door de uitvoeringsorganisatie binnen 2 werkdagen verwerkt. Urgente mutaties krijgen daarbij voorrang. De mutatietijd voor urgente mutaties wordt in overleg met de uitvoeringsorganisatie bepaald. Bij verwachte overschrijding van de (overeengekomen) verwerkingstijd, informeert de uitvoeringsorganisatie de deelnemer hierover.
- **Resultaat:** De uitvoeringsorganisatie 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. Uitvoeringsorganisatie vraagt de deelnemer om het verzoek aan te passen.

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.
    - Uitvoeringsorganisatie 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. De uitvoeringsorganisatie verzoekt de deelnemer alsnog de benodigde informatie aan te leveren. Mocht een deelnemer (herhaaldelijk) in gebreke blijven, dan treedt het Nalevingsbeleid in werking.

Normenkader informatiebeveiliging

Het vertrouwen in MedMij valt of staat met de informatiebeveiliging van het stelsel. De beheersing van risico's op dit gebied is daarom cruciaal. Het normenkader informatiebeveiliging biedt een overzicht van de beheersmaatregelen die voor de informatiebeveiliging in het stelsel zijn opgenomen. Aanscherping van het normenkader vindt jaarlijks plaats in navolging van een stelselbrede risicoanalyse.

Uit een overkoepelende risicoanalyse op het afsprakenstelsel die is uitgevoerd is geconcludeerd dat een NEN 7510-certificering voor deelnemers en een ISO 27001-certificering voor de beheerorganisatie, 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, met uitzondering van een aantal maatregelen die raken aan de beschikbaarheid van systemen, de informatieclassificatie en de afhandeling van incidenten, calamiteiten en kwetsbaarheden (waarvoor nog inrichting nodig is bij de beheerorganisatie). In een volgende release worden ook deze maatregelen opgenomen in het stelsel. Deelnemers dienen de maatregelen in het normenkader mee te laten nemen in hun NEN 7510-certificeringsproces.

NEN 7510-certificering is gangbaar en wettelijk verplicht bij de gegevensuitwisseling in het zorgaanbiedersdomein. 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 zorgaanbiedersdomein 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.

Ook de beheerorganisatie zal voor de uitvoering van haar diensten binnen het MedMij netwerk gebonden zijn aan de NEN 7510 norm.

Certificeringseisen deelnemers

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 zorgaanbiedersdomein zijn. 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 7510:2017 is begin juni 2018 gepubliceerd. MedMij stelt de volgende eisen aan een NEN 7510-certificering voor deelnemers:

- De dienstverlener in het zorgaanbiedersdomein moet de zorgaanbieders als belanghebbenden hebben geïdentificeerd en de bijkomende verantwoordelijkheden hebben meegenomen bij het uitvoeren/herijken van de risicoanalyse (zie ook hetgeen hierover is opgenomen bij Wbp/AVG in het Juridisch kader);
- In de certificering moet het afsprakenstelsel MedMij onderdeel uitmaken van de scope;
- 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 toont jaarlijks met een **aanvullende auditverklaring met een onderbouwende rapportage** aan te voldoen aan de eisen voor MedMij. 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. Tevens dient het NEN 7510 certificaat te zijn opgenomen in het door NEN beheerde nationale certificatenregister NEN 7510. Voor de onderbouwende rapportage bij de auditverklaring wordt door MedMij een format beschikbaar gesteld.

