# Aanvullende auditverklaring en onderbouwende rapportage

# Organisatiegegevens

De gegevens van de (aspirant) MedMij deelnemer.

|  |  |
| --- | --- |
| **Naam** |  |
| **Adres** |  |
| **Vertegenwoordigd door** |  |
| **Rol** | DVP/DVZA |

# Certificatiegegevens

De gegevens van het onderliggende NEN 7510-certificaat.

|  |  |
| --- | --- |
| **Norm** | NEN 7510-1:2017 |
| **Scope** |  |
| **Certificaatnummer** |  |
| **Vervaldatum** |  |

# Auditgegevens

Gegevens over de audit.

|  |  |
| --- | --- |
| **CBI** |  |
| **Bezochte locatie(s)** |  |
| **Lead auditor** |  |
| **Overige teamleden** |  |

# Rapport

Gegevens over dit rapport.

|  |  |
| --- | --- |
| **Datum rapport** |  |
| **Status rapport** | Concept/Definitief |
| **Bijlagen bij dit rapport** |  |

# Onderbouwende rapportage

| **Beheersmaatregel** | **DVP** | **DVZA** | **BO** | **Implementatie** | **Voldoet** | **Opmerkingen** |
| --- | --- | --- | --- | --- | --- | --- |
| [A. 5.1.1 Beleidsregels voor informatiebeveiliging](file:///C:\display\PUBLIC\A.+5.1.1+Beleidsregels+voor+informatiebeveiliging) | C:\e3a1ea86ba20bd0eafa1be07310fe1c5 | C:\e3a1ea86ba20bd0eafa1be07310fe1c5 | C:\e3a1ea86ba20bd0eafa1be07310fe1c5 | De beleidsdocumenten MOETEN de beleidsmaatregelen die van toepassing zijn op MedMij (onder andere gespecificeerd in [Privacy- en informatiebeveiligingsbeleid](file:///C:\display\PUBLIC\Privacy-+en+informatiebeveiligingsbeleid)) specifiek benoemen. |  |  |
| [A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging](file:///C:\display\PUBLIC\A.+6.1.1+Rollen+en+verantwoordelijkheden+bij+informatiebeveiliging) | C:\0056c42e72d0810a1578b80fe151956b | C:\0056c42e72d0810a1578b80fe151956b | C:\0056c42e72d0810a1578b80fe151956b | De (eind)verantwoordelijkheid voor informatiebeveiliging MOET belegd zijn. Deze functionaris(sen) dient/dienen mandaat te hebben om bij (een dreiging van) een crisis spoedbesluiten te nemen ten aanzien van MedMij en deze besluiten met spoed te kunnen (laten) realiseren.  De verantwoordelijke en operationele functionaris(sen) (inclusief eventuele onderaannemers) dient/ dienen hiervoor tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur. |  |  |
| [A. 7.2.2 (1) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging](file:///C:\display\PUBLIC\A.+7.2.2+(1)+Bewustzijn,+opleiding+en+training+ten+aanzien+van+informatiebeveiliging) | C:\7b8dc5f1f343274890262538236db0e6 | C:\7b8dc5f1f343274890262538236db0e6 | C:\7b8dc5f1f343274890262538236db0e6 | De verantwoordelijke functionaris(sen) zoals benoemd in [A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging](file:///C:\display\PUBLIC\A.+6.1.1+Rollen+en+verantwoordelijkheden+bij+informatiebeveiliging) MOET(EN) deelgenomen hebben aan de training over de algemene werking van het stelsel. |  |  |
| [A. 7.2.2 (2) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging](file:///C:\display\PUBLIC\A.+7.2.2+(2)+Bewustzijn,+opleiding+en+training+ten+aanzien+van+informatiebeveiliging) | C:\640775a33c9f8fd66af1f9c37e62487e | C:\640775a33c9f8fd66af1f9c37e62487e | C:\640775a33c9f8fd66af1f9c37e62487e | Overige medewerkers die werkzaamheden verrichten gerelateerd aan MedMij MOETEN een training hebben gevolgd over de algemene werking van het stelsel en op de voor hem/haar van toepassing zijnde beveiligingsmaatregelen. |  |  |
| [A. 8.2.1 Classificatie van informatie](file:///C:\display\PUBLIC\A.+8.2.1+Classificatie+van+informatie) | C:\96a02798fe39c06415ff837b6c134fc4 | C:\96a02798fe39c06415ff837b6c134fc4 | C:\96a02798fe39c06415ff837b6c134fc4 | De gegevens die binnen het stelsel worden verwerkt MOETEN worden behandeld conform het Informatieclassificatiebeleid (van MedMij). |  |  |
