Rapport

MedMij
Grip op je eigen gezondheidsgegevens

1

Consultatiedocument MedMij-basiseisen

MedMij-afsprakenstelsel

Auteur	MedMij
Versie	v1.0 voor openbare consultatie
Datum	20 december 2016

Dit consultatiedocument is het vertrekpunt voor de consultatie over de basiseisen voor persoonlijke gezondheidsomgevingen en ICT-systemen die aan willen sluiten op het MedMij-netwerk.

MedMij

Grip op je eigen gezondheidsgegevens

Inhoudsopgave

1. Inleiding

1.1 Doel van dit document

Partijen die gegevens willen uitwisselen moeten afspraken maken met elkaar die veelal worden vastgelegd in overeenkomsten en convenanten. Dit betreffen afspraken over de wijze van samenwerking, over de informatie die gedeeld wordt met elkaar en over de manier hoe gegevens worden uitgewisseld, via welke kanalen en hoe vaak. Zo moeten op alle niveaus van interoperabiliteit afspraken worden gerealiseerd.

Voor een persoonlijke gezondheidsomgeving is gegevensuitwisseling essentieel, relevante gezondheidsgegevens verzamelen en delen is onderdeel van de definitie om als persoon regie te verkrijgen over je eigen gezondheid. Leveranciers van een persoonlijke gezondheidsomgeving zouden daarom afspraken moeten maken met een groot aantal zorgaanbieders en overheden voor het verkrijgen en beschikbaar stellen van gegevens. Het afsprakenstelsel moet daarin helpen. Het afsprakenstelsel wil juist voorkomen dat een leverancier van een persoonlijke gezondheidsomgeving met alle zorgaanbieders en overheden overeenkomsten moet afsluiten.

Dit document heeft als doel de context en het bereik van het afsprakenstelsel te beschrijven, de organisatie en het ontwerp van het afsprakenstelsel te schetsen en een beschrijving van de afspraken zelf te geven. De afspraken moeten worden gerealiseerd tussen enerzijds leveranciers van persoonlijke gezondheidsomgevingen en anderzijds zorgaanbieders, overheden en zorgverzekeraars. Het zijn dus geen afspraken met individuele personen, ook al is MedMij gepositioneerd om het voor personen mogelijk te maken om gegevens te verzamelen en te delen. Personen moeten hiervoor echter gebruik maken van de diensten van een leverancier van een persoonlijke gezondheidsomgeving.

Dit document is met name bedoeld voor partijen die een rol in het afsprakenstelsel willen vervullen en diensten willen aanbieden voor het uitwisselen van gezondheidsgegevens. Maar ook partijen die gebruik willen maken van het afsprakenstelsel kunnen via dit document meer te weten komen over de werking van het stelsel.

1.1. Structuur en gehanteerde methode

Het document bevat de structuur zoals hieronder beschreven.

1. Hoofdstuk 2 behandelt de problemen in de huidige situatie, problemen die tot op heden een barrière vormen om te komen tot gegevensuitwisseling tussen zorgaanbieders en overheden enerzijds en een persoonlijke gezondheidsomgeving anderzijds.
2. In hoofdstuk 3 zijn de doelstellingen beschreven van MedMij.
3. Hoofdstuk 4 beschrijft de principes die voor het afsprakenstelsel worden gehanteerd.
4. Hoofdstuk 5 richt zich op de eisen en randvoorwaarden voor de organisatie en inrichting van het afsprakenstelsel;

5. De hoofdstukken 6, 7 en 8 beschrijven de aannames en eisen en uiteindelijk de afspraken die met het afsprakenstelsel moeten worden gerealiseerd;
6. Bijlage 1 bevat een lijst van referenties naar bronnen die gebruikt zijn in dit document.

Dit document beschrijft stellingen niet als voldongen feit, maar benadert een stelling als een aanname. Het document bevat daarom veel zinnen met aannames. De aannames zijn een rationale voor eisen, een reden waarom een eis wordt opgenomen. Eisen vormen weer de reden waarom daadwerkelijke afspraken gemaakt worden. Afspraken die onderdeel zullen zijn van het afsprakenstelsel.

1.2. Totstandkoming

De afspraken beschreven in dit document zijn voortgekomen uit een proces van co-creatie:

- Gesprekken met mensen die bezig zijn met hun gezondheid;
- Gesprekken met marktpartijen;
- Expertsessies met experts uit het gehele gezondheidsdomein;
- Werkgroepbijeenkomsten met experts van leveranciers van XIS-en, persoonlijke gezondheidsomgevingen en uitwisselingsinfrastructuren.

Alleen met hun medewerking is het mogelijk geweest dit document op te stellen, waarvoor veel dank!

De afspraken komen voor een deel voort uit bestaande sets van afspraken, zoals die van Zelfzorg Ondersteund (ZO!) [1] en van het Landelijk schakelpunt (LSP) [2].

1.3. Documentbeheer

In deze versie van het document zijn de volgende onderwerpen gerealiseerd:

1. De afspraken in dit document zijn gericht op de afspraken voor gegevensuitwisseling ten behoeve van de inzage van gegevens afkomstig vanuit een professioneel medisch informatiesysteem en het delen van gegevens vanuit een persoonlijke gezondheidsomgeving met derden.

In dit document wordt met name de term “zorgaanbieder” gehanteerd omdat in deze versie van het document de aandacht ligt op gegevensuitwisseling met zorgaanbieders. Voor de realisatie van het afsprakenstelsel zal echter ook rekening gehouden moeten worden met andere partijen zoals overheden en zorgverzekeraars. In het document kan daarom de term zorgaanbieder ook gelezen worden als overheid en zorgverzekeraar.

Deze versie van het document geeft een weergave van de aannames, eisen en afspraken zoals deze in 2016 tot stand zijn gekomen, en is een momentopname om de kennis, ideeën en beelden over de werking van het afsprakenstelsel vast te leggen. Het document heeft de status van openbare consultatie meegekregen zodat in 2017 met belanghebbenden en betrokkenen verder gewerkt kan worden aan een eerste versie van de afspraken.

1.3.1. Voorgaande versies

De afspraken 2016 is de eerste versie van MedMij.

1.3.2. Werklijst voor opname in toekomstige versies

Er zijn op het moment van verschijnen van dit document nog geen definitieve keuzes gemaakt voor onderwerpen met betrekking tot toekomstige versies.

2. Achtergrond en probleemanalyse

De Patiëntenfederatie Nederland zet zich al jaren in voor de bevordering van zelfmanagement en eHealth voor patiënten. Patiënten, of personen in het algemeen, willen zelf meer sturing geven aan hun gezondheid en de zorg en ondersteuning die zij ontvangen. Een persoonlijke gezondheidsomgeving is een van de belangrijkste hulpmiddelen om invulling te kunnen geven aan zelfsturing volgens de visie van de Patiëntenfederatie Nederland [3].

Wat is een persoonlijke gezondheidsomgeving?
De onderstaande definitie wordt, overeenkomstig de visie van de Patiëntenfederatie Nederland, gehanteerd voor het afsprakenstelsel.

Een persoonlijke gezondheidsomgeving:

- Is een universeel toegankelijk, voor leken begrijpelijk, gebruiksvriendelijk en levenslang hulpmiddel om:
  - Relevante gezondheidsgegevens te verzamelen, te beheren en te delen;
  - Regie te kunnen nemen over gezondheid en zorg;
  - Zelfmanagement te ondersteunen via gestandaardiseerde gegevensverzamelingen voor gezondheidsgegevens en geïntegreerde digitale zorgdiensten.
- Wordt beheerd en/of gedeeld door de persoon 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.

Een persoonlijke gezondheidsomgeving is met andere woorden een digitale omgeving die je in staat stelt om al je relevante gezondheidsgegevens, die verspreid staan opgeslagen bij zorgaanbieders en overheden, overzichtelijk en veilig in te zien, aan te vullen met zelf gegenereerde gegevens en te delen met wie je dat wilt.

Grootschalige implementatie blijft nog achterwege
Maar grootschalige implementatie van persoonlijke gezondheidsomgevingen blijft echter achterwege door een aantal barrières die opschaling in de weg staan met als gevolg een terughoudendheid van investeringen. Deze barrières zijn onder meer te herleiden naar onduidelijkheid en vragen met betrekking tot het medisch geheim en aansprakelijkheid en technische vraagstukken omtrent interoperabiliteit en authenticatie. De kwaliteit van de huidige persoonlijke gezondheidsomgevingen is niet als probleem gesignaleerd.

2.1. Vragen met betrekking tot medisch geheim en aansprakelijkheid

Er zijn juridische vraagstukken over het delen van medische gegevens door zorgaanbieders en het verkrijgen van gegevens van personen. Vraagstukken met betrekking tot het medisch geheim, medische aansprakelijkheid, goed hulpverlenerschap en de manier waarop wet- en regelgeving hieromtrent moet worden geïnterpreteerd.

Zorgaanbieders zijn door deze vraagstukken terughouden in het delen van gegevens via een persoonlijke gezondheidsomgeving. De gegevens komen namelijk niet alleen terecht bij een persoon, maar ook bij de leverancier van de persoonlijke gezondheidsomgeving. Zorgaanbieders willen graag duidelijkheid of dat is toegestaan en onder welke voorwaarden dat is toegestaan. Daarnaast willen zorgaanbieders graag zekerheid over de vraag in welke mate zij aansprakelijk gesteld kunnen worden bij medische schade die het gevolg is van gegevens uit een persoonlijke gezondheidsomgeving. En wat van een zorgaanbieder verwacht kan en moet worden als deze gegevens ontvangt vanuit een persoonlijke gezondheidsomgeving in het kader van goed hulpverlenerschap.

2.2. Beschikbaarheid van betrouwbare authenticatiemiddelen

Voor zorgaanbieders spelen ook onzekerheden een rol over de mogelijkheid om te voldoen aan de wettelijke eisen rond gegevensbescherming. Zo zijn er nauwelijks generieke authenticatievoorzieningen beschikbaar die voldoende sterk zijn om personen te identificeren met een hoog betrouwbaarheidsniveau.

2.3. Randvoorwaarden voor interoperabiliteit zijn niet ingevuld

Voor zowel de leveranciers van persoonlijke gezondheidsomgevingen als voor zorgaanbieders speelt eveneens de onzekerheid over interoperabiliteit. Bij gebrek aan standaardisatie en de complexiteit van interoperabiliteit met veel partijen, zijn investeringskeuzes risicovol. In de volgende paragrafen is een aantal thema's benoemd die als belemmerend zijn geïdentificeerd.

2.3.1. Gebrek aan standaarden en afspraken

De huidige persoonlijke gezondheidsomgevingen hebben beperkte integratiemogelijkheden met zorgaanbieders, als er al integratie aanwezig is. Integratie is lastig te realiseren omdat standaarden veelal ontbreken en als er al standaarden zijn, dan zijn deze niet altijd uitwisselbaar met elkaar. Daarom blijven huidige oplossingen voor een persoonlijke gezondheidsomgevingen beperkt in gebruik. Samenvattend kunnen de volgende oorzaken worden genoemd:

- De oplossing richt zich op één aspect van de gezondheid, is niet opgezet vanuit het perspectief van de persoon, maar vanuit de faciliterende organisatie (voorbeeld: ziekenhuisportalen);
- Gebrek aan gegevensstandaarden voor uitwisseling;
- Gebrek aan standaarden en afspraken hoe gegevens vanuit verschillende bronnen uitwisselbaar kunnen worden gemaakt, bronnen die veelal hun eigen terminologie en werkwijze hanteren (bijvoorbeeld laboratoriumuitslagen van een streeklaboratorium, van het ziekenhuis en eigen metingen).

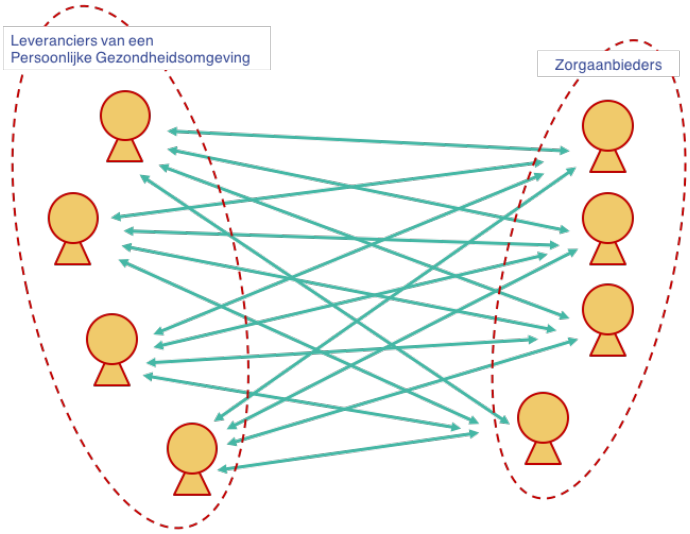
2.3.2. Beperkte beschikbaarheid van gegevens (ontsluiten van gegevens)

Voor een goed overzicht over de eigen gezondheid zijn gegevens nodig vanuit alle zorgaanbieders waarmee de persoon te maken heeft. Het gaat hierbij om zowel gegevens die voor computersystemen betekenisvol (gestructureerd) kunnen worden uitgewisseld als betekenisloos (ongestructureerd). Hoewel zorgaanbieders steeds vaker medische gegevens digitaal beschikbaar stellen, is dit nog niet overal het geval. Het ontsluiten van gegevens uit oude en veelal monolithische

systemen van zorgaanbieders is complex, en zorgt ervoor dat bijvoorbeeld de elektronische overdracht van gestructureerde (betekenisvol) gegevens nog in de beginfase verkeert. Zorgaanbieders hebben daarnaast ook veelal een applicatie- en gegevenslandschap die versplinterd is. Een 'virtueel' patiëntendossier met een afdoende datakwaliteit is lang niet altijd aanwezig. Een andere oorzaak is dat gegevens nog veelal ongestructureerd worden opgeslagen in tekstvelden, waardoor het gestructureerd uitwisselen van gegevens wordt bemoeilijkt. Hoge investeringen zijn waarschijnlijk noodzakelijk om gegevens te ontsluiten en betekenisvol vast te leggen.

2.3.3. Complexiteit en omvang van afspraken maken met relevante partijen

Voor elektronische gegevensuitwisseling moet een leverancier van persoonlijke gezondheidsomgevingen veel afspraken realiseren. Afspraken met een groot aantal zorgaanbieders en met de softwareleveranciers van deze zorgaanbieders. Er moeten bijvoorbeeld afspraken worden gemaakt over verantwoordelijkheden, over rechten en plichten, over bedrijfs- en werkprocessen, over de te hanteren gegevensstandaarden, techniek en de maatregelen voor de bescherming van persoonsgegevens. Afspraken op alle interoperabiliteitsniveaus die vastgelegd moeten worden in contracten en convenanten.