Normenkader

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

Norm (NEN 7510: 2017)	DVP	DVZA	BO	Implementatie
A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	✓	✓		Opgeslagen persoonlijke gezondheidsgegevens MOETEN beschermd worden door middel van disk-level en/of database-level encryptie, gebruikmakend van een "veilig", "goed" of "betrouwbaar" algoritme. *Pagina 16 van https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html benoemt algoritmen die hiervoor gebruikt kunnen worden.*
A.12.1.2 Wijzigingsbeheer	✓	✓		Er is een overkoepelend Proces Change and Release gedefinieerd om wijzigingen aan functionele-, operationele- en beveiligingseigenschappen te ontwerpen, testen, communiceren en te implementeren. Deelnemers dienen aan te sluiten op dit proces.
A.12.1.3 Capaciteitsbeheer	✓	✓	✓	• Beschikbaarheid en responsetijden voor **deelnemers** zijn vastgelegd in Gegevens en performance in UCI Verzamelen en UCI Delen. • Beschikbaarheid en responsetijden voor de **beheerorganisatie** zijn vastgelegd in Gegevens en performance inzake opvragen lijsten.
A.12.3.1 Back-up van informatie	✓	✓		De dienstverlener persoon dient een backupschema in plaats te hebben met bijbehorende (minimaal jaarlijks geteste) recovery procedures die ervoor zorgen dat de gegevens van de persoon binnen een dag (24u) terug kunnen worden geplaatst in geval van een inciden
A.12.4.1 Gebeurtenissen registreren	✓	✓	✓	1. Logging moet plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie Processen en informatie onder Logging) 2. Verzoeken en toestemmingsverklaring van gebruikers ten aanzien van het opvragen van informatie bij zorgverleners dienen onweerlegbaar en controleerbaar te worden vastgelegd.
A.12.4.4 Kloksynchronisatie	✓	✓	✓	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met **pool.ntp.org**. Het is toegestaan te synchroniseren met een lokale NTP-server, zolang deze ten minste 1x per 24 uur synchroniseert met bovengenoemde NTP-server.
A.12.5.1 Software installeren op operationele systemen	✓	✓	✓	Het uitvoeren van kritische handelingen op systemen en gegevens die direct impact (kunnen) hebben op de beschikbaarheid, integriteit of vertrouwelijkheid van de keten, dienen op basis van het vier-ogen-principe te worden uitgevoerd.
A.12.6.1 Beheer van technische kwetsbaarheden	✓	✓		Deelnemers dienen aan te sluiten bij het proces van beheren van technische kwetsbaarheden in het afsprakenstelsel (Operationele processen).
A.14.2.1 Beleid voor beveiligd ontwikkelen	✓	✓	✓	Er moeten door de deelnemers beveiligingsstandaarden worden toegepast in de ontwikkelde internet facing applicaties. Minimale

				beveiligingsstandaarden waaraan alle ontwikkelde applicaties van deelnemers moeten voldoen: 1. Voor webapplicaties worden de ICT- Beveiligingsrichtlijnen voor webapplicaties van het NCSC gehanteerd. In het bijzonder zijn dan de maatregelen uit het "Uitvoeringsdomein" van belang, https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html. 2. Voor mobiele applicaties kan worden gesteund op richtlijnen var OWASP die zijn opgesteld in samenwerking met ENISA (https://www.owasp.org/index.php /OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Contrc).
A.16.1.1 Verantwoordelijkheden en procedures	✓	✓		Deelnemers moeten aansluiten bij het proces voor incidenten en calamiteiten zoals dit is gedefinieerd in het afsprakenstelsel (Operationele processen).
A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	✓	✓	✓	Er is een meldplicht voor alle deelnemers en de beheerorganisatie om incidenten die betrekking hebben op patiëntgegevens of het functioneren van het MedMij stelsel binnen 48 uur te melden bij centrale incident management team. Zie Deelnemersovereenkomsten.
A.16.1.7 Verzamelen van bewijsmateriaal	✓	✓	✓	Deelnemers en de beheerorganisatie dienen medewerking te verlenen aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties.
A.18.2.3 Beoordeling van technische naleving	✓	✓	✓	1. Tenminste jaarlijks laten de deelnemers en de beheerorganisati **whitebox** applicatiepenetratietesten en code reviews uitvoeren op de externe koppelvlakken. *Non-conformiteiten* worden gemeld bij de beheerorganisatie. 2. Tenminste jaarlijks laat de beheerorganisatie **blackbox** infrastructuur penetratietesten uitvoeren op de externe koppelvlakken van de deelnemers ten behoeve van het MedMij stelsel.
A.5.1.1 Beleidsregels voor informatiebeveiliging	✓	✓	✓	De beleidsdocumenten van deelnemers dienen de beleidsmaatregelen die van toepassing zijn op MedMij (zoals gespecificeerd in Privacy- en informatiebeveiligingsbeleid) specifiek te benoemen.
A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging				Elke deelnemer en de beheerorganisatie dient een verantwoordelijkheid te beleggen met betrekking tot alle zaken rond informatiebeveiliging, met mandaat om besluiten te nemen ten aanzier van MedMij. De organisatie dient tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur op dit onderwerp. (Conform de betreffende Deelnemersovereenkomsten)
A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging				Elke medewerker van de deelnemers en de beheerorganisatie die werkzaamheden verricht gerelateerd aan MedMij dient onderwezen te worden over de algemene werking van het stelsel en op de voor hem /haar van toepassing zijnde beveiligingsmaatregelen. Deze training wordt door de beheerorganisatie beheerd en gefaciliteerd.
A.8.2.1 Classificatie van informatie	✓	✓	✓	

Classificatie van gegevens die binnen het stelsel worden uitgewisseld (gezondheidsgegevens, metagegevens, operationele gegevens) worden door MedMij geclassificeerd conform het Informatieclassificatiebeleid.