| [A. 9.1.1 Beleid voor toegangsbeveiliging](file:///C:\display\PUBLIC\A.+9.1.1+Beleid+voor+toegangsbeveiliging) | C:\c6e2a896f28bd4ad1aae88aeed7bfd3e | C:\c6e2a896f28bd4ad1aae88aeed7bfd3e | C:\c6e2a896f28bd4ad1aae88aeed7bfd3e | Er MOETEN technische en organisatorische maatregelen worden genomen om inzage van persoonlijke gezondheidsgegevens door medewerkers te voorkomen. De organisatie dient minimaal elk halfjaar en na grote wijzigingen een self-assessment uit te voeren om vast te stellen dat deze  maatregelen nog effectief zijn.  In (zeer) uitzonderlijke gevallen is inzage in persoonlijke gezondheidsgegevens niet te voorkomen. Hiervoor dient de organisatie een (nood)procedure te documenteren. Deze procedure dient in te gaan op:   * Functiescheiding tussen vragen van toestemming voor inzage en het geven van toestemming door een verantwoordelijke functionaris; * Randvoorwaarden en maatregelen met als doel dat inzage plaatsvindt op een gecontroleerde en zo beperkt mogelijke (in tijd en hoeveelheid gegevens) wijze; * Borging dat de deelnemer voldoet wordt aan wet- en regelgeving (AVG, Meldplicht Datalekken) en de geldende versie van het MedMij Afsprakenstelsel; * Vastlegging en verantwoording van de getroffen acties. |  |  |
| [A. 9.2.5 Beoordeling van toegangsrechten van gebruikers](file:///C:\display\PUBLIC\A.+9.2.5+Beoordeling+van+toegangsrechten+van+gebruikers) | C:\7d6b1dbd76420a44873c1dae9cd3b967 | C:\7d6b1dbd76420a44873c1dae9cd3b967 | C:\7d6b1dbd76420a44873c1dae9cd3b967 | 1. Toegangsrechten die zijn verstrekt op IT-componenten waar persoonlijke gezondheidsgegevens worden worden verwerkt MOETEN ten minste maandelijks worden gecontroleerd. 2. Hierbij MOET functiescheiding gewaarborgd zijn. 3. Dit geldt ook voor eventuele onderaannemers. 4. Tijdens deze controle moet aandacht zijn voor medewerkers die geen gebruik (meer) maken van de toegangsrechten (met aantoonbare opvolging). |  |  |
| [A. 9.4.1 Beperking toegang tot informatie](file:///C:\display\PUBLIC\A.+9.4.1+Beperking+toegang+tot+informatie) | C:\050ddd14e325a139c3ffeb9de5560596 |  |  | Authenticatie van personen (eindgebruikers) MOET plaatsvinden op basis van minimaal twee factoren. Na succesvolle authenticatie krijgen personen alleen toegang tot hun eigen persoonlijke gezondheidsgegevens of de gegevens van de vertegenwoordigde.  Scope: Dit geldt voor het gehele MedMij PGO en voor alle gebruikers die hier toegang toe krijgen. Dit is onafhankelijk of deze gebruikers MedMij uitwisselingen gebruiken of niet.  Naast SMS MOET een deelnemer ook een sterkere tweede factor aanbieden. De Persoon bepaalt zelf welke tweede factor wordt gebruikt. |  |  |
| [A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen](file:///C:\display\PUBLIC\A.10.1.1+Beleid+inzake+het+gebruik+van+cryptografische+beheersmaatregelen) | C:\35e0eea0f228f0fcca9c1bfc8e5158d8 | C:\35e0eea0f228f0fcca9c1bfc8e5158d8 |  | Opgeslagen persoonlijke gezondheidsgegevens MOETEN beschermd worden door middel van encryptie. Hiervoor wordt verwezen naar de aanbevelingen die gelden voor 'near term protection' en 'long-term protection' in de aanbevelingen, zie <https://www.keylength.com/>. |  |  |
| [A.12.1.2 (1) Wijzigingsbeheer](file:///C:\display\PUBLIC\A.12.1.2+(1)+Wijzigingsbeheer) | C:\3494aab6c91d74875e90df124187e764 | C:\3494aab6c91d74875e90df124187e764 | C:\3494aab6c91d74875e90df124187e764 | De IT-beheerprocessen MOETEN aansluiten op het MedMij Change- en releasebeleid. |  |  |