Afbeelding 1 Het veel-op-veel-probleem voor het realiseren van afspraken

Het realiseren en implementeren van alle afspraken is complex en kostbaar. Voor zorgaanbieders is het niet mogelijk om dezelfde afspraken met alle leveranciers te realiseren, net als het voor leveranciers van persoonlijke gezondheidsomgevingen niet mogelijk is om standaarden voor alle zorgaanbieders af te spreken. Dit vereist een landelijke aanpak om alle partijen bij elkaar te brengen.

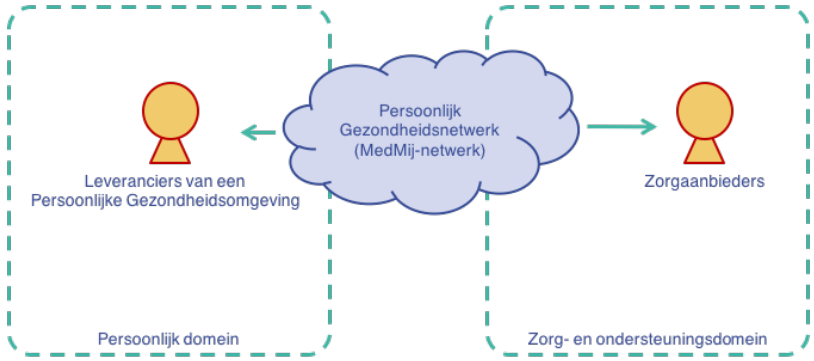
2.4. Financiering

Tot slot is er onduidelijkheid over de financiering van functionaliteiten van een persoonlijke gezondheidsomgeving en de daaraan gerelateerde diensten. Het is niet helder op welke wijze investeringen worden terugverdiend.

Voor het realiseren en implementeren van gegevensuitwisseling zijn voorzieningen en oplossingen nodig die niet altijd haalbaar gefinancierd kunnen worden door een individuele zorgaanbieder of door een leverancier van een persoonlijke gezondheidsomgeving. Oorzaak hiervan kan gevonden worden in het feit dat opbrengsten en kosten niet altijd bij dezelfde partij ligt. En soms zijn opbrengsten alleen op macroniveau aanwezig als maatschappelijk opbrengsten. Financiering en haalbaarheid moet dan ook gezamenlijk beoordeeld worden.

3. Doelstellingen

Het afsprakenstelsel heeft als doel om afspraken vast te leggen voor het uitwisselen van aan gezondheid gerelateerde gegevens. Een persoon is hierdoor in staat is om relevante gezondheidsgegevens te verzamelen en te delen met behulp van een persoonlijke gezondheidsomgeving. De afspraken moeten ervoor zorgen dat barrières worden weggenomen en dat gezondheidsgegevens kunnen worden uitgewisseld.



Afbeelding 2 Context van het MedMij-netwerk

Het domein waarover de afspraken worden gemaakt wordt het persoonlijke gezondheidsnetwerk genoemd, oftewel het MedMij-netwerk. Het MedMij-netwerk is het onderwerp van de afspraken in het afsprakenstelsel met als doel te komen tot gegevensuitwisseling tussen de gebruikers van het netwerk. In eerste instantie zijn de leveranciers van een persoonlijke gezondheidsomgeving en zorgaanbieders de gebruikers van het netwerk.

3.1. Realisatie van juridisch kader

Met juridische kaders wordt de relevante wet- en regelgeving bedoeld en de interpretatie die hieraan wordt gegeven. Deze kaders zijn van belang gezien de huidige vraagstukken, bijvoorbeeld de vraagstukken met betrekking tot het medisch geheim en aansprakelijkheid. De juridische kaders worden niet in dit document beschreven, maar worden uitgewerkt door een juridische werkgroep van het Ministerie van Volksgezondheid, Welzijn en Sport (VWS). De resultaten van de juridische werkgroep zijn opgenomen in het document juridische aspecten [4].

De resultaten van de juridische werkgroep heeft gevolgen voor de afspraken over de werking en het gebruik van het stelsel, over de manier waarop de gegevensuitwisseling tot stand kan worden gebracht. Deze impact zal in dit document worden beschreven.

3.2. Realisatie van afspraken voor gegevensuitwisseling

Een van de huidige barrières is dat de randvoorwaarden voor interoperabiliteit niet zijn ingevuld. Het doel van het afsprakenstelsel is om juiste deze randvoorwaarden in te vullen en afspraken te realiseren waar deze nodig zijn om de markt haar werk te kunnen laten doen. In deze paragraaf wordt een opsomming gegeven van de behoefte aan afspraken voor gegevensuitwisseling.

3.2.1. Integriteit en herkomst van medische gegevens

De medische gegevens in een persoonlijke gezondheidsomgeving moeten kunnen worden vertrouwd en op waarde kunnen worden geschat door zorgaanbieders die gebruik willen maken van de gegevens. Met integriteit wordt een mate van zekerheid gevraagd dat gegevens niet zijn gewijzigd. Ook de herkomst van de gegevens moet onweerlegbaar zijn. Het moet met andere woorden met een hoge mate van zekerheid kunnen worden bewezen dat de gegevens afkomstig zijn van een zorgaanbieder.

Naast de betrouwbaarheid van de gegevens is de integriteit en herkomst ook van belang vanuit het oogpunt van medische aansprakelijkheid. Zorgaanbieders kunnen alleen aansprakelijk zijn voor gegevens waarvan de integriteit en herkomst onweerlegbaar is.

3.2.2. Vertrouwelijkheid gegevensuitwisseling

Het afsprakenstelsel moet afspraken realiseren voor passende maatregelen om de vertrouwelijkheid van de gegevensuitwisseling te borgen. De gegevensuitwisseling bevat persoonsgegevens van bijzondere aard, namelijk medische gegevens die mogelijk herleid kunnen worden naar de persoon op wie het betrekking heeft. De vertrouwelijkheid omvat de maatregelen voor de bescherming van de persoonsgegevens en is een vereiste.

3.2.3. Gebruik van standaarden

Met het afsprakenstelsel moeten keuzes voor standaarden worden gerealiseerd. Dit betreft zowel standaarden voor gegevensverzamelingen als standaarden voor de technieken die gebruikt worden voor gegevensuitwisseling.

3.2.4. Betrouwbare authenticatiemiddelen

Het afsprakenstelsel moet afspraken realiseren voor een lijst van betrouwbare authenticatiemiddelen die gehanteerd kunnen worden door zorgaanbieders. Zorgaanbieders en andere organisaties werkzaam in het domein van de zorg en ondersteuning moeten de mogelijkheid hebben te kiezen voor een authenticatiemiddel (bijvoorbeeld iDIN of Idensys).

Zorgaanbieders moeten kunnen kiezen voor een authenticatiemiddel die het hoogste niveau van zekerheid biedt en het burgerservicenummer kan leveren op basis van de vastgestelde identiteit.

3.2.5. Catalogus van gegevensdiensten

Het afsprakenstelsel moet afspraken realiseren voor gegevensdiensten die betrekking hebben op zowel het verkrijgen van gegevens als het beschikbaar stellen van gegevens aan anderen. Personen moeten gegevens kunnen verkrijgen en delen met zorgaanbieders, maar moeten ook gegevens kunnen delen met andere personen.

De beschikbare gegevensdiensten moeten een MedMij-catalogus vormen. Een zorgaanbieder moet expliciet aangeven welke gegevensdiensten uit de MedMij-catalogus deze ondersteunt evenals een leverancier van een persoonlijke gezondheidsomgeving. Een zorgaanbieder zal echter niet alle gegevensdiensten kunnen ondersteunen. Zo zal een apotheker waarschijnlijk geen laboratoriumwaarden als gegevensdienst opnemen.

3.3. Onderzoek financiële haalbaarheid en afspraken over financiering

De financiële haalbaarheid voor de implementatie van het afsprakenstelsel is onderwerp van onderzoek. Het is op het moment van schrijven niet bekend of afspraken over financiering een onderdeel zijn van het afsprakenstelsel.

4. Principes

Voor het realiseren van het afsprakenstelsel is een aantal aannames gedaan die als principes voor het ontwerp van de oplossing en de daaraan gerelateerde afspraken worden gehanteerd. In de onderstaande paragrafen zijn deze beschreven.

4.1. Persoon heeft regierol

Het initiatief voor gegevensuitwisseling met een persoonlijke gezondheidsomgeving ligt bij de persoon als gebruiker van de omgeving. De persoon neemt het initiatief om vanuit de persoonlijke gezondheidsomgeving via MedMij de zorgaanbieder te benaderen en gegevens op te halen. Ook voor het verkrijgen van updates en nieuwe gegevens van de zorgaanbieder ligt het initiatief (al dan niet geautomatiseerd) bij de persoon om dit van de zorgaanbieder te vragen.

Een keuze voor het initiatief ligt in lijn met de juridische benadering voor de aansprakelijkheid van de arts in de verwerking van data, dat daarmee “goed hulpverlenerschap” kan volgen. In het kader van “goed hulpverlenerschap” kan namelijk de verwachting bestaan dat zorgaanbieders een persoonlijke gezondheidsomgeving moeten raadplegen als deze is verbonden met het elektronisch patiëntendossier van de zorgaanbieder. Vanuit het juridisch kader is aangegeven dat het initiatief voor delen bij de persoon ligt en de verplichting om de persoonlijke gezondheidsomgeving te raadplegen voor zorgaanbieders niet bestaat.

4.2. Gebruik van internationale open standaarden en profielen

Voor het vaststellen van de gehanteerde standaarden en profielen in het afsprakenstelsel zal zoveel mogelijk gebruik worden gemaakt van (nationale extensies van) open internationale standaarden en profielen. Tegelijkertijd wordt rekening gehouden met reeds bestaande en breed geïmplementeerde oplossingen.

4.3. Diensten voor gegevensuitwisseling worden concurrentieel aangeboden

In de afwegingen voor het afsprakenstelsel is ook overwogen om een platform te realiseren. Een platform is een model waarbij één partij alle diensten levert voor de gegevensuitwisseling en een platform biedt waarop alle gebruikers kunnen aansluiten. De aanname is gedaan dat regels van mededinging de realisatie van dit model verhinderen. Daarnaast is aangenomen dat een platform alleen zou kunnen bestaan als deze wettelijk verankerd zou zijn en gefinancierd zou worden met publieke middelen. Een optie waarvan is aangenomen dat deze niet haalbaar is.

Daarom is gekozen voor een model van een persoonlijk gezondheidsnetwerk (MedMij-netwerk) waarin de diensten van gegevensuitwisseling door meerdere partijen, als makelaars voor gegevensuitwisseling, concurrentieel kunnen worden aangeboden. Aangenomen is dat deze benadering ook beter past in een markt bestaande uit private partijen, met vele leveranciers van persoonlijke gezondheidsomgevingen en vele zorgaanbieders.

4.4. Gegevensbescherming door ontwerp en door standaardinstellingen

Voor de gegevensuitwisseling met een persoonlijke gezondheidsomgeving kan de aanname worden gedaan dat persoonsgegevens van bijzondere aard worden uitgewisseld. Een goede gegevensbescherming is dan ook een van de pijlers voor het vertrouwen in de gegevensuitwisseling. Een persoon moet erop kunnen vertrouwen dat zijn of haar persoonlijke gegevens goed worden beschermd tegen inzage door niet-bevoegden, en dat de integriteit van de gegevens is gewaarborgd.

De Algemene Verordening Persoonsgegevens [5] vertaalt in artikel 25 gegevensbescherming door ontwerp (privacy by design) en door standaardinstelling (privacy by default) naar het nemen van passende organisatorische en technische maatregelen. Deze maatregelen gaan uit van 7 principes [6] die hieronder zijn benoemd

1. Proactief en preventief met maatregelen, zoals versleuteling en het gebruik van pseudoniemen, waarmee preventief wordt voorkomen dat de privacy van een persoon wordt geschonden;
2. Privacy wordt gebruikt als standaardinstelling wat betekent dat de gegevens van een persoon worden beschermd zonder dat deze daarvoor actie hoeft te ondernemen (dataminimalisatie oftewel Datensparsamkeit [7] is hiervan een voorbeeld);
3. Privacy is ingebed in het ontwerp en is daarmee een integraal onderdeel van het systeem;
4. Daar waar afwegingen moeten worden gemaakt tussen bijvoorbeeld privacy en veiligheid, wordt gezocht naar een “win-win”, een manier waarbij geen afbreuk hoeft worden gedaan aan beide belangen en doelstellingen;
5. De bescherming van een persoonsgegeven is van belang gedurende de gehele levenscyclus van dat gegeven, van creatie tot en met vernietiging;
6. Open en transparant naar belanghebbenden over de verwerking van persoonsgegevens, en dat deze verwerking overeenkomt met gedane beloften en doestellingen, en onderworpen is aan verificatie door een onafhankelijke instantie;
7. Het belang van de gebruiker, van de persoon, staat centraal in het systeem en kenmerkt zich door gebruikersvriendelijke keuzes en passende meldingen die de gebruiker in staat stellen maatregelen te nemen.

De bovenstaande principes hebben gevolgen voor de afspraken in het afsprakenstelsel. Een gevolg is dat het afsprakenstelsel niet alleen op basis van bestaande normen afspraken zal opnemen, maar ook aanvullende afspraken zal opnemen indien de gegevensbescherming daardoor wordt verhoogd.

4.5. Gebruikers moeten worden ontzorgd

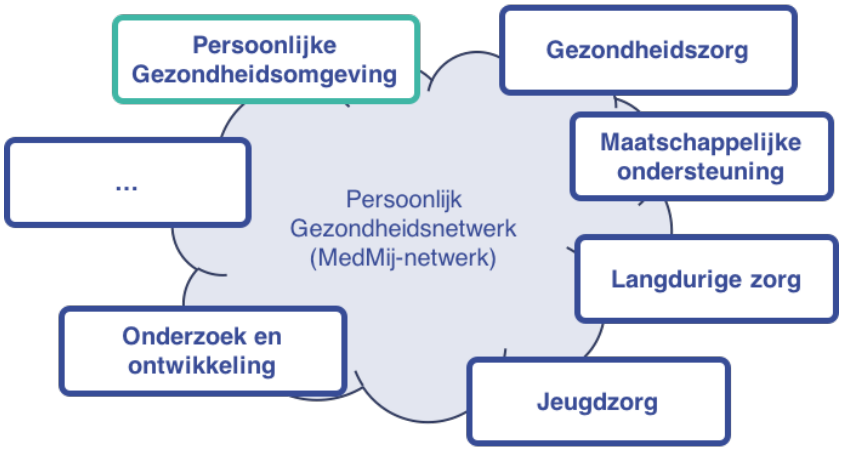
Het afsprakenstelsel probeert zoveel mogelijk de persoon, de leverancier van een persoonlijke gezondheidsomgeving en de zorgaanbieder te ontzorgen op techniek, proces en juridisch vlak. De aanname die hieraan ten grondslag ligt is dat leveranciers van persoonlijke gezondheidsomgevingen moeten kunnen focussen op datgeen waar zij goed in zijn, namelijk functionaliteit realiseren voor een persoon. Hetzelfde is van toepassing voor zorgaanbieders. Veilige en betrouwbare gegevensuitwisseling is complex, maar de gebruikers zouden daar niks van moeten merken.