> **Release 1.1 versie 0.8**
>
> Het Informatieclassificatiebeleid wordt nog uitgewerkt in release 1.1 versie 1.0.

A.9.1.1 Beleid voor toegangsbeveiliging			Het inzien van persoonlijke gezondheidsgegevens door (medewerkers van) deelnemers en door de beheerorganisatie is niet toegestaan. Er dienen passende technische maatregelen te worden genomen om dit t voorkomen en te kunnen controleren. Indien dit (tijdelijk) wel mogelijk is (geweest) dient dit te worden gemeld bij de beheerorganisatie.
A.9.2.5 Beoordeling van toegangsrechten van gebruikers	✔	✔	Toegangsrechten en het gebruik daarvan op systemen waar persoonlijke zorginformatie wordt opgeslagen of worden verwerkt dienen periodiek gecontroleerd te worden.
A.9.4.1 Beperking toegang tot informatie	✔	✔	Gebruikers kunnen enkel toegang krijgen tot persoonlijke gezondheidsgegevens na authenticatie op basis van twee factoren.

A.5.1.1 Beleidsregels voor informatiebeveiliging

Norm

Rationale	Deze maatregel borgt dat beleidsdocumenten van alle partijen in lijn zijn met het Afsprakenstelsel.
Implementatie	De beleidsdocumenten van deelnemers dienen de beleidsmaatregelen die van toepassing zijn op MedMij (zoals gespecificeerd in Privacy- en informatiebeveiligingsbeleid) specifiek te benoemen.
Toetsing	Door middel van interviews en het tonen van evidence (beleidsdocumenten).
NEN 7510: 2017	A.5.1.1 Beleidsregels voor informatiebeveiliging
NEN 7510: 2011	A.5.1.1 Beleidsdocument voor informatiebeveiliging

Rollen

DVP	✔
DVZA	✔
BO	✔

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, 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	Elke deelnemer en de beheerorganisatie dient een verantwoordelijkheid te beleggen met betrekking tot alle zaken rond informatiebeveiliging, met mandaat om besluiten te nemen ten aanzien van MedMij. De organisatie dient tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur op dit onderwerp. (Conform de betreffende Deelnemersovereenkomsten)
Toetsing	Stel vast dat er overeenkomstige rollen zijn ingevuld en dat de vereiste bereikbaarheid geborgd is.
NEN 7510: 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

Rollen

DVP	
DVZA	
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

A.7.2.2 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	Elke medewerker van de deelnemers en de beheerorganisatie die werkzaamheden verricht gerelateerd aan MedMij dient onderwezen te worden over de algemene werking van het stelsel en op de voor hem/haar van toepassing zijnde beveiligingsmaatregelen. Deze training wordt door de beheerorganisatie beheerd en gefaciliteerd.
Toetsing	Stel vast dat de partij deel heeft genomen aan de training van MedMij en 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

Rollen

DVP	
DVZA	
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, 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. Het gaat hier met name om (zeer) vertrouwelijke informatie, zoals risicoanalyses, pentestrapporten en de whitelist.
Implementatie	Classificatie van gegevens die binnen het stelsel worden uitgewisseld (gezondheidsgegevens, metagegevens, operationele gegevens) worden door MedMij geclassificeerd conform het Informatieclassificatiebeleid. **Release 1.1 versie 0.8** Het Informatieclassificatiebeleid wordt nog uitgewerkt in release 1.1 versie 1.0.
Toetsing	Door middel van interviews en/of het tonen van evidence (zoals het informatieclassificatieschema of -beleid van de partij).
NEN 7510: 2017	A.8.2.1 Classificatie van informatie
NEN 7510: 2011	A.7.2.1 Richtlijnen voor classificatie