| [A.12.1.2 (2) Wijzigingsbeheer](file:///C:\display\PUBLIC\A.12.1.2+(2)+Wijzigingsbeheer) | C:\314fb451f75be3d41f826c46d8d0780f | C:\314fb451f75be3d41f826c46d8d0780f | C:\314fb451f75be3d41f826c46d8d0780f | Niet-standaard wijzigingen op de IT componenten die gebruikt worden binnen de scope van MedMij MOETEN op basis van het vier-ogen-principe worden uitgevoerd. |  |  |
| [A.12.1.2 (3) Wijzigingsbeheer](file:///C:\display\PUBLIC\A.12.1.2+(3)+Wijzigingsbeheer) | C:\cc175962817d638429ccb32c0d61b16a | C:\cc175962817d638429ccb32c0d61b16a | C:\cc175962817d638429ccb32c0d61b16a | Indien er wijzigingen plaatsvinden die mogelijk significante impact hebben op de informatiebeveiliging, MOET de penetratietest zoals benoemd in [A.18.2.3 (1) Beoordeling van technische naleving](file:///C:\display\PUBLIC\A.18.2.3+(1)+Beoordeling+van+technische+naleving) voor deze componenten opnieuw uitgevoerd worden. |  |  |
| [A.12.1.3 (1) Capaciteitsbeheer](file:///C:\display\PUBLIC\A.12.1.3+(1)+Capaciteitsbeheer) | C:\ee5ebb37fd4d4f4e54e793b7b6aad760 | C:\ee5ebb37fd4d4f4e54e793b7b6aad760 |  | Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in [Token interface](file:///C:\display\PUBLIC\Token+interface) en [Resource interface](file:///C:\display\PUBLIC\Resource+interface). |  |  |
| [A.12.1.3 (2) Capaciteitsbeheer](file:///C:\display\PUBLIC\A.12.1.3+(2)+Capaciteitsbeheer) |  |  | C:\ee5ebb37fd4d4f4e54e793b7b6aad760 | Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in [GNL-, OCL- en ZAL-interface](file:///C:\display\PUBLIC\GNL-,+OCL-+en+ZAL-interface). |  |  |
| [A.12.3.1 Back-up van informatie](file:///C:\display\PUBLIC\A.12.3.1+Back-up+van+informatie) | C:\204721dbb1341ab4fb172d6a90e75c2f |  |  | Er MOETEN maatregelen zijn geïmplementeerd waardoor het gegevensverlies van persoonlijke gezondheidsinformatie maximaal 24 uur bedraagt. Daarnaast moet een herstelprocedure zijn ingericht waardoor de gegevens van een persoon binnen 24 uur terug kunnen worden geplaatst in geval van een incident. Deze herstelprocedure wordt minimaal jaarlijks getest. |  |  |
| [A.12.4.1 Gebeurtenissen registreren](file:///C:\display\PUBLIC\A.12.4.1+Gebeurtenissen+registreren) | C:\86bd67524f522f86f9449a4aee45d126 | C:\86bd67524f522f86f9449a4aee45d126 |  | Logging MOET plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie [Processen en informatie](file:///C:\display\PUBLIC\Processen+en+informatie) onder Logging)  Daarnaast MOETEN de volgende acties ten minste 12 maanden onweerlegbaar en controleerbaar worden gelogd:   * De actie waarbij de persoon via de DVP bij de DVZA gegevens wil opvragen * De acties waarbij de persoon toestemming geeft voor de uitwisseling conform de specificaties in het afsprakenstelsel (indien uitgevoerd onder verantwoordelijkheid van de DVZA) |  |  |
| [A.12.4.3 Logbestanden van beheerders en operators](file:///C:\display\PUBLIC\A.12.4.3+Logbestanden+van+beheerders+en+operators) | C:\45a613a0042979a9cb2ac6a6ca7b880f | C:\45a613a0042979a9cb2ac6a6ca7b880f |  | 1. Het gebruik van toegangsrechten op IT-componenten waar persoonlijke gezondheidsgegevens worden verwerkt MOET worden gelogd; 2. Deze logging MOET ten minste maandelijks worden gecontroleerd. Dit geldt ook voor eventuele onderaannemers; 3. Hierbij MOET functiescheiding gewaarborgd zijn; 4. Tijdens deze controle moet aandacht zijn voor onterecht/onnodig gebruik door medewerkers (met aantoonbare opvolging). |  |  |
| [A.12.4.4 Kloksynchronisatie](file:///C:\display\PUBLIC\A.12.4.4+Kloksynchronisatie) | C:\d04bb82f730804fc1231b72ee5ab0c82 | C:\d04bb82f730804fc1231b72ee5ab0c82 | C:\d04bb82f730804fc1231b72ee5ab0c82 | De klokken van IT componenten die communiceren via MedMij en logging in het kader van MedMij bijhouden, MOETEN worden gesynchroniseerd met [pool.ntp.org](https://pool.ntp.org).  Het is toegestaan te synchroniseren met een alternatieve NTP-server, wanneer maatregelen zijn getroffen om de afwijking met [pool.ntp.org](https://pool.ntp.org) niet groter dan plus of min 500 ms te laten zijn. |  |  |