Indien er keuzes in de oplossing moeten worden gemaakt, dan prefereert de oplossing die het minst van de gebruiker of de zorgaanbieder zelf vereist.

4.6. Het MedMij-netwerk verbindt 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.



Afbeelding 3 Het MedMij-netwerk is toegankelijk voor meerdere domeinen

De illustratie hierboven toont een aantal voorbeelden van domeinen die moeten kunnen aansluiten op het MedMij-netwerk.

5. Het stelsel van afspraken

MedMij is een afsprakenstelsel met afspraken die gerealiseerd worden voor een persoonlijke gezondheidsomgeving zodat individuele personen in staat zijn gegevens te verzamelen en te delen. In dit hoofdstuk worden de eisen en randvoorwaarden beschreven voor het afsprakenstelsel, waarbij gedacht kan worden aan de rollen en verantwoordelijkheden, de functies voor het beheer van de afspraken en de toetsing en handhaving dat afspraken worden nagekomen.

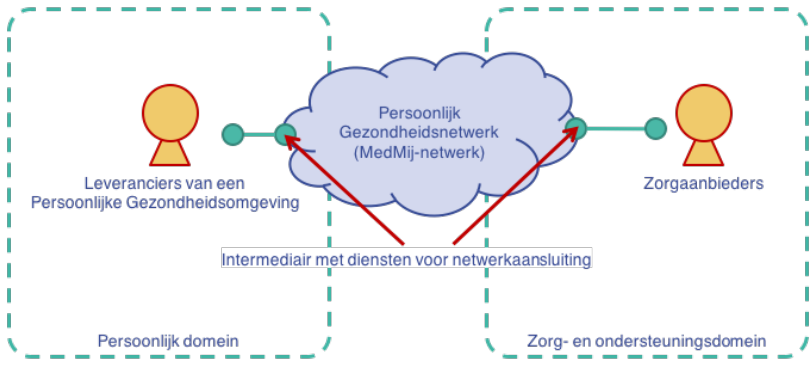
5.1. Aannames en eisen voor het realiseren van de gewenste uitkomsten

In de doelstellingen is een aantal onderwerpen genoemd dat ingevuld moeten worden om interoperabiliteit te verkrijgen tussen leveranciers van persoonlijke gezondheidsomgevingen en zorgaanbieders. Met het afsprakenstelsel moeten deze doelstellingen worden gerealiseerd. Naast de doelstellingen die als eis meegenomen moeten worden in de realisatie, is in deze paragraaf een aantal specifieke eisen opgenomen voor de invulling van het afsprakenstelsel.

5.1.1. Het afsprakenstelsel hanteert intermediaire rollen

Aangenomen is dat de gebruikers van het MedMij-netwerk zoveel mogelijk geholpen moeten worden met het implementeren van de juridische kaders, de technieken en de processen voor gegevensuitwisseling. Daarom worden voor het MedMij-netwerk intermediaire rollen gedefinieerd die onderdeel zijn van het netwerk en deelnemen in het netwerk. Een intermediair is een normaal verschijnsel daar waar specialisatie nodig is over de werking van een markt, materie of van een stelsel. Voorbeelden van intermediairs zijn vastgoedmakelaars, verzekeringstussenpersonen of advocaten. Binnen het MedMij-netwerk moet de MedMij-toegangsverlener zorgdragen voor het aansluiten van gebruikers en moet deze zorgdragen voor een veilige en betrouwbare gegevensuitwisseling.

Een leverancier van een persoonlijke gezondheidsomgeving of een zorgaanbieder kan ervoor kiezen om zelf de rol in te vullen dan wel hiervoor een marktpartij te vragen. Vanuit het principe dat diensten concurrentieel moeten worden aangeboden kan eenieder zich kwalificeren om deel te nemen in een rol van het afsprakenstelsel.



Afbeelding 4 Intermediairs leveren diensten voor netwerkaansluiting

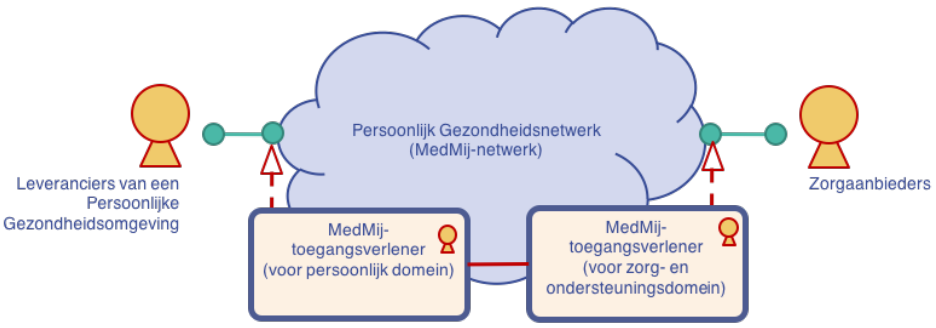
Het MedMij-netwerk onderkent de MedMij-toegangsverlener als rol. Een MedMij-toegangsverlener levert diensten aan de gebruikers van het netwerk op het gebied van netwerkaansluiting en gegevensuitwisseling, aan de leverancier van een persoonlijke gezondheidsomgeving en/of aan de zorgaanbieder.

5.1.2. Het afsprakenstelsel stelt richtlijnen op voor de bescherming van gegevens

Voor de gegevensuitwisseling is aangenomen dat met de komst van de Algemene Verordening Gegevensbescherming (AVG) [5] niet duidelijk is wat passende maatregelen zijn voor de bescherming van persoonsgegevens. Ook het principe “gegevensbescherming door ontwerp en door standaardinstellingen” dat met de AVG wordt geïntroduceerd moet nader worden ingevuld. Het afsprakenstelsel omvat daarom een ontwerp van de gegevensuitwisseling met richtlijnen voor het gebruik van standaarden ten behoeve van gegevensbescherming. Aangenomen wordt dat met het eenmalig vastleggen van een ontwerp in een afsprakenstelsel eenvoudiger gecontroleerd kan worden dat het ontwerp voldoet aan de letter en de geest van de verordening.

5.1.3. Het afsprakenstelsel maakt onderscheid naar marktsegment

Voor het afsprakenstelsel is gekozen voor een aanpak van marktdifferentiatie. De aanname die hieraan ten grondslag ligt is dat leveranciers van een persoonlijke gezondheidsomgeving andere wensen hebben dan zorgaanbieders, en daarmee ook behoefte hebben aan andere diensten. De rollen in het afsprakenstelsel zijn onderverdeeld naar een rol gericht op leveranciers van persoonlijke gezondheidsomgevingen en een rol gericht op zorgaanbieders en andere organisaties werkzaam in het domein van de zorg en ondersteuning.



Afbeelding 5 Rollen onderverdeeld naar marktsegment

5.2. Randvoorwaarden naar aanleiding van het juridisch kader

De juridische kaders voor het afsprakenstelsel worden separaat uitgewerkt en vallen niet binnen het bereik van dit document. Meer informatie over de juridische kaders kan gevonden worden in het document juridische aspecten [4]. De impact van de conclusies uit de juridische kaders zijn hieronder opgenomen in de paragraaf over wet- en regelgeving.

5.2.1. Een toegangsverlener als bewerker van persoonsgegevens?

In het MedMij-netwerk worden persoonsgegevens uitgewisseld van bijzondere aard. In de uitwerking van het juridische kader is opgenomen dat de leverancier van een persoonlijke gezondheidsomgeving en de zorgaanbieder verantwoordelijk zijn voor de verwerking van persoonsgegevens overeenkomstig de Wet bescherming persoonsgegevens (Wbp).

Afhankelijk van het feit of een toegangsverlener macht kan uitoefenen over de persoonsgegevens die via haar worden doorgegeven, zal een toegangsverlener wel of niet als bewerker moeten opereren. Als voorbeeld kan een huurlijn van een telecomprovider worden genoemd die zodanig is beveiligd dat de telecomprovider feitelijk geen enkele macht kan uitoefenen over de gegevens die door hem worden doorgegeven.

5.2.2. Een persoonlijke gezondheidsomgeving registreert geen burgerservicenummer

Binnen de Wbp worden bijzondere persoonsgegevens onderkend, waaronder het burgerservicenummer. Het burgerservicenummer is bijzonder omdat het een uniek en tot de persoon herleidbaar nummer is. Een organisatie mag geen bijzondere persoonsgegevens gebruiken, tenzij daarvoor in de wet een uitzondering is (bron: Autoriteit persoonsgegevens). Binnen de zorg is het gebruik van het burgerservicenummer opgenomen in het “Besluit gebruik burgerservicenummer in de zorg”. Deze wet is echter niet van toepassing op de leveranciers van persoonlijke gezondheidsomgevingen omdat het in de wet alleen aan zorgaanbieders, het indicatieorgaan en aan zorgverzekeraars wordt toegestaan het burgerservicenummer te gebruiken.

Een persoonlijke gezondheidsomgeving mag daarom geen burgerservicenummer registreren en het burgerservicenummer kan daarom niet in de gegevensuitwisseling worden opgenomen. Voor de partijen die afhankelijk zijn van het burgerservicenummer zal binnen het afsprakenstelsel een afspraak gerealiseerd moeten worden om op basis van authenticatie tot het burgerservicenummer te komen.

Bovenstaande argumenten zijn een juridisch kader die gebaseerd zijn op de huidige wet- en regelgeving, maar het houdt geen rekening met een functionele of technische noodzaak om het burgerservicenummer te gebruiken. Vanuit gegevensbescherming door ontwerp is het echter ook niet gewenst om het burgerservicenummer te gebruiken omdat het de privacy niet verhoogd. Het ophalen van persoonsgegevens door een persoonlijke gezondheidsomgeving mag namelijk niet gebaseerd zijn op het burgerservicenummer dat wordt opgegeven, maar moet gebaseerd zijn op de authenticatie van een persoon en de autorisatie dat de persoonlijke gezondheidsomgeving toestemming heeft van die persoon om de gegevens op te halen. De aanbieder van zorg en/of ondersteuning is verantwoordelijk voor de authenticatie en autorisatie, en zal op basis van de authenticatie een koppeling moeten leggen met het burgerservicenummer voor eigen gebruik.

5.2.3. De zorgaanbieder is verantwoordelijk voor rechtmatigheid gegevensuitwisseling

Een gegevensproducent van medische gegevens, de zorgaanbieder, is verantwoordelijk voor de rechtmatigheid van een gegevensuitwisseling. Een zorgaanbieder moet erop toezien dat met een substantiële of hoge mate van zekerheid (hoog voor de gegevens waarop het medisch beroepsgeheim van de zorgverlener rust) aangetoond kan worden dat het de persoon zelf is die de gegevensuitwisseling met een persoonlijke gezondheidsomgeving autoriseert. Het MedMij-netwerk authentiseert geen personen, maar MedMij-toegangsverleners zullen diensten aanbieden voor de

autorisatie van een gegevensuitwisseling. Nadat de gegevens zijn verkregen en zijn opgeslagen in de persoonlijke gezondheidsomgeving is het de verantwoordelijkheid van de persoon om gegevens wel of niet te delen met anderen.

Met betrekking tot (wettelijke) vertegenwoordiging van personen wordt geadviseerd de landelijke ontwikkelingen te volgen rondom digitaal machtigen (zoals DigiD Machtigen). Dit betreft de gegevensuitwisseling met zorgaanbieders. Het delen van gegevens vanuit een persoonlijke gezondheidsomgeving is een verantwoordelijkheid van de betrokken persoon die in de persoonlijke gezondheidsomgeving zijn of haar gegevens verzamelt.

5.3. Randvoorwaarden aan de werking van het stelsel

Voor een goede werking van het afsprakenstelsel zijn randvoorwaarden opgesteld. Aangenomen wordt dat met deze randvoorwaarden een bijdrage kan worden geleverd aan het vertrouwen in het afsprakenstelsel.

5.3.1. Het afsprakenstelsel hanteert deelnamevoorwaarden voor intermediairs

Een MedMij-toegangsverlener is een cruciale rol voor het afsprakenstelsel. Het vertrouwen in het afsprakenstelsel en de kwaliteit van de uitvoering hangt af van de wijze waarop MedMij-toegangsverlener de afspraken implementeren. Aangenomen wordt dat niet iedere marktpartij de gewenste kwaliteit kan leveren en het juiste volwassenheidsniveau heeft om de afspraken te implementeren. Een partij die de rol van MedMij-toegangsverlener wil invullen binnen het afsprakenstelsel moet daarom voldoen aan deelnamevoorwaarden.

Het instellen van deelnamevoorwaarden geeft ook verplichtingen met betrekking tot handhaving is de veronderstelling.

5.3.2. De afspraken worden beheerd en gehandhaafd door een beheerorganisatie

Aangenomen wordt voor besturing en governance een beheerorganisatie wordt ingesteld voor de verdere ontwikkeling van het afsprakenstelsel.

De beheerorganisatie voor het afsprakenstelsel zal processen definiëren voor toe- en uittreding van partijen in de rol van MedMij-toegangsverlener. Daarnaast zal door middel van een periodieke audit worden toegezien dat bestaande deelnemers nog steeds voldoen aan de deelnamevoorwaarden. Het afsprakenstelsel zal maatregelen definiëren bij niet nakomen van afspraken.

5.3.3. De afspraken worden gerealiseerd binnen het Nederlands recht

De aanname is dat het afsprakenstelsel een overeenkomst is tussen de beheerorganisatie en de deelnemers in het afsprakenstelsel, een overeenkomst die valt binnen het Nederlandse privaatrecht. Zowel voor de deelnemers als voor de gebruikers van het netwerk is daarom van toepassing dat zij vallen onder het Nederlands recht, waarbij rechtspersonen verplicht zijn tot een registratie bij de Kamer van Koophandel (KvK).

Het afsprakenstelsel bevat geen afspraken die reeds als wet- en regelgeving van toepassing zijn omdat aangenomen is dat iedere rechtspersoon gehouden is aan de geldende wet- en regelgeving overeenkomstig het Nederlands recht.

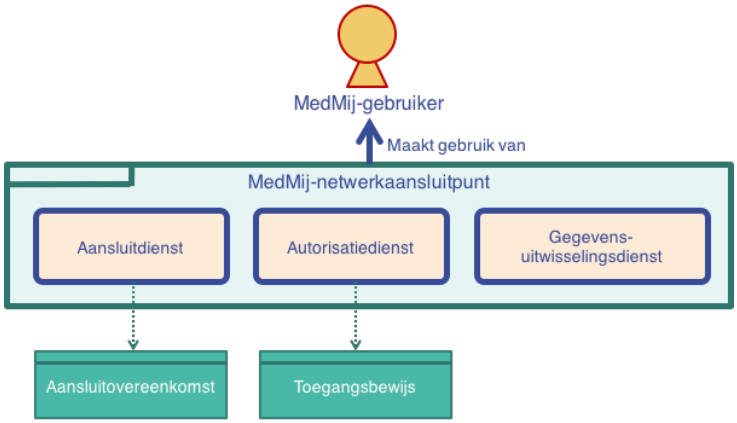
6. Afspraken over de rol van toegangsverlener

Het MedMij-netwerk is het systeem dat moet zorgdragen voor de uitwisseling van gezondheidsgegevens. Het netwerk bestaat uit, en wordt verzorgd door alle deelnemende toegangsverleners. Toegangsverlener is de naam van de rol voor de intermediairs in het afsprakenstelsel.