Rollen

DVP	✔
DVZA	✔
BO	✔

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

A.9.1.1 Beleid voor toegangsbeveiliging

Norm

Rationale	Deze maatregel borgt dat persoonlijke gezondheidsgegevens alleen toegankelijk zijn voor de zorgverlener en de patiënt (zie ook A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen) en A.16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen nieuw).
Implementatie	Het inzien van persoonlijke gezondheidsgegevens door (medewerkers van) deelnemers en door de beheerorganisatie is niet toegestaan. Er dienen passende technische maatregelen te worden genomen om dit te voorkomen en te kunnen controleren. Indien dit (tijdelijk) wel mogelijk is (geweest) dient dit te worden gemeld bij de beheerorganisatie.
Toetsing	Stel vast dat het technisch onmogelijk is gemaakt dat (medewerkers van) partijen zich zonder notificatie inzage kunnen verschaffen in persoonlijke gezondheidsgegevens en dat er een proces bestaat om afwijkingen te melden aan de beheerorganisatie.
NEN 7510: 2017	A.9.1.1 Beleid voor toegangsbeveiliging
NEN 7510: 2011	A.11.1.1 Toegangsbeleid

Rollen

DVP	
DVZA	
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, 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 systemen.
Implementatie	Toegangsrechten en het gebruik daarvan op systemen waar persoonlijke zorginformatie wordt opgeslagen of worden verwerkt dienen periodiek gecontroleerd te worden.
Toetsing	Stel vast dat de partij toegangsrechten (en het gebruik daarvan) op systemen waar patiëntgegevens worden opgeslagen of verwerkt, periodiek controleert.
NEN 7510: 2017	A.9.2.5 Beoordeling van toegangsrechten van gebruikers
NEN 7510: 2011	A.11.2.4 Beoordeling van toegangsrechten van gebruikers

Rollen

DVP	✔
DVZA	✔
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

A.9.4.1 Beperking toegang tot informatie

Norm

Rationale	Deze maatregel borgt dat gebruikers alleen toegang kunnen krijgen tot persoonlijke gegevens na een betrouwbare authenticatie, alleen een gebruikersnaam en wachtwoord is niet veilig genoeg.
Implementatie	Gebruikers kunnen enkel toegang krijgen tot persoonlijke gezondheidsgegevens na authenticatie op basis van twee factoren.
Toetsing	Stel door middel van technische documentatie en de werking vast dat twee factor authenticatie wordt toegepast.
NEN 7510: 2017	A.9.4.1 Beperking toegang tot informatie
NEN 7510: 2011	A.11.5.2 Gebruikersindentificatie en -authenticatie

Rollen

DVP	✔
DVZA	✔
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen

Norm

Rationale	Deze maatregel borgt dat bij het versleutelen van persoonlijke gezondheidsgegevens gebruik wordt gemaakt van als veilig aangemerkte algoritmen.
Implementatie	Opgeslagen persoonlijke gezondheidsgegevens MOETEN beschermd worden door middel van disk-level en/of database-level encryptie, gebruikmakend van een "veilig", "goed" of "betrouwbaar" algoritme. *Pagina 16 van https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html benoemt algoritmen die hiervoor gebruikt kunnen worden.*
Toetsing	Dit kan worden aangetoond door het tonen van architectuurdiagrammen, waar de auditor door middel van steekproeven moet laten aantonen dat op die punten is voldaan aan de gestelde eisen. Aantonen kan plaatsvinden door middel van uitleg of door het tonen van evidence.
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

Rollen

DVP	✔
DVZA	✔
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

A.12.1.2 Wijzigingsbeheer

Norm

Rationale	Deze maatregel borgt dat wijzigingen binnen de keten beheerst verlopen. Zie ook A. 12.5.1 Software installeren op operationele systemen.
Implementatie	Er is een overkoepelend Proces Change and Release gedefinieerd om wijzigingen aan functionele-, operationele- en beveiligingseigenschappen te ontwerpen, testen, communiceren en te implementeren. Deelnemers dienen aan te sluiten op dit proces.
Toetsing	Dit kan worden aangetoond door het volgen van een recente change/release, of door het aantonen van de raakvlakken van de eigen processen voor wijzigingsbeheer met die van het afsprakenstelsel.
NEN 7510: 2017	A.12.1.2 Wijzigingsbeheer
NEN 7510: 2011	A.10.1.2 Wijzigingsbeheer