| [A.12.6.1 Beheer van technische kwetsbaarheden](file:///C:\display\PUBLIC\A.12.6.1+Beheer+van+technische+kwetsbaarheden) | C:\a18c3e6d5ba54e2244ff5002ec829fc5 | C:\a18c3e6d5ba54e2244ff5002ec829fc5 | C:\a18c3e6d5ba54e2244ff5002ec829fc5 | De processen MOETEN aansluiten op de [Operationele processen](file:///C:\display\PUBLIC\Operationele+processen) in het afsprakenstelsel ten aanzien van het beheer van technische kwetsbaarheden.  Dit dient te omvatten:   * Identificeren van kwetsbaarheden in de eigen technologie, onderzoeken van relevantie van door de beheerorganisatie geïdentificeerde kwetsbaarheden + terugkoppeling naar de beheerorganisatie hieromtrent; * Het patchen van systemen of anderzijds mitigeren van de kwetsbaarheid; * Het tijdig kunnen doorlopen van de gehele procedure bij hoog risico-kwetsbaarheden. |  |  |
| [A.14.2.1 Beleid voor beveiligd ontwikkelen](file:///C:\display\PUBLIC\A.14.2.1+Beleid+voor+beveiligd+ontwikkelen) |  | C:\42520d1122417db5adb60064f2d5ba99 | C:\42520d1122417db5adb60064f2d5ba99 | Bij het vaststellen voor het beleid voor beveiligd ontwikkelen MOETEN de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC uit het "Uitvoeringsdomein" overwogen worden (<https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties>).  Voor mobiele applicaties MOETEN de Beveiligingsrichtlijnen voor mobiele applicaties van het NCSC overwogen worden (<https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beveiligingsrichtlijnen-voor-mobiele-apparaten>). |  |  |
| [A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten](file:///C:\display\PUBLIC\A.15.1.2+Opnemen+van+beveiligingsaspecten+in+leveranciersovereenkomsten) | C:\42520d1122417db5adb60064f2d5ba99 | C:\42520d1122417db5adb60064f2d5ba99 | C:\42520d1122417db5adb60064f2d5ba99 | Organisaties MOETEN relevante MedMij beheersmaatregelen contractueel beleggen bij hun leveranciers. |  |  |
| [A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers](file:///C:\display\PUBLIC\A.15.2.1+Monitoring+en+beoordeling+van+dienstverlening+van+leveranciers) | C:\42520d1122417db5adb60064f2d5ba99 | C:\42520d1122417db5adb60064f2d5ba99 | C:\42520d1122417db5adb60064f2d5ba99 | Organisaties MOETEN toezien op correcte naleving van de relevante MedMij beheersmaatregelen die bij een leverancier belegd zijn. |  |  |
| [A.16.1.1 Verantwoordelijkheden en procedures](file:///C:\display\PUBLIC\A.16.1.1+Verantwoordelijkheden+en+procedures) | C:\42520d1122417db5adb60064f2d5ba99 | C:\42520d1122417db5adb60064f2d5ba99 | C:\42520d1122417db5adb60064f2d5ba99 | De processen voor het behandelen van incidenten en calamiteiten moeten aansluiten op de [Operationele processen](file:///C:\display\PUBLIC\Operationele+processen) in het afsprakenstelsel. |  |  |
| [A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging](file:///C:\display\PUBLIC\A.16.1.3+Rapportage+van+zwakke+plekken+in+de+informatiebeveiliging) | C:\42520d1122417db5adb60064f2d5ba99 | C:\42520d1122417db5adb60064f2d5ba99 | C:\42520d1122417db5adb60064f2d5ba99 | Kwetsbaarheden en incidenten die betrekking hebben op persoonlijke gezondheidsgegevens of het functioneren van het MedMij stelsel MOETEN binnen 48 uur gemeld te worden bij het centrale incident management team. Zie [Deelnemersovereenkomsten](file:///C:\display\PUBLIC\Deelnemersovereenkomsten).  DVZA maken hierover zonodig afspraken met de aangesloten ZA's. |  |  |