6.1. Verantwoordelijkheden van een toegangsverlener

6.1.1. Toegangsverleners bieden een netwerkaansluitpunt aan

De toegangsverleners leveren diensten aan leveranciers van persoonlijke gezondheidsomgevingen en/of aan organisaties werkzaam in het domein van zorg en ondersteuning. Deze gebruikers kunnen worden aangesloten via een netwerkaansluitpunt op het MedMij-netwerk. De toegangsverlener levert vervolgens diensten op het gebied van integratie en autorisatie en stelt hiervoor koppelvlakken beschikbaar.



Afbeelding 6 Diensten van een toegangsverlener

De diensten zijn onder te verdelen naar een dienst voor het aansluiten van gebruikers op het netwerk, diensten voor het autoriseren van een gegevensuitwisseling door individuele personen en diensten voor de gegevensuitwisseling zelf. De autorisatie betreft de toestemming die een persoon moet geven voor het uitwisselen van gegevens tussen een persoonlijke gezondheidsomgeving en een zorgaanbieder. Ondanks dat voor de beeldvorming een persoon de gegevens verzamelt in zijn of haar omgeving, is het wettelijk gezien de leverancier van een persoonlijke gezondheidsomgeving die de gegevens verzamelt en verwerkt. Een persoon moet daarom toestemming geven aan de zorgaanbieder dat deze gegevens uitwisselt met de leverancier van de persoonlijke gezondheidsomgeving.

De koppelvlakken die een toegangsverlener met een persoonlijke gezondheidsomgeving of met een zorgaanbieder biedt zijn concurrentieel, omdat wordt aangenomen dat een toegangsverlener een zo

goed mogelijke dienstverlening wil realiseren en juist op de koppelvlakken en de aansluiting op de koppelvlakken het onderscheid kan maken.

6.1.2. Toegangsverleners ontzorgen gebruikers

Een van de principes is dat gebruikers van hun zorgen moeten worden ontnomen, hun zorgen ten aanzien van een veilige en betrouwbare gegevensuitwisseling. Een van de redenen voor de keuze om intermediaire rollen te hanteren. De toegangsverleners moeten daarom ook effectief gebruikers gaan ontzorgen en dienstverlening aanbieden in de vorm van hulpmiddelen en ondersteuning die gevolg geeft aan het principe.

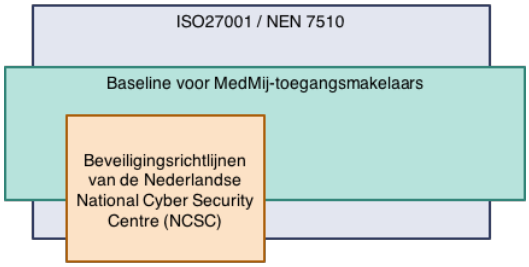
6.1.3. Toegangsverleners vormen het communicatiekanaal richting een gebruiker

Door een gebruiker te koppelen aan 1 toegangsverlener van het MedMij-netwerk wordt het veel-op-veel-probleem opgelost. Een gebruiker heeft slecht 1 communicatiekanaal voor de gegevensuitwisseling via het netwerkaansluitpunt, en kan via dat ene communicatiekanaal gegevens uitwisselen met alle andere gebruikers van het netwerk.

6.1.4. Toegangsverleners dragen zorg voor een goede gegevensbescherming

Het mag worden aangenomen dat de gegevens die via het MedMij-netwerk worden uitgewisseld persoonlijke gegevens zijn, persoonsgegevens van bijzondere aard in veel gevallen. Daarom zijn passende maatregelen noodzakelijk voor de bescherming van deze persoonsgegevens.

Voor het bepalen van de passende maatregelen moeten toegangsverleners een risicoanalyse en beoordeling hebben uitgevoerd en op basis daarvan de matregelen hebben genomen overeenkomstig NEN-ISO/IEC 27002 en NEN 7510 (inclusief NEN 7512 en NEN 7513). Een baseline voor MedMij-toegangsverlener is vooralsnog een optie waar verder onderzoek voor nodig is. De mogelijkheid van een baseline is gebaseerd op de aanname dat de risico's van toegangsverleners veel overeenkomsten hebben en dat een gelijke beoordeling van risico's van belang is als rechtvaardigheidsprincipe voor de marktpartijen die diensten willen aanbieden in de rol van toegangsverlener.

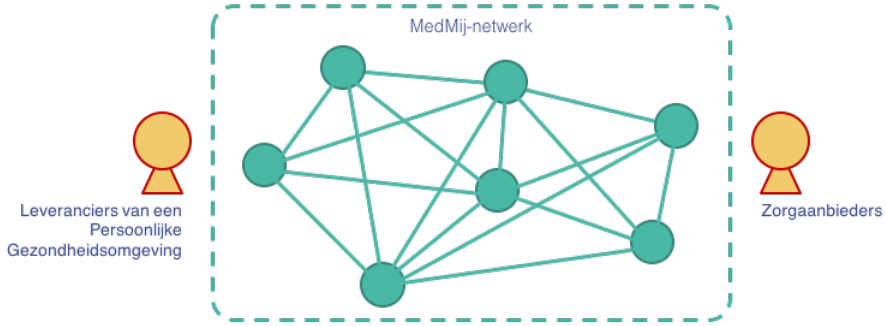


Afbeelding 7 Positionering normenkader en richtlijnen

Voor de uitvoering van de maatregelen voor de bescherming van persoonsgegevens zal een toegangsverlener de richtlijnen moeten implementeren van de Nederlandse National Cyber Security Centre (NCSC) voor de diensten, zie ook https://www.ncsc.nl/actueel/whitepapers.

6.1.5. Toegangsverleners conformeren zich aan de MedMij-standaarden en profielen

Met de rollen van toegangsverlener gedefinieerd, de aanname dat meerdere partijen zullen toetreden in de rol van toegangsverlener en de keuze voor 1 communicatiekanaal per gebruiker, dan is het noodzakelijk standaarden te hanteren voor de gegevensuitwisseling tussen toegangsverleners. Voor de gegevensuitwisseling tussen toegangsverleners zal daarom een gestandaardiseerd koppelvlak worden gehanteerd waaraan eenieder zich moet conformeren.



Afbeelding 8 Gegevensuitwisseling tussen toegangsverleners via een gestandaardiseerd koppelvlak

Met het conformeren aan de MedMij-standaarden en profielen conformeert een toegangsverlener zich ook aan de principes en richtlijnen van de architectuur van het afsprakenstelsel.

6.1.6. Toegangsverleners hanteren en handhaven aansluit- en gebruiksvoorwaarden

Betrouwbaarheid en veiligheid van het MedMij-netwerk is essentieel voor het vertrouwen. Voor het MedMij-netwerk wordt daarom een beleid gevoerd van beperkte toegang. Alleen gebruikers die voldoen aan de afspraken opgesteld in het afsprakenstelsel, en verwoord door middel van aansluit- en gebruiksvoorwaarden, kunnen een netwerkaansluitpunt verkrijgen.

Vooralsnog worden onderstaande aansluit- en gebruiksvoorwaarden gehanteerd:

– *Gebruikers dragen zorg voor een goede gegevensbescherming*
  Aangenomen kan worden dat gebruikers een goede gegevensbescherming willen voor de persoonsgegevens die worden verzameld. In de aansluit- en gebruiksvoorwaarden wordt daarom opgenomen dat een gebruiker die wil aansluiten voldoet aan de NEN-ISO/IEC 27001 waarbij naast de beheersmaatregelen uit de NEN-ISO/IEC 27002 ook de maatregelen uit de NEN 7510/7512/7513 in de scope zijn opgenomen.

– *persoonlijke gezondheidsomgevingen zijn toegankelijk*
  Personen die gebruik maken van een persoonlijke gezondheidsomgeving moeten dat bij voorkeur zonder drempels kunnen doen. Voor leveranciers van een persoonlijke gezondheidsomgeving wordt daarom de volgende voorwaarde opgenomen ten aanzien van de kwaliteit: de gebruiker hanteert de WCAG 2.0 standaard, niveau AA, voor het ontwerp van de gebruikersinterface van webapplicaties. Dit betreft alleen de schermen die noodzakelijk zijn voor de interactie met het afsprakenstelsel.

6.2. Functies van een toegangsverlener

Een toegangsverlener moet een aantal functies vervullen voor enerzijds de werking van het netwerk en anderzijds voor het ontzorgen van gebruikers. In deze paragraaf worden deze functies beschreven.

6.2.1. Aansluiten van gebruikers

Toegangsverleners leveren een netwerkaansluitpunt aan leveranciers van persoonlijke gezondheidsomgevingen, aan zorgaanbieders, zorgverzekeraars en aan overheden werkzaam in het domein van zorg en ondersteuning. Met het leveren van een netwerkaansluitpunt worden deze gebruikers aangesloten op het MedMij-netwerk. Met de aansluiting verkrijgt een gebruiker een adres binnen het netwerk en de sleutels voor het gebruik van de diensten van het netwerkaansluitpunt.

Met de overeenkomst moet ook een bewerkersovereenkomst worden afgesloten als aangenomen kan worden dat de toegangsverlener verwerker is van persoonsgegevens.

6.2.2. Levering van hulpmiddelen voor het autoriseren van een gegevensuitwisseling

De aanname is dat personen toestemming moeten verlenen voor het uitwisselen van gegevens van een zorgaanbieder naar een persoonlijke gezondheidsomgeving. Zowel zorgaanbieders als de leveranciers van een persoonlijke gezondheidsomgeving moeten worden ontzorgd is de gedachte. Een toegangsleverancier zal daarom hulpmiddelen leveren voor het autoriseren van de gegevensuitwisseling.

6.2.3. Leveren van hulpmiddelen voor de gegevensuitwisseling

Gebruikers willen zeer waarschijnlijk op een zo eenvoudige mogelijke manier gebruik kunnen maken van de gegevensuitwisseling, met een zo laag mogelijke inspanning. Vanuit het principe van het ontzorgen van gebruikers zal een toegangsverlener daarom hulmiddelen leveren zodat gebruikers vanuit hun software eenvoudig gebruik kunnen maken van de koppelvlakken voor gegevensuitwisseling.

6.2.4. Routering en bezorging van berichten

Een kernfunctie van een toegangsverlener is het routeren en bezorgen van berichten. Een bericht wordt aangeboden door een gebruiker bij een toegangsverlener en moet via een (waarschijnlijk andere) toegangsverlener worden bezorgd aan een andere gebruiker.

6.2.5. Ondersteuning van gebruikers

In het kader van het ontzorgen van gebruikers wordt aangenomen dat gebruikersondersteuning gewenst is. Gebruikersondersteuning kan op vele manieren worden ingericht en is niet gebonden aan een telefonische helpdesk. Ook mogelijkheden tot monitoring en traceerbaarheid van berichten wordt gezien als gebruikersondersteuning.

Zoals reeds bij de aannames en eisen benoemd vormt een toegangsverlener het communicatiekanaal richting de gebruiker. Dit is ook van toepassing voor de ondersteuning waarbij een toegangsverlener functioneert als single-point-of-contact voor gebruikersondersteuning over alle zaken met betrekking tot het MedMij-netwerk.

7. Afspraken voor een gegevenscatalogus

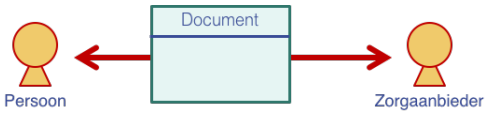
In de gegevenscatalogus zijn de type documenten opgenomen die door zorgaanbieders en overheden kunnen worden gedeeld met een persoon. Maar ook de eigen registraties van een persoon, die gedeeld kunnen worden, zijn als type opgenomen in de catalogus.

Een document is een generieke naam voor een container met daarin een verzameling gegevens die tussen twee partijen kunnen worden uitgewisseld. Ieder document is het resultaat van een proces. Document en type document zijn misschien wat abstracte termen, maar documenten zien we iedere dag om ons heen, bijvoorbeeld een doktersrecept, een visitekaartje, een factuur of de belastingaanslag. Het daadwerkelijke papieren doktersrecept is in deze het document terwijl de naam doktersrecept aangeeft dat het document van het type doktersrecept is. Van een papieren doktersrecept kan ook een elektronische weergave worden gemaakt die tussen twee computersystemen kan worden uitgewisseld.

7.1. Aannames en eisen

7.1.1. Gestandaardiseerde documenten

Aangenomen wordt dat voor de uitwisseling van gegevens gestandaardiseerde documenten nodig zijn. Voor ieder type document moeten daarom afspraken worden gemaakt welke gegevens in het document zijn opgenomen en indien terminologie wordt gebruikt, wat de betekenis is van de termen.



Afbeelding 9 Gestandaardiseerde documenten

7.1.2. Gegevens gebaseerd op informatiebouwstenen

Informatiebouwstenen zijn gestandaardiseerde verzamelingen van gegevens. Persoonsgegevens en adresgegevens zijn bekende voorbeelden van gegevens die gestandaardiseerd kunnen worden. Aangenomen wordt dat de gegevens in de documenten ook veelal gestandaardiseerd kunnen worden tot informatiebouwstenen zodat deze bouwstenen in meerdere type documenten kunnen worden hergebruikt.

7.1.3. Aangeven welke type documenten beschikbaar zijn voor welke gegevensdiensten

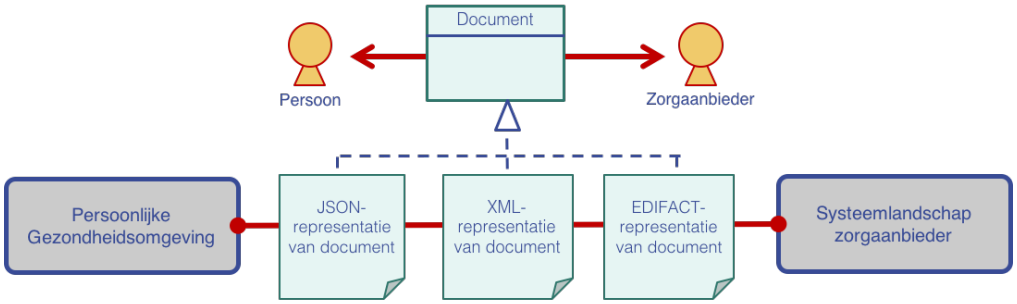
Aangenomen wordt dat een persoonlijke gezondheidsomgeving kennis moet kunnen nemen van de gegevensdiensten van zorgaanbieders. Niet iedere zorgaanbieder heeft dezelfde gegevensdiensten, maar biedt de gegevensdiensten die behoren bij haar competentie. Een gegevensdienst kan een opdracht zijn of een melding over een gebeurtenis, bijvoorbeeld de melding aan een apotheek dat een persoon medicatie heeft gebruikt of de opdracht om een afspraak in te plannen dan wel het verkrijgen en kunnen lezen van reeds geplande afspraken. In het laatste geval zou een afspraakkaart als document kunnen worden opgeleverd met daarin de afspraken die gepland zijn.