Rollen

DVP	✔
DVZA	✔
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

A.12.1.3 Capaciteitsbeheer

Norm

Rationale	Deze maatregel borgt dat alle systemen in de keten voldoen aan de afgesproken eisen omtrent beschikbaarheid en responsetijden.
Implementatie	• Beschikbaarheid en responsetijden voor **deelnemers** zijn vastgelegd in Gegevens en performance in UCI Verzamelen en UCI Delen. • Beschikbaarheid en responsetijden voor de **beheerorganisatie** zijn vastgelegd in Gegevens en performance inzake opvragen lijsten.
Toetsing	Partijen kunnen dit aantonen door middel van eigen rapportages/metingen.
NEN 7510: 2017	A.12.1.3 Capaciteitsbeheer
NEN 7510: 2011	A.10.3.1 Capaciteitsbeheer

Rollen

DVP	✔
DVZA	✔
BO	✔

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

A.12.3.1 Back-up van informatie

Norm

Rationale	Deze maatregel borgt dat deelnemers beschikken over een bruikbare back-up.
Implementatie	De dienstverlener persoon dient een backupschema in plaats te hebben met bijbehorende (minimaal jaarlijks geteste) recovery procedures die ervoor zorgen dat de gegevens van de persoon binnen een dag (24u) terug kunnen worden geplaatst in geval van een incident.
Toetsing	Dit kan worden aangetoond door het aantonen van de raakvlakken van de eigen backup-policy met die van het afsprakenstelsel.
NEN 7510: 2017	A.12.3.1 Back-up van informatie
NEN 7510: 2011	A.10.5.1 Reservekopieën (back-ups)

Rollen

DVP	✔
DVZA	✔
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, 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 zorgaanbieder door patienten, het inzien of wijzigen van een PGO of het wijzigen aan loggen van gebruikers aan hun PGO) ten minste 12 maanden inzichtelijk blijven.
Implementatie	1. Logging moet plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie Processen en informatie onder Logging) 2. Verzoeken en toestemmingsverklaring van gebruikers ten aanzien van het opvragen van informatie bij zorgverleners dienen onweerlegbaar en controleerbaar te worden vastgelegd.
Toetsing	1. Dit kan worden aangetoond door het tonen van logbestanden (maximaal 12 maanden oud) van alle systemen waar gezondheidsgegevens zijn opgeslagen of worden verwerkt, waarbij specifiek moet worden gelet op de zaken die in het afsprakenstelsel worden gespecificeerd. 2. Dit kan worden aangetoond door het tonen van een registratie van dergelijke verzoeken.
NEN 7510: 2017	A.12.4.1 Gebeurtenissen registreren
NEN 7510: 2011	A.10.10.1 Aanmaken audit-logbestanden A.10.10.2 Controle van systeemgebruik

Rollen

DVP	✔
DVZA	✔
BO	✔

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, 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 alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met **pool.ntp.org**. Het is toegestaan te synchroniseren met een lokale NTP-server, zolang deze ten minste 1x per 24 uur synchroniseert met bovengenoemde NTP-server.
Toetsing	Dit kan worden aangetoond door configuratie of logging van synchronisatie met de genoemde NTP-server.
NEN 7510: 2017	A.12.4.4 Kloksynchronisatie
NEN 7510: 2011	A.10.10.6 Synchronisatie van systeemklokken

Rollen

DVP	✔
DVZA	✔
BO	✔

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

A.12.5.1 Software installeren op operationele systemen

Norm

Rationale	Deze maatregel borgt dat er altijd twee medewerkers betrokken zijn bij werkzaamheden aan systemen (configuratiewijzigingen, onderhoud, installatie van updates) en vermindert het risico op onbeschikbaarheid van de keten.
Implementatie	Het uitvoeren van kritische handelingen op systemen en gegevens die direct impact (kunnen) hebben op de beschikbaarheid, integriteit of vertrouwelijkheid van de keten, dienen op basis van het vier-ogen-principe te worden uitgevoerd.
Toetsing	Dit kan worden aangetoond door het tonen van procedures en door interviews met verantwoordelijke medewerkers.
NEN 7510: 2017	A.12.5.1 Software installeren op operationele systemen
NEN 7510: 2011	A.12.4.1 Beheersing van operationele programmatuur

Rollen

DVP	✔
DVZA	✔
BO	✔

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, 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. Reageren kan bestaan uit: 1. Het onderzoeken of een (vermeende) kwetsbaarheid relevant is voor de eigen systemen 2. Hierover terugkoppelen 3. Het patchen van systemen (zie A.12.5.1 Software installeren op operationele systemen) Zie ook A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging.
Implementatie	Deelnemers dienen aan te sluiten bij het proces van beheren van technische kwetsbaarheden in het afsprakenstelsel (Operationele processen).
Toetsing	Dit kan worden aangetoond door middel van interviews en door het tonen van processen.
NEN 7510: 2017	A.12.6.1 Beheer van technische kwetsbaarheden
NEN 7510: 2011	A.12.6.1 Beheersing van technische kwetsbaarheden