| [A.16.1.7 Verzamelen van bewijsmateriaal](file:///C:\display\PUBLIC\A.16.1.7+Verzamelen+van+bewijsmateriaal) | C:\42520d1122417db5adb60064f2d5ba99 | C:\42520d1122417db5adb60064f2d5ba99 | C:\42520d1122417db5adb60064f2d5ba99 | Medewerking MOET worden verleend aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties.  DVZA maken hierover zonodig afspraken met de aangesloten ZA's. |  |  |
| [A.18.2.3 (1) Beoordeling van technische naleving](file:///C:\display\PUBLIC\A.18.2.3+(1)+Beoordeling+van+technische+naleving) | C:\42520d1122417db5adb60064f2d5ba99 | C:\42520d1122417db5adb60064f2d5ba99 |  | Tenminste jaarlijks MOET een whitebox applicatiepenetratietesten worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie.  De volgende specifieke MedMij eisen moeten ook aantoonbaar getoetst zijn in de pentest rapportage;   * DNSSEC zie [core.dns.300](https://afsprakenstelsel.medmij.nl/display/MMOntwikkeling/.Verantwoordelijkheden%2C+Core+v1.6.0#id-.Verantwoordelijkheden,Corev1.6.0-core.dns.300) en  [core.dns.301](https://afsprakenstelsel.medmij.nl/display/MMOntwikkeling/.Verantwoordelijkheden%2C+Core+v1.6.0#id-.Verantwoordelijkheden,Corev1.6.0-core.dns.301) * TLS zie verantwoordelijkheid [core.tls.301](https://afsprakenstelsel.medmij.nl/display/MMOntwikkeling/.Verantwoordelijkheden%2C+Core+v1.6.0#id-.Verantwoordelijkheden,Corev1.6.0-core.tls.301) in combinatie met [core.tls.302](https://afsprakenstelsel.medmij.nl/display/MMOntwikkeling/.Verantwoordelijkheden%2C+Core+v1.6.0#id-.Verantwoordelijkheden,Corev1.6.0-core.tls.302) en [core.tls.304](https://afsprakenstelsel.medmij.nl/display/MMOntwikkeling/.Verantwoordelijkheden%2C+Core+v1.6.0#id-.Verantwoordelijkheden,Corev1.6.0-core.tls.304) * NCSC webapplicatie richtlijnen U/PW.02, U/PW.03, U/WA.03, U/WA.04 NB deze zijn voor DigiD assessments al verplicht. Zie NOREA Handreiking DigiD assessments   **Voor toetreding** heeft deze minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost.  Voor penetratietesten die worden uitgevoerd na toetreding, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's (CVSS-score (Common Vulnerability Scoring System) van 4,0 of hoger) ten aanzien van de MedMij dienstverlening. Dit actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd. |  |  |
| [A.18.2.3 (2) Beoordeling van technische naleving](file:///C:\display\PUBLIC\A.18.2.3+(2)+Beoordeling+van+technische+naleving) |  |  | C:\42520d1122417db5adb60064f2d5ba99 | Tenminste jaarlijks MOET een greybox applicatiepenetratietest worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie.  *De externe koppelvlakken zijn:*   * *DVP: Burgerfrontend, OAuth Client Redirect* * *DVA: Resourceserver koppelvlak, Autorization server interface(s) eindgebruiker en voor de DVP.* * *BO:  Stelselnode en administratieve front-end*   ***Voor toetreding****heeft een whitebox applicatiepentratietest minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost.*  ***Bij grootschalige wijziging of herbouw*** *vereisen eenmalig een whitebox applicatiepenetratietest.*  Voor penetratietesten die worden uitgevoerd **na toetreding**, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's ten aanzien van de MedMij dienstverlening. Dit actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd. |  |  |

# Ondertekening

Hierbij verklaren ondergetekenden (auditor en vertegenwoordiger CBI) dat bovengenoemde Organisatie **wel/niet** voldoet aan het aanvullend normenkader informatiebeveiliging van de hieronder genoemde versie van het MedMij Afsprakenstelsel, zoals door Stichting MedMij is uitgegeven.

(Versie van het afsprakenstelsel)

(Naam auditor, datum, handtekening)

(Naam vertegenwoordiger CBI, datum, handtekening)