De gegevensdiensten die door zorgaanbieders en overheden aangeboden worden en de documenten die daarbij kunnen worden verkregen of beschikbaar kunnen worden gesteld moeten alle als onderdeel van de gegevenscatalogus worden opgenomen.

7.1.4. Documenten en uitwisselingsformaten

Zoals wordt aangenomen zal een persoon een persoonlijke gezondheidsomgeving gebruiken voor het verzamelen van gezondheidsgegevens van verschillende zorgaanbieders. Een persoon heeft bijvoorbeeld contact met zorgprofessionals in meerdere ziekenhuizen, verkrijgt medicijnen van zowel zijn of haar eigen apotheek als van een ziekenhuisapotheek, gaat op consult bij een huisarts, tandarts of fysiotherapeut en mogelijk naar een huisartsenpost voor spoedeisende hulp. Al deze partijen gebruiken hun eigen informatiesystemen en naar wordt aangenomen van verschillende softwareleveranciers.

Om gegevens elektronisch te kunnen uitwisselen zijn afspraken nodig voor gestandaardiseerde uitwisselingsformaten van documenten. Een informatiesysteem moet deze documenten, en de daarin opgenomen gegevens, kunnen ontvangen, interpreteren en functioneel correct kunnen toepassen.



Afbeelding 10 Documenten kunnen verschillende uitwisselingsformaten hebben

De gestandaardiseerde uitwisselingsformaten die binnen het MedMij-netwerk kunnen worden uitgewisseld zijn onderdeel van de gegevenscatalogus waarin voor ieder type document wordt aangegeven welke uitwisselingsformaten worden ondersteund.

7.2. Afspraken over de documenten en uitwisselingsformaten

Binnen het domein van zorg- en ondersteuning zijn verschillende organisaties actief met het realiseren van documenten en uitwisselingsformaten zoals Nictiz, VNG/KING, Vektis en Zorginstituut Nederland. Aangenomen wordt dat documenten en uitwisselingsformaten opgesteld door deze organisaties onderdeel zullen uitmaken van de gegevenscatalogus. De uitwisselingsformaten opgenomen in de gegevenscatalogus betreffen uiteindelijk de afspraak dat deze geaccepteerd moeten worden door de gegevensdiensten van zorgaanbieders, zorgverzekeraars en overheden. Dit zijn met andere woorden de uitwisselingsformaten die via het MedMij-netwerk kunnen worden uitgewisseld.

Het mag worden aangenomen dat in de loop van de tijd meerdere versies van uitwisselingsformaten zullen worden vrijgegeven. In de gegevenscatalogus zal daarom de versie moeten worden opgenomen die door de zorgaanbieder wordt ondersteund, waarbij wordt aangenomen dat dit veelal de actuele en de voorgaande versie zal zijn.

8. Afspraken over de technische werking

8.1. Aannames en eisen

Gegevensuitwisseling tussen applicaties betekent dat twee applicaties met elkaar kunnen samenwerken en dat gebruikers gegevens die in de ene applicatie zijn ingevoerd kunnen hergebruiken in een andere applicatie. Gegevens kunnen op verschillende manieren worden uitgewisseld, met verschillende stijlen voor integratie en verschillende uitvoeringspatronen.

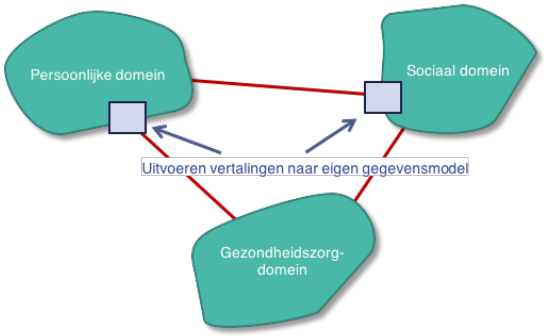
8.1.1. Softwaresystemen zijn niet altijd beschikbaar

Aangenomen wordt dat systemen van zorgaanbieders en overheden, maar ook persoonlijke gezondheidsomgevingen niet continue beschikbaar zijn, maar door onderhoudsintervallen tijdelijk even niet beschikbaar kunnen zijn. Een persoonlijke gezondheidsomgeving kan ook niet beschikbaar zijn omdat de persoon zijn of haar telefoon heeft uitgezet.

Hoewel aangenomen moet worden dat een persoonlijke gezondheidsomgeving niet altijd beschikbaar is, moet een persoonlijke gezondheidsomgeving altijd beschikbaar zijn op de momenten dat een persoon deze omgeving wil gebruiken. Een persoonlijke gezondheidsomgeving mag daarom niet afhankelijk zijn van de beschikbaarheid van de systemen van zorgaanbieders en overheden, maar moet zelfstandig kunnen functioneren met een eigen database met gegevens.

8.1.2. Contextuele kaders hebben een eigen gegevensmodel

Een persoonlijke gezondheidsomgeving is software die gerealiseerd is met als doel een persoon regie te geven over diens gezondheid. Dit is een ander doel dan waarvoor software is gerealiseerd voor zorgaanbieders, zorgverzekeraars en overheden.



Afbeelding 11 Contextuele kaders hebben eigen gegevensmodellen en structuren

De verschillende softwaresystemen moeten met andere woorden een andere waarde opleveren, en hebben derhalve andere vereisten en een ander ontwerp. Aangenomen wordt dat dit verschil in contextuele kaders tot gevolg heeft dat het gegevensontwerp van deze systemen verschillend is met als gevolg verschillende modellen, structuren en betekenis van gegevens.

Daarom wordt als uitgangspunt gehanteerd dat de mogelijkheid moet bestaan om vertalingen uit te voeren van het ene contextueel kader naar een ander contextueel kader. Vertalingen worden altijd

binnen de verantwoordelijkheid van een contextueel kader uitgevoerd, dus onder verantwoordelijkheid van een leverancier van een persoonlijke gezondheidsomgeving, een zorgaanbieder, een zorgverzekeraar of een overheid.

8.1.3. Geen onbestelbare berichten in het netwerk

Een van de eigenschappen van berichtuitwisseling is dat berichten onbestelbaar kunnen zijn. Het computersysteem waaraan een bericht was geadresseerd kan verhuisd zijn of zijn overleden. Met de aanname dat het berichtenverkeer in het MedMij-netwerk persoonsgegevens van bijzondere aard bevat, zou daarmee een situatie kunnen ontstaan dat persoonsgegevens voor een langere periode worden opgeslagen in het netwerk. Naar wordt aangenomen is dit niet acceptabel vanuit het principe van gegevensbescherming door ontwerp. Berichten worden daarom niet bewaard in het netwerk.

8.1.4. Alleen gegevens leveren waarvan de zorgaanbieder de gegevensproducent bent

Aangenomen wordt dat een zorgaanbieder alleen gegevens verstrekt waarvoor zij zelf de gegevensproducent is. Dit is gebaseerd op de aanname dat gegevens alleen betrouwbaar door de bron van de gegevens geleverd kunnen worden, om te voorkomen dat gegevens dubbel worden geleverd en/of correcties in de gegevens niet zijn opgenomen. Zorgaanbieders, zorgverzekeraars en overheden leveren daarom alleen de gegevens waarvan zij de bron zijn. Personen kunnen daarentegen gegevens delen die afkomstig zijn van andere zorgaanbieders dan de zorgaanbieder met wie de gegevens wordt gedeeld waarbij onweerlegbaar aangetoond moet kunnen worden dat deze gegevens afkomstig zijn van een betrouwbare bron.

8.1.5. Zorgaanbieders stellen nieuwe gegevens actief beschikbaar

Mede gebaseerd op de aannames dat systemen niet altijd beschikbaar zijn en dat berichten niet onbestelbaar achter mogen blijven wordt als uitgangspunt gehanteerd dat zorgaanbieders een persoon actief informeren over het feit dat er nieuwe gegevens beschikbaar zijn. Nieuwe gegevens komen altijd beschikbaar naar aanleiding van een gebeurtenis. Zorgaanbieders informeren dan ook het feit dat een gebeurtenis heeft plaatsgevonden en doen dat op basis van de wens van een persoon gebruik te maken van de gegevensdiensten van de zorgaanbieder.

Vanuit het principe van dataminimalisatie wordt als uitgangspunt gehanteerd dat een persoonlijke gezondheidsomgeving alleen een melding ontvangt over een gebeurtenis, maar dat de persoonsgegevens zelf alleen beschikbaar worden gesteld na een expliciete opvraag door de persoonlijke gezondheidsomgeving. Meldingen mogen in deze dan verloren gaan en verwijderd worden indien onbestelbaar.

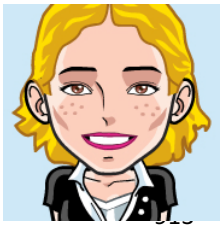
8.1.6. Personen verzamelen gegevens en delen gegevens met anderen

Een persoon heeft het initiatief, al dan niet geautomatiseerd, bij het verzamelen en delen van gegevens. Op basis van een melding van een zorgaanbieder haalt de persoonlijke gezondheidsomgeving de gegevens op. Het delen van gegevens vindt ook plaats op initiatief van een persoon. Als een persoon aangeeft dat deze gegevens wil delen met een zorgaanbieder, dan verzendt de persoonlijke gezondheidsomgeving deze gegevens op een manier overeenkomstig een “remote procedure call” naar de zorgaanbieder zonder dat hieraan een melding vooraf gaat.

8.2. Infrastructurele gebruiksscenario's

De gebruiksscenario's zijn beschreven in de vorm van een verhaal vanuit het gezichtspunt van een belanghebbende om vanuit zijn of haar ervaringen het scenario te kunnen belichten, een persoonlijk verhaal. Het verhaal in dit document is vooralsnog geschreven vanuit het gezichtspunt van een persoon genaamd Roos die gegevens wil verkrijgen in haar persoonlijke gezondheidsomgeving. Met de scenario's wordt een beschrijving gegeven van de mogelijke werking van de diensten in het MedMij-netwerk, diensten die via het netwerkaansluitpunt van een toegangsverlener worden aangeboden. Deze diensten zijn de autorisatiedienst en de gegevensuitwisselingsdienst.

8.2.1. Kennismaking met de persona, 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 persoonlijk gezondheidsnetwerk waarmee ik informatie kan delen met zorgaanbieders en overheden. 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.

Informatie krijgen van Ed over de medicijnen die aan mij zijn verstrekt heeft mij erg geholpen. Toen ik mij onzeker voelde, geen overzicht had en voor mijn gevoel geen grip had over de medicijnen die ik moest slikken. Daarom wil ik mijn ervaringen delen, zodat jullie ook kennis kunnen maken met MedMij en daar gebruik van kunnen maken.

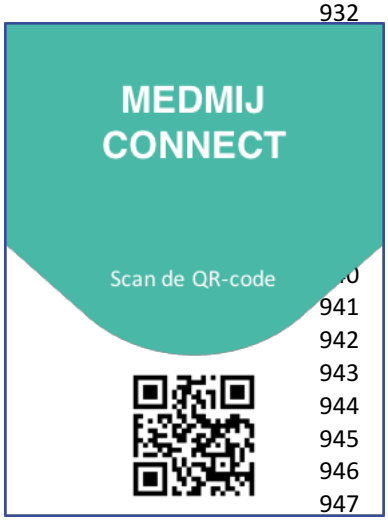
Al een aantal jaren heb ik diabetes en sinds kort maak ik gebruik van een applicatie op mijn telefoon om mijn bloedwaarden en gewicht in de gaten te kunnen houden en een actueel overzicht te hebben van mijn medicatie. De bloedwaarden en gewicht deel ik met Evelien als ik voor controle ben. Met de applicatie kan ik ook het gebruik van insuline bijhouden en Ed krijgt automatisch een melding als mijn voorraad onder het minimumniveau zakt, zodat ik mijn voorraad kan aanvullen.

8.2.2. De stappen om de gegevensuitwisseling te autoriseren

Ik moest zowel bij mijn huisarts als bij mijn apotheek toestemming verlenen. Omdat ik de ene keer via mijn telefoon toestemming gaf en de andere keer achter mijn laptop, zal ik beide ervaringen met jullie delen.

Toestemming verlenen via mijn telefoon

Tijdens een controle bij Evelien, de praktijkondersteuner van mijn huisarts viel een poster aan de muur mij op. Het was een poster over MedMij om gegevens uit te wisselen met mijn huisarts. En ik zag meer reclamemateriaal en folders van MedMij in de wachtkamer. Ik vroeg Evelien ernaar.



"Wat leuk dat je ernaar vraagt, gebruik je al een app?" reageerde Evelien gelijk heel enthousiast.

"Uuh, ja" stamelde ik en ik greep mijn telefoon om de app op te starten. "Ik gebruik deze app om mijn bloedwaarden en gewicht zelf bij te houden" vertelde ik aan Evelien.

"Wat goed. Die waarden kun je met mij delen net als dat ik kan delen wat we hier meten. Zo hebben we beiden een vollediger beeld."

Ik zag dat de app ondersteuning gaf aan gegevensuitwisseling via MedMij het logo werd getoond. Ik kon aan de lijst met zorgaanbieders een zorgaanbieder toevoegen. Mijn lijst was overigens nog helemaal leeg want ik had nog niemand gekoppeld.

Ik gaf aan dat ik een nieuwe zorgaanbieder wilde toevoegen en ik moest aangeven dat ik dat via een zogenaamde QR-code wilde doen. Zo heet het symbool dat op de poster staat en een adres in computertaal voorstelt.

De camera van mijn telefoon ging aan en ik kwam in een scherm terecht waarin ik de QR-code kon gaan scannen. Ik richtte de camera op de poster en de app las het adres.

Vervolgens werd de MedMij-webpagina van de huisarts van Marlou geopend waarop ik moest inloggen. Het was het bekende inlogscherm van Idensys dat ik al vaker had gebruikt om in te loggen bij een overheidsdienst. Ik gaf mijn gebruikersnaam en wachtwoord in en ontving een sms. Na de sms-code ingevuld te hebben kreeg ik toegang en kon ik toestemming geven.

Ik kreeg te zien dat mijn app, mijn persoonlijke gezondheidsomgeving, toestemming vroeg om consultverslagen en laboratoriumwaarden te lezen, en eigen metingen beschikbaar te stellen.

Ik gaf toestemming.

De browser op mijn telefoon sloot zich en ik kwam weer terug in de app. Ik zag ik dat in de lijst met zorgaanbieders mijn huisarts was toegevoegd met vermelding van de gegevensdiensten waarvoor ik toestemming had gegeven.

Ik was gekoppeld met mijn huisarts en klaar om gegevens uit te wisselen.

Toestemming verlenen voor een webapplicatie

Naast de app op mijn telefoon kan ik mijn gegevens ook in een persoonlijke gezondheidsomgeving raadplegen via de browser op mijn laptop. De stappen die ik moest uitvoeren waren vrijwel identiek aan de stappen op mijn telefoon. Alleen had ik de QR-code niet van een poster gescand, maar had ik

deze QR-code gekregen van mijn apotheek via een brief. Via de camera van mijn laptop kon ik de QR-code op de brief scannen en werd ik vervolgens naar de inlogpagina geleid.