Rollen

DVP	✔
DVZA	✔
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, 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, om te voorkomen dat bekende programmeerfouten worden gemaakt.
Implementatie	Er moeten door de deelnemers beveiligingsstandaarden worden toegepast in de ontwikkelde internet facing applicaties. Minimale beveiligingsstandaarden waaraan alle ontwikkelde applicaties van deelnemers moeten voldoen: 1. Voor webapplicaties worden de ICT- Beveiligingsrichtlijnen voor webapplicaties van het NCSC gehanteerd. In het bijzonder zijn dan de maatregelen uit het "Uitvoeringsdomein" van belang, https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html. 2. Voor mobiele applicaties kan worden gesteund op richtlijnen van OWASP die zijn opgesteld in samenwerking met ENISA (https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Controls).
Toetsing	Door middel van interviews en het tonen van evidence kan worden vastgesteld of het beleid voor beveiligd ontwikkelen van de partij voldoet aan de eisen die het afsprakenstelsel stelt.
NEN 7510: 2011	Deze maatregel bestond nog niet in NEN 7510:2011

Rollen

DVP	✔
DVZA	✔
BO	✔

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, 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	Deelnemers moeten aansluiten bij het proces voor incidenten en calamiteiten zoals dit is gedefinieerd in het afsprakenstelsel (Operationele processen).
Toetsing	Door middel van interviews en het tonen van evidence, zoals het incidentenproces van de deelnemer.
NEN 7510: 2017	A.16.1.1 Verantwoordelijkheden en procedures
NEN 7510: 2011	A.13.2.1 Verantwoordelijkheden en procedures

Rollen

DVP	✔
DVZA	✔
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, 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	Er is een meldplicht voor alle deelnemers en de beheerorganisatie om incidenten die betrekking hebben op patiëntgegevens of het functioneren van het MedMij stelsel binnen 48 uur te melden bij centrale incident management team. Zie Deelnemersovereenkomsten.
Toetsing	Stel vast dat medewerkers op de hoogte zijn van deze eis door middel van interviews of het tonen van beleidsdocument en/of processen.
NEN 7510: 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

Rollen

DVP	✔
DVZA	✔
BO	✔

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, 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	Deelnemers en de beheerorganisatie dienen medewerking te verlenen aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties.
Toetsing	Door middel van interviews en het tonen van evidence, zoals processen of beleidsdocumenten.
NEN 7510: 2017	A.16.1.7 Verzamelen van bewijsmateriaal
NEN 7510: 2011	A.13.2.3 Verzamelen van bewijsmateriaal

Rollen

DVP	✔
DVZA	✔
BO	✔

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

A.18.2.3 Beoordeling van technische naleving

Norm

Rationale	Deze maatregel borgt dat deelnemers en de beheerorganisatie met regelmaat (en gebruikmakend van verschillende partijen) hun software en systemen laten toetsen op bekende kwetsbaarheden.
Implementatie	1. Tenminste jaarlijks laten de deelnemers en de beheerorganisatie **whitebox** applicatiepenetratietesten en code reviews uitvoeren op de externe koppelvlakken. *Non-conformiteiten* worden gemeld bij de beheerorganisatie. 2. Tenminste jaarlijks laat de beheerorganisatie **blackbox** infrastructuur penetratietesten uitvoeren op de externe koppelvlakken van de deelnemers ten behoeve van het MedMij stelsel.
Toetsing	Door middel van interviews en het tonen van evidence (auditrapporten).
NEN 7510: 2017	A.18.2.3 Beoordeling van technische naleving
NEN 7510: 2011	A.15.2.2 Controle op technische naleving

Rollen

DVP	✔
DVZA	✔
BO	✔

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

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 zorgaanbieder. 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 zorgaanbieder);
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 zorgaanbieder 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 de Zorgaanbieder.

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.

Gebruik van het merk door de zorgaanbieder vindt zoveel mogelijk plaats in combinatie met de unieke zorgaanbiedersnaam.

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 zorgaanbieder bijvoorbeeld met het merk aan de Zorgaanbieder 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.

Consistente toepassing van het merk

Een consistente toepassing van het merk draagt bij aan de waarde hiervan. In veel gevallen betekent deze toepassing dat een deelnemer een logo presenteert of een tekstuele verwijzing maakt naar MedMij. De volgende logo's mogen hierbij gebruikt worden (bij online gebruik is het toegestaan deze logo's te linken naar de MedMij-website):

Voor de herkenbaarheid van de communicatie vanuit MedMij, is verdergaand gebruik van de huisstijl in principe voorbehouden aan de beheerorganisatie. 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 zorgaanbieders in de digitale gegevensuitwisseling via MedMij te vergroten. Richting de Persoon wordt de Gebruikersvoorlichting persoonsdomein en richting de Zorgaanbieder de Gebruikersvoorlichting zorgaanbiedersdomein 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

De toestemmingsverklaring is een verplichte tekst die de Dienstverlener zorgaanbieder dient voor te leggen aan de Persoon bij het ophalen van gezondheidsgegevens 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 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 UC Verzamelen 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 Persoon - Zorgaanbieder

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.

U verleent hierbij `NaamZorgaanbieder` toestemming om `NaamGegevensdienst` uit te wisselen met `NaamLeverancierPGO` voor het doel deze (persoons)gegevens en gezondheidsinformatie in uw persoonlijke gezondheidsomgeving op te nemen.

Korte tekst

U geeft hierbij `NaamZorgaanbieder` toestemming om `NaamGegevensdienst` uit te wisselen met `NaamLeverancierPGO` voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.

Verplicht toestemmingsscherm

De (volledige) toestemmingsverklaring is onderdeel van onderstaand verplichte toestemmingsscherm. De Dienstverlener zorgaanbieder dient dit scherm en de variabelen hierin volgens de instructies bij Gegevens en performance in UCI Verzamelen en UCI Delen te implementeren. De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina (MedMij toestemmings- en bevestigingsscherm.zip).

MedMij
Grip op je eigen gezondheidsgegevens

U geeft hierbij NaamZorgaanbieder 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

☐ Toon uitgebreide toestemmingsverklaring

U geeft hierbij NaamZorgaanbieder 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

☑ Toon uitgebreide 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.

Bevestigingsverklaring

De bevestigingsverklaring is een verplichte tekst 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 UC Delen staat beschreven hoe het proces rondom de bevestiging eruit ziet. De Dienstverlener zorgaanbieder implementeert de bevestigingsverklaring en toont deze aan de Persoon.

Bevestigingsverklaring delen van gegevens met de Zorgaanbieder

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.

Korte tekst

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.

Verplicht bevestigingsscherm

De (volledige) bevestigingsverklaring en de korte tekst zijn onderdeel van een verplicht bevestigingsscherm. De Dienstverlener zorgaanbieder dient dit scherm en de variabelen hierin volgens de instructies bij Gegevens en performance in UCI Verzamelen en UCI Delen te implementeren. De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina (MedMij toestemmings- en bevestigingsscherm.zip).

MedMij
Grip op je eigen 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

☐ Toon uitgebreide 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.

✔ Ja, ik bevestig

Nee, ik bevestig niet

☑ Toon uitgebreide 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.

Managementinformatie

Om het gebruik van MedMij inzichtelijk te maken, leveren deelnemers managementinformatie aan bij de uitvoeringsorganisatie. Deze informatie wordt geaggregeerd tot een managementrapportage voor de stichting. Concurrentiegevoelige informatie wordt hierbij zoveel mogelijk weggehaald.

Van deelnemers wordt verwacht de volgende informatie maandelijks aan te leveren:

Dienstverlener persoon

- Aantal gebruikers;
- Aantal actieve gebruikers: minimaal één keer al dan niet succesvol gegevens hebben opgevraagd;
- Aantal actieve gebruikers: minimaal één keer al dan niet succesvol gegevens hebben gedeeld;
- Per gegevensdienst (indien van toepassing: een gegevensdienst is in de praktijk verbonden aan hetzij UC Verzamelen, hetzij UC Delen):
    - Aantal keer succesvol verzameld (succesvol afgeronde UC Verzamelen);
    - Aantal keer onsuccesvol verzameld (niet afgeronde UC Verzamelen);
    - Aantal keer succesvol gedeeld (succesvol afgeronde UC Delen);
    - Aantal keer onsuccesvol gedeeld (niet afgeronde UC Delen).