Initiëren verlenen toestemming via website zorgaanbieder
In plaats van een QR-code scannen had ik ook naar de website van mijn huisarts of mijn apotheek kunnen gaan. Eenmaal ingelogd kon ik daar een QR-code laten aanmaken die ik met mijn telefoon moest scannen. Nadat ik de code had gescand werd mij gevraag of ik akkoord ging met de gegevensuitwisseling. Na mijn akkoord kwam de gegevensuitwisseling direct op gang.

Initiëren verlenen toestemming via doorgifte van een adres via een code
Een zorgaanbieder toevoegen was ook mogelijk geweest zonder dat ik naar de huisarts was gegaan of zou moeten inloggen op de website van mijn apotheek. Een code ingeven is ook mogelijk en door een telefoontje naar de assistente van Marlou, of even kijken op haar website, zou ik de code hebben kunnen verkrijgen.

8.2.3. De stappen voor gegevensuitwisseling

Ik heb zowel bij mijn huisarts als bij mijn apotheek toestemming verleend om gegevens uit te wisselen met mijn persoonlijke gezondheidsomgeving. Nadat ik toestemming had gegeven kwam de gegevensuitwisseling gelijk tot stand.

De initiële gegevensuitwisseling na verlenen toestemming
De autorisatie voor gegevensuitwisseling tussen mijn persoonlijke gezondheidsomgeving en het apothekerssysteem van Ed was de eerste stap om een overzicht te krijgen van de medicatie die door de apotheek aan mij verstrekt zijn. Een actueel medicatieoverzicht heet dat volgens Ed.

De autorisatie voor mijn mobiele app, mijn persoonlijke gezondheidsomgeving, had ik verkregen via de website van mijn apotheek. Daarover kun je meer lezen in het verhaal over mijn ervaringen met het autoriseren. Eenmaal akkoord gegeven zag ik medicatiegegevens binnenkomen in het actueel medicatieoverzicht van de app. Dit overzicht had ik daarna altijd beschikbaar, ook als ik met mijn telefoon even geen bereik had.

Veranderingen in de medicatie
Iedere keer als ik de medicijnen van een herhaalrecept of van een nieuw recept had gekregen zag ik dat mijn medicatieoverzicht werd bijgewerkt. Ik vond dat zo leuk dat ik dat aan Ed vertelde.

Hij reageerde gelijk ook heel enthousiast: “Mooi hè, iedere keer als wij medicijnen aan jou verstrekken wordt een melding naar jouw persoonlijke gezondheidsomgeving gestuurd.”
“En in die melding staat maar heel weinig, alleen de gebeurtenis dat er vandaag nieuwe medicatie is verstrekt. Vervolgens kan jouw persoonlijke gezondheidsomgeving aan het werk omdat het weet dat er nieuwe gegevens beschikbaar zijn.”

“Wat weet je er veel vanaf” 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. Wist je dat veel apps ook kunnen doorgeven welke medicatie je gebruikt, en dat je dat aan mij kunt doorgeven?”

"Ja, ik heb zoiets gezien in de app" zei ik. "Ik heb net een doosje paracetamol bij de drogist gehaald, zal ik dat erin zetten?" vroeg ik.

Aan de blik van Ed kon ik gelijk zien dat hij graag wilde dat ik het probeerde. Ik pakte daarom het doosje uit mijn tas samen met mijn telefoon. In de app kon ik inderdaad opgeven welke andere medicijnen nog aan mij verstrekt waren, en ik kon ook opgeven welke van de medicatie ik gebruikte. Ik voerde het doosje paracetamol op als verstrekte medicatie. Met het bewaren kon ik ook gelijk opgeven of ik de nieuwe gegevens wilde delen en met wie ik het wilde delen. Ik gaf op dat ik het mijn apotheek wilde delen en bevestigde mijn antwoord.

"Wat er nu gebeurt" zei Ed "is dat jouw persoonlijke gezondheidsomgeving contact opneemt met ons apotheeksysteem om het doosje paracetamol door te geven".

"Gaat dat ook met een melding?" vroeg ik.

"Nee" zei Ed, "dit wordt direct doorgegeven. Ik weet het niet precies maar het had geloof ik te maken dat ons apotheeksysteem anders van jouw telefoon gegevens zou moeten lezen, en dat gaat in de praktijk niet zo makkelijk."

"Maar ik heb het doosje paracetamol in mijn systeem staan" zei Ed helemaal blij.

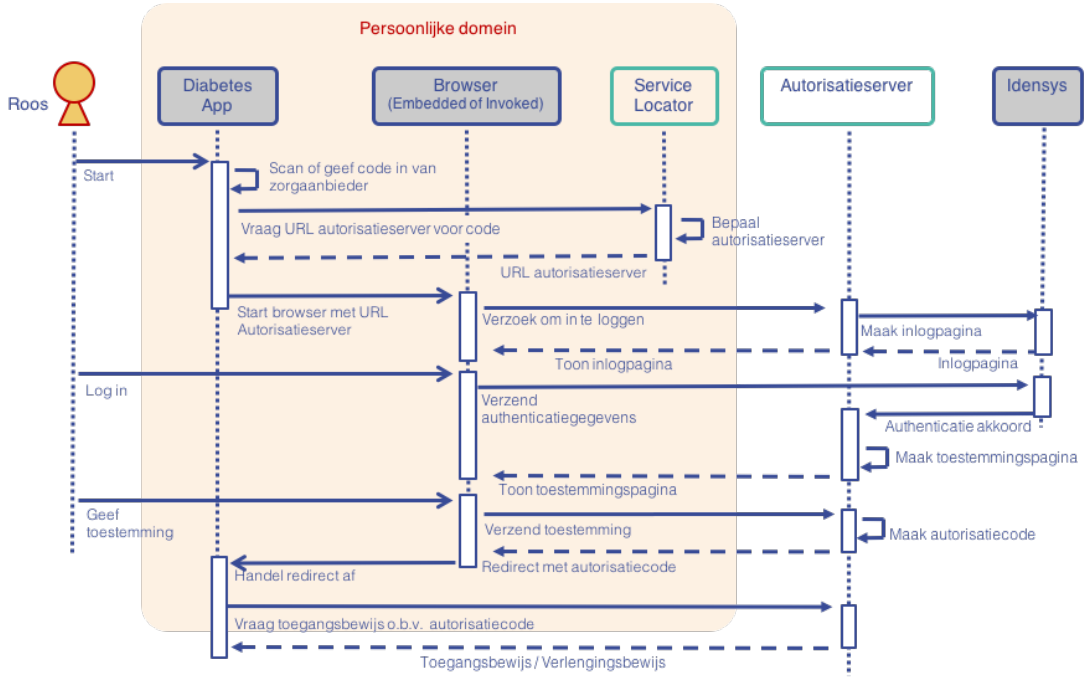
Voortaan ging ik alles bijhouden met mijn app en ging ik ook bijhouden wat ik wel en niet gebruikte. Naast dat ik Ed er heel erg blij mee maakte, had ik vooral zelf er veel baat bij. Ik had overal en altijd een actueel overzicht met wat ik aan medicatie verstrekt kreeg en wat ik gebruikte. Zeker in gesprekken met artsen was dat super.

8.3. Architecturale bouwstenen – sequentiediagrammen

In deze paragraaf is een technische uitwerking gerealiseerd als voorbeeld voor het realiseren van de diensten van een toegangsverleners. Het autoriseren van de gegevensuitwisseling is een realisatie van de autorisatiedienst en de gegevensuitwisseling van de gegevensuitwisselingsdienst.

8.3.1. Autoriseren van de gegevensuitwisseling

De techniek voor het autoriseren kan gerealiseerd worden met de open standaard van OAuth2. Deze standaard wordt veel toegepast door Google, Facebook, Twitter en anderen om applicaties te autoriseren voor toegang tot gegevens. Ook binnen de HL7 FHIR-community wordt gebruik gemaakt van OAuth2 om toegang te verkrijgen tot gegevens.



Afbeelding 12 Sequentiediagram van de OAuth2 stappen

In de bovenstaande afbeelding zijn de stappen weergegeven die OAuth2 uitvoert om de persoonlijke gezondheidsomgeving te autoriseren voor het verkrijgen van gegevens van het Huisartssysteem dat Marlou, de huisarts van Roos, gebruikt.

Een aantal stappen toegelicht

In de paragrafen hieronder worden een aantal specifieke stappen toegelicht uit het sequentiediagram.

– *Vragen URL voor autorisatieserver*
  De app[1] moet op basis van een code die de zorgaanbieder identificeert eerst het adres (URL) ophalen van de autorisatieserver. De code kan handmatig zijn ingegeven of via een QR-code verkregen.

– *Inloggen via Idensys*
  Voor de gegevensuitwisseling met het systeem van de huisarts is een identiteitsleverancier nodig op het hoogste betrouwbaarheidsniveau die eveneens het burgerservicenummer kan verlenen. In het verhaal is daarom voor Idensys gekozen. Andere systemen die het burgerservicenummer niet nodig hebben kunnen ook voor een andere leverancier kiezen, bijvoorbeeld iDIN[2].

[1] De app moet herkend kunnen worden als een legitieme app die gebruik mag maken van de service locator. Hiervoor wordt gedacht aan OAuth2 voor server-to-server (met een autorisatieserver van, en authenticatie door, de toegangsverlener). Een leverancier van een PERSOONLIJKE GEZONDHEIDSOMGEVING moet met deze techniek zich kunnen authentiseren bij de service locator. Een mogelijk veiliger alternatief is om alle interactie via de gateway te laten plaatsvinden met authenticatie door de gateway.

[2] Voor de combinatie OAuth2 en een identiteitsleverancier moet door middel van een proof-of-concept de werking worden bewezen.

Binnen de standaard van OAuth2 authentiseert de autorisatieserver de persoon en vraagt vervolgens aan de persoon of deze toestemming verleent voor de gegevensuitwisseling. Voor MedMij is het echter noodzakelijk dat de autorisatieserver een uitstap maakt naar de identiteitsleverancier voor het laten samenstellen van de inlogpagina en het daadwerkelijk authentiseren van de persoon.

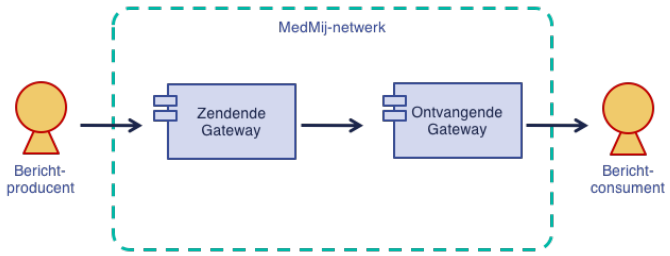
In het sequentiediagram is het verkrijgen van het attribuut burgerservicenummer via het BSN-Koppelregister niet opgenomen. Dit is noodzakelijk om een koppeling te realiseren tussen het toegangsbewijs en het burgerservicenummer. Op basis van de authenticatie moet de zorgaanbieder het burgerservicenummer kunnen achterhalen als attribuut. Zolang het BSN-Koppelregister niet beschikbaar is zal de zorgaanbieder het voor de gegevensstroom uitgegeven en gehanteerde pseudoniem in haar eigen administratie moeten koppelen aan het burgerservicenummer.

– *Toegangsbewijs en verlengingsbewijs*
  Het toegangsbewijs vormt het bewijs voor de persoonlijke gezondheidsomgeving dat deze de gegevens van de persoon mag opvragen bij het systeem van de zorgaanbieder, gebruik mag maken van het koppelvlak (api). Het toegangsbewijs wordt meegezonden met de berichten van de persoonlijke gezondheidsomgeving.

  Een toegangsbewijs heeft een beperkte geldigheid. Als het toegangsbewijs is verlopen kan met behulp van het verlengingsbewijs opnieuw een toegangsbewijs worden gevraagd. Op dat moment zal ook de authenticatie opnieuw moeten worden uitgevoerd (technisch niet noodzakelijk, maar mogelijk vanuit het oogpunt van beveiliging toch gewenst).

8.3.2. Gegevensuitwisseling

Voor de gegevensuitwisseling wordt gebruik gemaakt van het MedMij-netwerk. Het netwerk is een netwerk van toegangsverleners die samenwerken om berichten uit te wisselen tussen het persoonlijke domein en het zorg- en ondersteuningsdomein.



Afbeelding 13 Zendende en ontvangende gateways

Voor de gegevensuitwisseling wordt het component “Gateway” gebruikt. Tijdens de gegevensuitwisseling wordt per domein een gateway gehanteerd zodat er voor een bericht altijd een zendende gateway is en een ontvangende gateway, zoals hierboven weergegeven. Als een

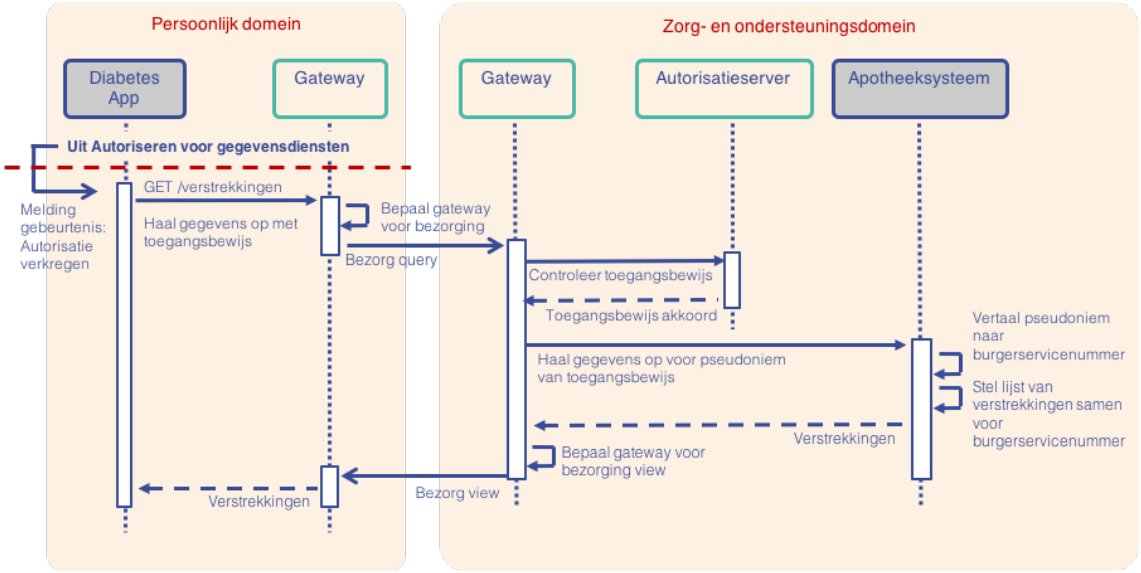
toegangsverlener diensten aanbiedt aan beide domeinen, dan zal deze toegangsverlener 2 gateways moeten implementeren.