Dienstverlener zorgaanbieder

- De reactietijd waarmee de Resource Server de geslaagde en volledige FHIR Responses in de afgelopen periode beschikbaar heeft gesteld (tijdsverschil tussen binnenkomen FHIR Request en beschikbaar stellen FHIR Response).

Release 1.1 versie 0.8

De manier van aanleveren van de reactietijd wordt nog vastgesteld in release 1.1 versie 1.0.

Catalogus

Relatie Catalogus-afsprakenset

De Catalogus is in release 1.1 losgekoppeld van releases van het afsprakenstelsel. Uitbreiding van de Catalogus wordt medio 2018 voorzien. Op deze pagina is nu de Catalogus te vinden zoals die is gepubliceerd samen met release 1.0, toen de Catalogus nog onderdeel was van de afsprakenset.

Meta-informatie

De meta-informatie in onderstaande tabel wordt gevuld bij de publicatie van een zelfstandige Catalogus.

Release catalogus	nvt
Status	nvt
Vastgesteld in bestuur d.d.	nvt
Inwerkingtreding	nvt

Toelichting

De Catalogus bevat de *Gegevensdiensten* die over het MedMij-netwerk kunnen worden aangeboden. De catalogus is weergegeven als een (niet-genormaliseerde) tabel. De structuur van en de relaties tussen begrippen is afgeleid van het Metamodel. Daar zijn ook de geldige waarden en betekenis van enkele algemene concepten te vinden. De *Transacties* waaruit een *TransactieVerzameling* bestaat zijn onderdeel van de *Informatiestandaarden*. Het *Register van Informatiestandaarden* is in een nog niet geformaliseerde vorm te vinden op de MedMij-pagina Informatiestandaarden. Voor informatieve doeleinden bevat de hieronder weergegeven tabel ook enkele klassen uit het *Register van Informatiestandaarden*; deze helpen om de relatie tussen de Catalogus, het *Register van Informatiestandaarden* en de *Zorgaanbiederslijst* inzichtelijk te maken.

Wijzigingen in de Catalogus kunnen op grond van het Gegevensdienstenbeleid plaatsvinden onafhankelijk van releases van het afsprakenstelsel.

GegevensdienstId	Gegevensdienstnaam	Transactieverzameling	Aanvulling, ter informatie (uit Reg Informatiestandaarden)	
		.Transactie[i]. Transactienaam	.Transactie[i]. Informatiestandaard	.Transactie [i]. Systeemrol
1	Basisgegevens zorg	Beschikbaarstellen BgZ	Basisgegevensset Zorg	MM-1.0.0-BZB-FHIR

		Raadplegen BgZ	Basisgegevensset Zorg	MM-1.0.0-BZR-FHIR
2	Medicatieoverzichten	Beschikbaarstellen medicatieoverzicht	Medicatieproces	MP-9.0.4-MOB-FHIR
		Raadplegen medicatieoverzicht	Medicatieproces	MP-9.0.4-MOR-FHIR
3	Medicatiegegevens	Beschikbaarstellen medicatiegegevens	Medicatieproces	MP-9.0.4-MGB-FHIR
		Raadplegen medicatiegegevens	Medicatieproces	MP-9.0.4-MGR-FHIR
4	Laboratoriumresultaten	Beschikbaarstellen laboratoriumresultaten	Labuitwisseling	LAB-1.0.0-LRB-FHIR
		Raadplegen laboratoriumresultaten	Labuitwisseling	LAB-1.0.0-LRR-FHIR
5	Meetwaarden vitale functies	Beschikbaarstellen meetwaarden vitale functies	PLACEHOLDER	MM-1.0.0-MVB-FHIR
		Raadplegen meetwaarden vitale functies	PLACEHOLDER	MM-1.0.0-MVR-FHIR
6	Documenten	Beschikbaarstellen PDF /A metadata lijst	PLACEHOLDER	MM-1.0.0-PLB-FHIR
		Beschikbaarstellen PDF /A	PLACEHOLDER	MM-1.0.0-PDB-FHIR
		Raadplegen PDF/A metadata lijst	PLACEHOLDER	MM-1.0.0-PLR-FHIR
		Raadplegen PDF/A	PLACEHOLDER	MM-1.0.0-PDR-FHIR
7	Afspraken	Beschikbaarstellen afspraak	eAfspraak	EA-1.0.0-AFB-FHIR
		Raadplegen afspraak	eAfspraak	EA-1.0.0-AFR-FHIR