Een aantal stappen toegelicht

In de paragrafen hieronder worden een aantal specifieke stappen uit het gebruiksscenario toegelicht.

– *Initieel ophalen van de medicatie*

Nadat Roos toestemming heeft verleend voor de gegevensuitwisseling worden alle verstrekkingen die de apotheek heeft uitgevoerd opgehaald. Het initieel ophalen van de gegevens heeft als doel dat de persoonlijke gezondheidsomgeving van start kan gaan met de op dat moment bekende gegevens. Dit is gebaseerd op de aanname dat de persoonlijke gezondheidsomgeving een eigen contextueel kader vormt, het een eigen gegevensstructuur heeft en zelfstandig moet kunnen functioneren.

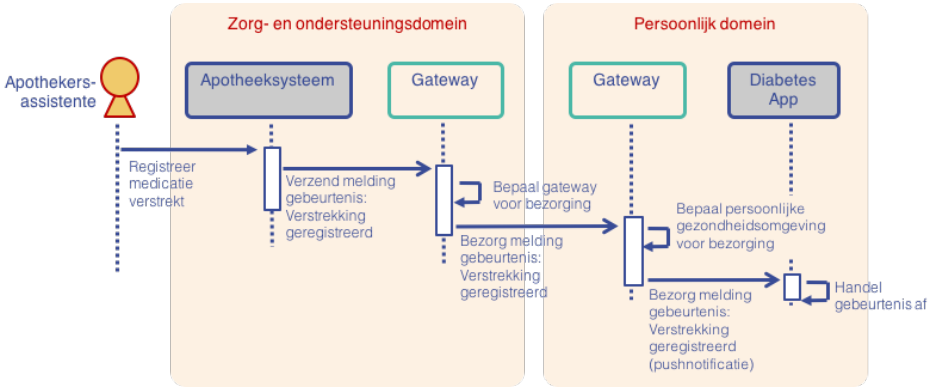


Afbeelding 14 Sequentiediagram voor ophalen verstrekkingen

– *Melden van een gebeurtenis*

Met het actuele medicatieoverzicht heeft de persoonlijke gezondheidsomgeving een actuele stand verkregen. Vanaf dat moment is het noodzakelijk dat de persoonlijke gezondheidsomgeving actueel blijft door wijzigingen op het overzicht te ontvangen en te verwerken. Een wijziging ontstaat door een gebeurtenis, bijvoorbeeld doordat medicatie aan Roos is verstrekt.

Een persoonlijke gezondheidsomgeving zal meldingen van gebeurtenissen ontvangen van de zorgaanbieder. Het betreft alleen de melding van de gebeurtenis, niet de gegevens die zijn geregistreerd bij de gebeurtenis.

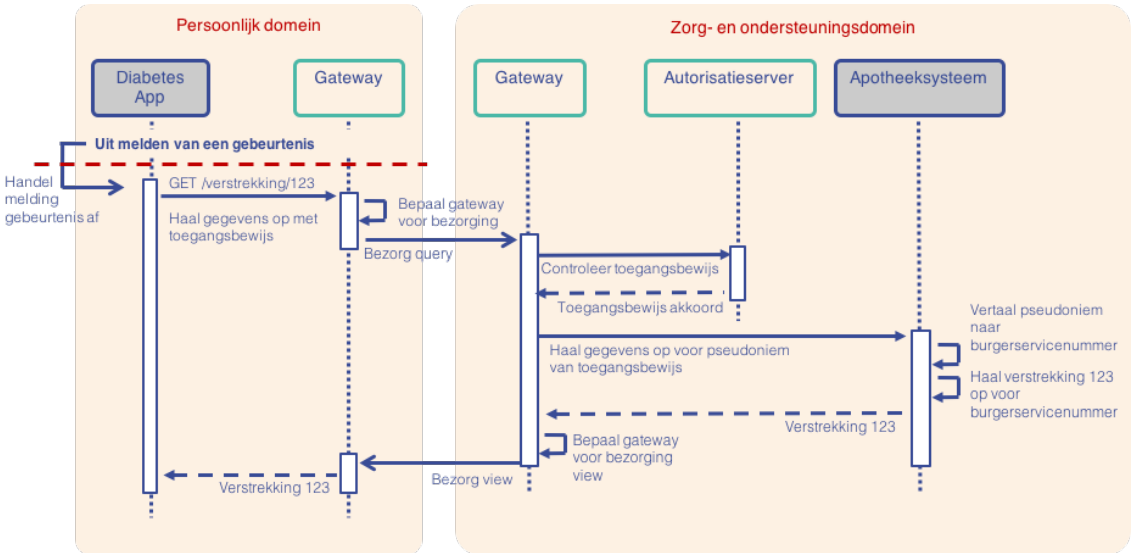


Afbeelding 15 Sequentiediagram voor melding gebeurtenis

Door de melding van gebeurtenissen is het niet noodzakelijk dat de app van Roos alle verstrekkingen moet ophalen voordat deze aan Roos kunnen worden getoond. De app is zelfstandig geworden en daardoor minder afhankelijk van de beschikbaarheid van het apothekerssysteem.

Een gateway moet voor het routeren en afleveren van meldingen kennis hebben van het adres van de persoonlijke gezondheidsomgeving. Uitgangspunt is dat de adressering door de zorgaanbieder wordt meegegeven met de melding.

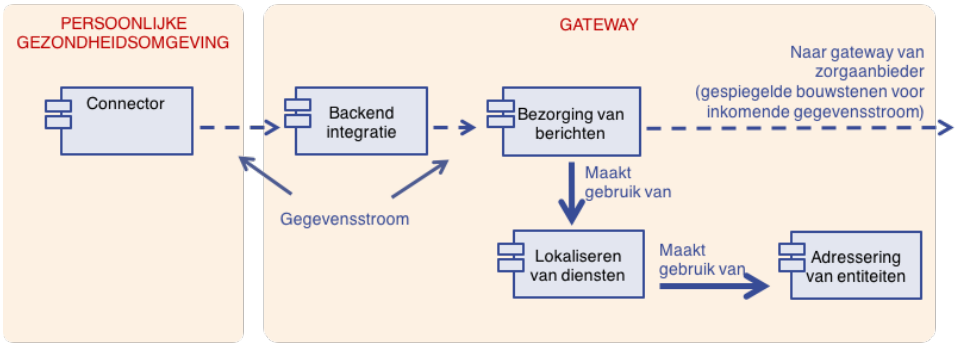
– *Ophalen gegevens naar aanleiding van melding gebeurtenis*
Nadat een melding van een gebeurtenis is ontvangen moeten de gegevens die bij de gebeurtenis zijn geregistreerd worden opgehaald. De werkwijze voor het ophalen van de gegevens is vrijwel identiek aan het ophalen van de initiële gegevens, met als verschil dat een andere vraag wordt gesteld voor het ophalen van de gegevens over de gebeurtenis.



Afbeelding 16 Sequentiediagram voor het ophalen van de gegevens van een gebeurtenis

8.4. Architecturale bouwstenen – berichtuitwisseling

De infrastructuur en de bouwstenen zijn gebaseerd op de integratiestijl van berichtuitwisseling. In onderstaande afbeelding zijn de bouwstenen in samenhang weergegeven.

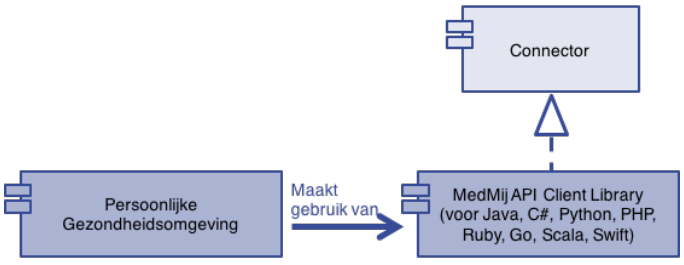


Afbeelding 17 Bouwstenen voor berichtuitwisseling

Het ontvangen van berichten is een spiegelbeeld van het verzenden van berichten. Via een connector koppelt een persoonlijke gezondheidsomgeving met de gateway, met een bouwsteen voor backend integratie. Tussen een connector en de backend integratie kan zowel een koppelvlak voor synchrone als asynchrone communicatie worden gerealiseerd. Gateways communiceren onderling altijd asynchroon. Door middel van adressering van berichten kan een gateway het afleveradres (een URL) van een gegevensdienst lokaliseren.

8.4.1. Connector

De connector is een bouwsteen die gebruikt kan worden door een leverancier van een persoonlijke gezondheidsomgeving en een zorgaanbieder voor het realiseren van een connectie met de toegangsverlener. Zoals hieronder getoond kan de connector in de vorm van een “MedMij API Client Library”, kort bibliotheek genoemd, beschikbaar worden gesteld. Per programmeertaal zal een bibliotheek moeten worden geïmplementeerd, zowel voor mobiel als voor webapplicaties.



Afbeelding 18 MedMij API Client Library als realisatie van een connector

Aangenomen wordt dat een connector concurrentieel is voor een toegangsverlener. Er moeten daarom afspraken worden gemaakt in hoeverre connectoren gezamenlijk worden ontwikkeld, door een toegangsverlener worden ontwikkeld dan wel met een gemeenschappelijk basis wordt

ontwikkeld. Dit is eveneens van toepassing op de limitatieve lijst van programmeertalen die gezamenlijk, dan wel alleen door de toegangsverlener, worden ondersteund door een bibliotheek.

De bibliotheek is vergelijkbaar met de Google API Client Library, zie https://developers.google.com/api-client-library/

Koppelvlak met een persoonlijke gezondheidsomgeving

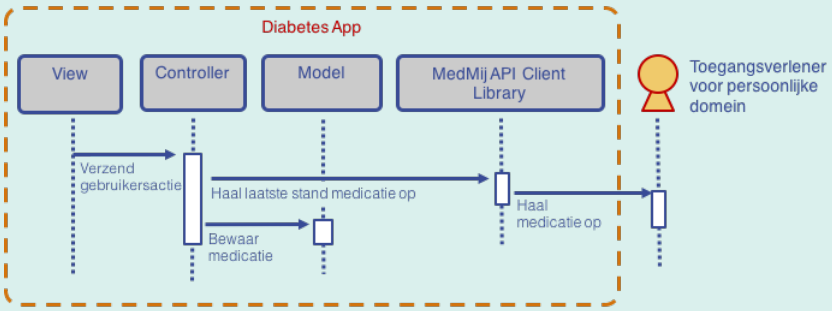
Een persoonlijke gezondheidsomgeving is het domein van de persoon, van de applicaties (apps) en de apparaten die de persoon gebruikt. Personen voeren de regie via een persoonlijke gezondheidsomgeving. Een persoonlijke gezondheidsomgeving wordt als één omgeving gerekend als de applicaties gebruik maken van hetzelfde platform, als de applicaties via het platform zijn geïntegreerd en gebruik maken van dezelfde database. Een persoon zou dus ook gebruik kunnen maken van meerdere persoonlijke gezondheidsomgevingen als hij of zij gebruik maakt van meerdere platformen.

Afbeelding 19 Aspecten van een persoonlijke gezondheidsomgeving

Een persoonlijke gezondheidsomgeving kan op diverse manieren zijn vormgegeven. Een persoon bepaalt uiteindelijk welke applicaties en apparaten hij of zij gebruikt en welke platformen hieronder zitten en worden gebruikt voor de integratie van de gegevens. De beschrijving hieronder geeft een voorbeeld van een aansluiting op het MedMij-netwerk.

Roos, 54 jaar, heeft diabetes type 2.
Roos gebruikt een bloedglucosemeter om de hoogte van haar bloedsuikers te volgen en ze gebruikt eveneens een slimme weegschaal om haar gewicht in de gaten te houden. Beide apparaten hebben een begeleidende iOS-app die zorgdraagt voor integratie met het platform van haar persoonlijke gezondheidsomgeving. Het platform bewaart de waarden in een versleutelde database.

Roos kan de rapportages en statistieken van de metingen zien in haar diabetes-app omdat deze app integreert met hetzelfde platform, en dat allemaal op haar iPhone. De diabetes-app ondersteunt MedMij, wat inhoud dat Roos de gegevens kan delen met zorgaanbieders.



De meeste iOS- en Android-apps hanteren een Model-View-Controller patroon zoals getoond in het sequentiediagram hierboven. De diabetes-app roept een service van de toegangs-provider aan om de medicatie op te halen. De diabetes-app bewaart de gegevens lokaal op de iPhone. Alle medicatiegegevens worden versleuteld opgeslagen in de database. Helaas ondersteunt het platform geen gestructureerde opslag van medicatiegegevens. De diabetes-app kan daarom niet de services van het platform gebruiken voor het bewaren van de medicatie, maar moet hierin voorzien met een eigen oplossing.

Met haar persoonlijke gezondheidsomgeving kan Roos regie nemen over haar diabetes. Deze omgeving bestaat niet alleen uit haar diabetes-app, maar ook uit haar bloedglucosemeter, de slimme weegschaal en de apps die bij deze apparaten horen. Het platform op haar iPhone laat al deze apps en apparaten met elkaar samenwerken tot 1 omgeving.

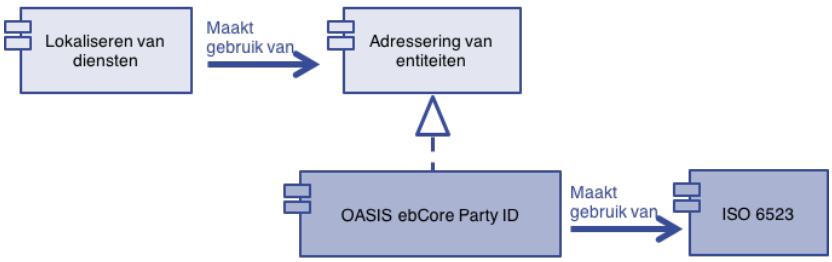
Aangenomen wordt dat een persoonlijke gezondheidsomgeving bestaat uit verschillende technologieën met verschillende architecturen. De aanname is dat de architectuur van een persoonlijke gezondheidsomgeving niet eenduidig kan worden weergegeven maar divers is. Daardoor is standaardisatie van het koppelvlak niet wenselijk. Verschillende soorten koppelvlakken met verschillende soorten protocollen (RESTful, SOAP, AMQP, MQTT of andere) zullen noodzakelijk zijn. Het wordt daarom aan de toegangsverlener overgelaten om een portfolio van koppelvlakken op te stellen waarmee zij haar markt kan bedienen en zich kan onderscheiden.

Koppelvlak met het systeemlandschap van zorgaanbieder en overheden
De meeste informatiesystemen van zorgaanbieders en overheden worden geleverd door commerciële partijen, en zijn veelal standaardapplicaties. Veelal wordt ook gebruik gemaakt van integratiesoftware, zeker als bijvoorbeeld de zorgaanbieder een grotere partij is zoals een ziekenhuis met een compleet systeemlandschap aan applicaties.

De verwachting is dat toegangsverleners connectoren en/of adapters zullen aanbieden om aan te sluiten op het MedMij-netwerk. Connectoren die opgenomen kunnen worden in het systeemlandschap van een zorgaanbieder. Connectoren kunnen functionaliteit voor transformatie en translatie bevatten.

8.4.2. Adressering van entiteiten
De URI die gebruikt wordt om de zorgaanbieder te identificeren ten behoeve van het lokaliseren van diensten is een OASIS ebCore Party ID, een URI met daarin een unieke code voor de zorgaanbieder

gebaseerd op ISO 6523. De code die gebruikt wordt voor de identificatie van de zorgaanbieder zou bijvoorbeeld het KvK-nummer kunnen zijn.

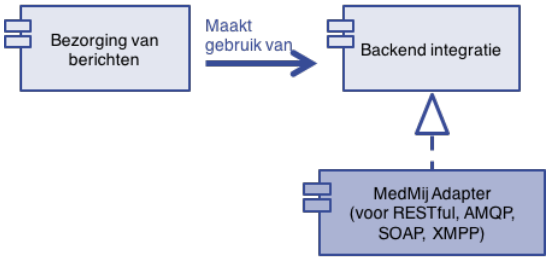


Afbeelding 20 OASIS ebCore Party ID voor de notatie van adressen

De adressering van entiteiten wordt gebruikt voor het adresseren van berichten zodat een toegangsverlener het bericht naar de juiste gebruiker kan verzenden.

8.4.3. Backend integratie

Gebruikers maken gebruik van koppelvlakken voor het verzenden van berichten en voor het ontvangen van berichten. Ook voor de query's en views zijn koppelvlakken nodig. De bouwsteen voor de backend integratie moet voor deze koppelvlakken zorgdragen. De koppelvlakken zijn asynchroon voor het verzenden van meldingen van gebeurtenissen en kunnen synchroon zijn voor het verzenden van opdrachten (bijvoorbeeld voor het ophalen van gegevens).



Afbeelding 21 Adapters voor realisatie backend integratie

De verwachting is dat toegangsverleners meerdere soorten adapters zullen ontwikkelen als koppelvlak naar hun diensten. Voor de hand liggende adapters zijn adapters voor RESTful (HL7 FHIR) en SOAP (HL7v3).

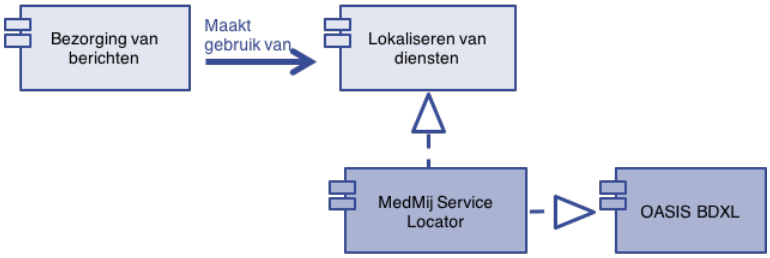
Transformatie en translatie

Binnen het verantwoordelijkheidsdomein van een leverancier van een persoonlijke gezondheidsomgeving of in het domein van een zorgaanbieder kan de behoefte ontstaan om uitwisselingsformaten te transformeren (verandering van syntax) of te transleren (verandering van semantiek). Translaties zijn bijvoorbeeld noodzakelijk als uitwisselingsformaten verschillende terminologie hanteren.

Toegangsverleners kunnen in de backend integratie aanvullende diensten leveren voor het transformeren en transleren van berichtformaten. Dit onder de aanname dat toegangsverleners de diensten leveren als bewerker in de betekenis van de Wbp.

8.4.4. Lokaliseren van diensten

Het lokaliseren van diensten vertaalt een URI met daarin een unieke code van een gebruiker naar een URL van het koppelvlak van een gateway die het bericht gaat afleveren. Het lokaliseren van diensten betreft alleen de diensten van de gateway en van de autorisatieserver. Het daadwerkelijk afleveren van het bericht bij een gebruiker is een verantwoordelijkheid van de toegangsverlener.



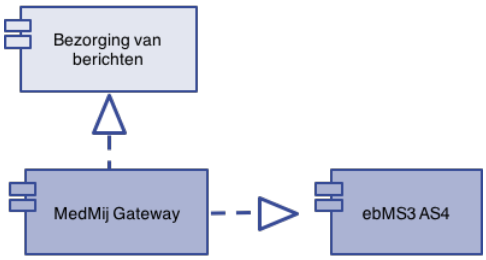
Afbeelding 22 MedMij Service Locator is een implementatie van OASIS BDXL

Voor het lokaliseren van diensten moet de optie tot distributie van routeringsregels worden onderzocht. Een journaal van routeringsregels zou gedistribueerd kunnen worden naar alle toegangsleveranciers en aldaar opgenomen kunnen worden in de Service Locator. Dit betekent dat iedere toegangsverlener haar eigen bouwsteen realiseert voor het lokaliseren van diensten en daarvoor OASIS BDXL zou kunnen implementeert. Door de verantwoordelijkheid voor het lokaliseren van diensten bij de toegangsverlener te plaatsen verkrijgt deze echter vrijheid om haar eigen implementatie te kiezen.

8.4.5. Bezorging van berichten

Het bezorgen van berichten is de kerndienst voor een toegangsverlener. Via de adapters worden gegevens op verschillende manieren ontvangen van gebruikers en eventueel getransformeerd tot een bericht. Ook de aflevering naar gebruikers verloopt via een adapter. Het koppelvlak tussen de gateways van toegangsverleners is vast gedefinieerd en implementeert OASIS ebMS3 AS4 met als uitbreiding de ondersteuning van het berichtuitwisselingspatroon voor tweezijdige communicatie ten behoeve van request-reply.

De keuze voor ebMS3 AS4 is gebaseerd op het principe om te kiezen voor open internationale standaarden, is gebaseerd op het feit dat ebMS reeds gekozen is als standaard binnen zowel de gezondheidszorg als bij de overheden en de aanname dat voor MedMij gekozen moet worden voor de meest recente stabiele versie. Daarnaast kan aangenomen worden dat met de keuze van ebMS3 AS4 voldaan kan worden aan de eisen ten aanzien van de bezorging van berichten omdat dit reeds bewezen technologie is.



Afbeelding 23 De MedMij Gateway implementeert ebMS3 AS4 voor de bezorging van berichten

Aangenomen wordt dat voor het verzenden van berichten twee patronen voor berichtuitwisseling nodig zijn, namelijk “One-Way/Push” voor meldingen over gebeurtenissen en “Two-Way/Push-and-Push” voor opdrachten om bijvoorbeeld gegevens op te halen. Het eerste patroon is een eenrichtingsweg voor berichten die niet direct een antwoord verwachten of geen antwoord verwachten. Het tweede patroon heeft betrekking op berichten die een request-response verlangen. Op basis van een identificatienummer worden de berichten in dit patroon aan elkaar gerelateerd.

8.5. Architecturale bouwstenen – vertrouwen, integriteit en onweerlegbaarheid

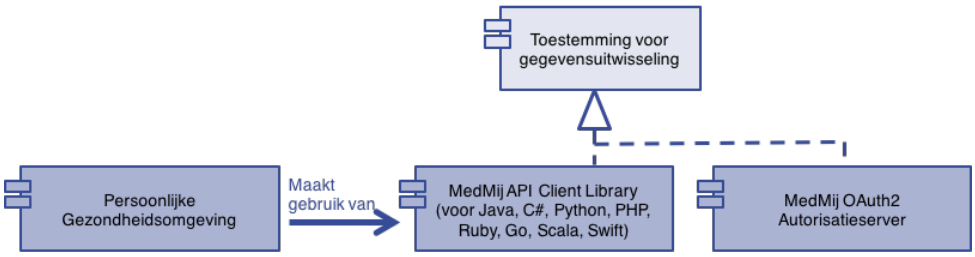
Personen verzamelen persoonlijke gezondheidsgegevens, waaronder medische gegevens. Dat zijn gegevens met een hoog risicoprofiel waarvoor de privacy gewaarborgd moet worden. Er moet dan ook met een substantiële of hoge mate van zekerheid vastgesteld kunnen worden dat een persoon alleen zijn of haar eigen gegevens verzamelt. Daarnaast zijn maatregelen noodzakelijk om de gegevens te beveiligen tijdens het transport.

Authenticatie van personen is geen bouwsteen in het MedMij-netwerk omdat hiervoor gebruik wordt gemaakt van externe identiteitsleveranciers (bijvoorbeeld iDIN of Idensys).

8.5.1. Toestemming voor gegevensuitwisseling

Een persoon moet toestemming geven voor de gegevensuitwisseling tussen een persoonlijke gezondheidsomgeving en de zorgaanbieder. Hiervoor zal OAuth2 worden geïmplementeerd. Dit betekent een interactie tussen een persoonlijke gezondheidsomgeving en een OAuth2 autorisatieserver.

Voor het vereenvoudigen van de interactie aan de persoonlijke gezondheidsomgeving zou gebruik kunnen worden gemaakt van de eerder geïntroduceerde bibliotheek. Aan de interactiekant van de zorgaanbieder moet een OAuth2 autorisatieserver worden gerealiseerd. Een toegangsverlener kan deze aanbieden.



Afbeelding 24 Toestemming voor gegevensuitwisseling via OAuth2

8.5.2. Authenticatie van gebruikers

Zowel voor een persoonlijke gezondheidsomgeving als voor het systeem van een zorgaanbieder vindt authenticatie plaats. Een toegangsverlener moet maatregelen nemen om de legitimiteit van het gebruik van de diensten vast te kunnen stellen. Een toegangsverlener heeft meerdere mogelijkheden om een leverancier van een persoonlijke gezondheidsomgeving of een zorgaanbieder te authentiseren, waarbij gedacht kan worden aan de uitgifte van een toegangsbewijs of gebruik maken van PKI-certificaten zoals het UZI-servercertificaat of het VECOZO-servercertificaat.

8.5.3. Vertrouwd netwerk door wederzijds erkende certificaten

Het netwerk tussen de gateways moet een vertrouwd netwerk zijn in die zin dat gateways andere gateways moeten herkennen en kunnen authentiseren als een vertrouwd systeem. Door een lijst te hanteren van vertrouwde gateways en hun certificaten (PKI-Overheid) kan dit worden gerealiseerd. Iedere gateway accepteert alleen berichten via de bouwsteen bezorging van berichten als deze worden bezorgd door een vertrouwde gateway.

8.5.4. Ondertekening van documenten

Voor gegevens afkomstig van zorgaanbieders is zowel de integriteit van het document als de onweerlegbaarheid van de herkomst van belang. De herkomst van het document is in deze de gegevensproducent zijnde een praktijk of instelling. De gegevens in een document moeten daarom digitaal ondertekend worden met een gekwalificeerd certificaat (PKI-Overheid) die de zorgaanbieder authentiseert met een hoog betrouwbaarheidsniveau. De ondertekening vindt plaats op de gegevens in het document, is onderdeel van het document en bewaakt de integriteit van het document, niet van de gegevens in de envelop van het bericht. De zorgaanbieder is verantwoordelijk voor het plaatsen van haar handtekening. De handtekening moet een geavanceerde elektronische handtekening (ADS) zijn door middel van bijvoorbeeld XML Advanced Electronic Signatures (XAdES) of PDF Advanced Electronic Signatures (PAdES). Met betrekking tot andere formaten moet worden onderzocht hoe de digitale handtekening kan worden meegezonden. Het valt echter op het moment van schrijven niet uit te sluiten dat de afspraak tot integriteit en onweerlegbaarheid beperkende gevolgen kan hebben voor de uitwisselingsformaten.

Voor de integriteit van documenten afkomstig van een persoonlijke gezondheidsomgeving wordt de afspraak vastgelegd dat de integriteit van de gegevens tussen de gateways wordt bewaakt door middel van een digitale handtekening van de gateway. Afspraken omtrent maatregelen voor de bewaking van de integriteit tussen gebruiker en gateway zijn geen onderdeel van het afsprakenstelsel. De herkomst van documenten afkomstig van een persoonlijke

gezondheidsomgeving kan bepaald worden op basis van het toegangsbewijs dat wordt meegezonden als bijlage in het bericht, het toegangsbewijs dat verkregen is bij het autoriseren van de gegevensuitwisseling.

8.5.5. Traceerbaarheid naar de herkomst van een bericht

Met de traceerbaarheid van berichten via een logboek wordt niet noodzakelijk de traceerbaarheid bedoelt naar de herkomst van de gegevens, naar de gegevensproducent. Een logboek is namelijk niet onweerlegbaar bewijs van de herkomst, maar het is een hulpmiddel om de logistieke afhandeling van berichten te verantwoorden. De gegevensproducent van gegevens wordt onweerlegbaar geauthentiseerd door middel van een digitale handtekening.

Traceerbaarheid betreft de traceerbaarheid waar berichten vandaan komen en waar ze naar toe zijn gegaan. Als een bericht wordt ontvangen of afgeleverd, dan wordt dit in een logboek vastgelegd. Zo kan een toegangsverlener altijd een overzicht van inkomende en uitgaande berichten tonen waarbij per inkomend bericht verantwoord kan worden dat deze juist is afgeleverd. Hiervoor is de afspraak noodzakelijk dat ieder bericht uniek wordt geïdentificeerd en met het unieke nummer gevolgd kan worden door de keten.

8.5.6. Bescherming van persoonsgegevens

Tussen de gateways worden de gegevens beschermd door zowel versleuteling van de documenten als versleuteling van het kanaal (TLS). Aangenomen wordt echter dat end-to-end versleuteling van documenten ook als een passende maatregel gezien moet worden. Dit vanuit het principe van gegevensbescherming door ontwerp. End-to-end betekent in deze versleuteling door een persoonlijke gezondheidsomgeving en ontcijfering door het zorgaanbiedersysteem (en vice versa).

Bescherming van gegevens tussen dienstaanbieder en gateway is een verantwoordelijkheid van de toegangsverlener. Afspraken omtrent maatregelen worden beperkt tot het voldoen aan de normen voor gegevensuitwisseling binnen de zorg (NEN 7512) met als aanscherping dat versleuteling van documenten als een passende maatregel moet worden gezien.

Bijlage 1 Referenties

[1] Zelfzorg Ondersteund, “Minimale basiseisen en normenkader | Zelfzorg Ondersteund”. .

[2] F. Bijl, “PvE GBP (v0 993 concept)”. vZVZ, 20-apr-2016.

[3] L. Bierma en M. Heldoorn, “Het persoonlijk gezondheidsdossier, de visie van patiëntenfederatie NPCF”. jun-2013.

[4] T. Hooghiemstra, “Juridische aspecten Persoonlijke gezondheidsomgeving”. 02-dec-2016.

[5] Het Europees parlement en de Raad van de Europese Unie, *Algemene verordening gegevensbescherming)*. 2016.

[6] *Privacy by design: the 7 foundational principles*. Office of the Information and Privacy Commissioner, 2009.

[7] M. Fowler, “Datensparsamkeit”, *martinfowler.com*, 12-dec-2013. [Online]. Beschikbaar op: http://martinfowler.com/bliki/Datensparsamkeit.html.