Identificatie, authenticatie & autorisatie

MedMij
Grip op je eigen gezondheidsgegevens

Voor het uitwisselen van gezondheidsgegevens binnen het MedMij-netwerk zijn twee partijen nodig, namelijk een persoon met een persoonlijke gezondheidsomgeving (een website of app) en een zorgaanbieder die gezondheidsgegevens opslaat in een informatiesysteem. MedMij stelt een afsprakenstelsel op met daarin spelregels voor deze uitwisseling. In dit afsprakenstelsel staat een duidelijke set kwaliteitseisen en informatiestandaarden waaraan de ICT-leveranciers van de persoonlijke gezondheidsomgevingen en de zorginformatiesystemen moeten voldoen om aangesloten te zijn op het MedMij-netwerk. Eén van de ontwerpprincipes die aan de basis staat van het MedMij Afsprakenstelsel is:

Gezondheidsgegevens worden veilig gepresenteerd, met optimale bescherming van de privacy en oog voor gebruiksvriendelijkheid.

Inloggen en authenticatie

Binnen MedMij wordt een onderscheid gemaakt tussen de toegang tot je eigen persoonlijke gezondheidsomgeving enerzijds en het opvragen van je gezondheidsgegevens via de benodigde digitale identificatie aan de hand van het Burgerservicenummer (BSN) bij de zorgaanbieder anderzijds. Deze laatste identificatie is nodig om aan te kunnen tonen dat 'jij ook echt jij bent' en dat je mag beschikken over de gegevens die bij het BSN horen uit het medisch dossier in het informatiesysteem van de zorgaanbieder.

Zorgaanbieders zijn wettelijk verplicht het BSN van patiënten vast te leggen in hun systeem en patiënten te identificeren zodat vastgesteld kan worden dat de gegevens uit het dossier ook bij de persoon horen die voor hun staat. Om die reden vragen erkende zorgaanbieders patiënten om een geldig legitimatiebewijs. De informatiesystemen van zorgaanbieders bevinden zich daarmee in het BSN-domein, waar de overheid toezicht op houdt.

Ook in de architectuur van MedMij is gedefinieerd dat bij het uitwisselen van gegevens tussen patiënt en zorgprofessional de persoon wordt geïdentificeerd aan de hand van een BSN. Deze plicht ligt overigens niet bij leveranciers van persoonlijke gezondheidsomgevingen, omdat de omgevingen onderdeel zijn van het persoonlijke domein. De informatiesystemen van zorgaanbieders liggen wel binnen het BSN-domein, waardoor identificatie aan de hand van BSN onder de verplichting van zorgaanbieders valt. Na de identificatie bij de zorgaanbieder kan de patiënt toestemming (autorisatie) geven en idealiter ook een abonnement vastleggen voor het uitwisselen van gezondheidsinformatie met de zorgaanbieder.

Binnen het MedMij-netwerk en de persoonlijke gezondheidsomgeving worden gezondheidsgegevens verwerkt die behoren tot de bijzondere persoonsgegevens. Deze gegevens vragen bescherming op een substantieel of hoog betrouwbaarheidsniveau op grond van onderzoek[1] dat is uitgevoerd aan de hand van jurisprudentie, specifieke beveiligingsnormen en bestaande privacy-wetgeving, zoals de 'Wet bescherming persoonsgegevens' (vanaf 2018 de 'Algemene verordening gegevensbescherming') en de Europese eIDAS-verordening. De Wet bescherming persoonsgegevens schrijft voor dat er passende beveiligingsmaatregelen moeten worden getroffen om bijzondere persoonsgegevens te beschermen. De maatregelen die binnen MedMij als passend worden bestempeld, volgen later dit jaar uit een risicoanalyse en worden verwerkt in een normenkader beveiliging van het afsprakenstelsel.

[1] PrivacyCare & PBLQ 2016
J. Krabben en T.Hooghiemstra, 'Betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de Zorg' in opdracht van de minister van VWS.

Identificatie en authenticatie aan de hand van het BSN onder verantwoordelijkheid zorgaanbieder

Om digitaal te identificeren is een authenticatiemiddel nodig. MedMij kan en gaat deze authenticatiemiddelen niet zelf ontwikkelen. Er is een landelijk programma, eID, dat burgers en bedrijven in staat stelt om veilig online (overheids)diensten af te nemen of hun zaken (met de overheid) digitaal te regelen. MedMij sluit vanwege efficiency aan op de landelijke ontwikkeling, maar ook omdat de wetgeving op het gebied van gezondheidzorg, privacy en beveiliging van gegevens in toenemende mate bepaald wordt door Europese regels. Bijvoorbeeld de eIDAS-verordening, die de toegang tot online dienstverlening regelt. Om aan deze Europese regels te kunnen voldoen zijn authenticatiemiddelen met een substantieel of hoog betrouwbaarheidsniveau noodzakelijk. In Nederland zijn deze middelen momenteel nog niet breed beschikbaar voor de identificatie aan de hand van het BSN, maar vanaf september 2018 moeten alle Europese burgers, consumenten en vertegenwoordigers van bedrijven bij alle Nederlandse organisaties in de publieke sector kunnen inloggen met hun eigen nationale inlogmiddel. Het is de bedoeling dat alle Nederlandse publieke organisaties vóór september 2018 eIDAS-proof zijn op het gebied van online toegang. Idensys is het publiek-private Nederlandse systeem voor elektronische identificatie (eID). Het ontwikkelt in dat kader de Nederlandse standaard voor toegang tot digitale dienstverlening en uitwisseling van persoonlijke informatie met de overheid en het bedrijfsleven.

MedMij sluit aan bij deze landelijke ontwikkeling van het eID-stelsel. DigiD op betrouwbaarheidsniveau ‘substantieel’ wordt volgens het Ministerie van Binnenlandse Zaken vanaf september 2017 uitgerold bij diverse partijen. Dit middel zal dus allereerst worden ingezet. MedMij volgt de planning van de minister geschetst in de kamerbrief van 23 juni 2017 ‘Voortgangsrapportage programma eID’ om binnen 3 jaar middelen op niveau ‘hoog’ toe te passen en heeft het Informatieberaad Zorg gevraagd om alles in het werk te stellen deze zo snel mogelijk breed beschikbaar te krijgen. Daarnaast ondersteunt MedMij de ontwikkeling van deze middelen door ze te gaan testen in een MedMij-kickstartomgeving.

Toegang tot de persoonlijke gezondheidsomgeving

Aan de toegangsverlening tot de persoonlijke gezondheidsomgeving stelt MedMij aparte eisen via het normenkader beveiliging (deze eisen volgen later dit jaar). Er is goede toegangsbeveiliging tot de persoonlijke gezondheidsomgeving noodzakelijk. De gevoeligheid van de gegevens maakt dat deze alleen beschikbaar moeten zijn voor de persoon die de persoonlijke gezondheidsomgeving heeft aangemaakt of aangeschaft. Omdat een persoonlijke gezondheidsomgeving buiten het BSN-domein valt is de omgeving niet gerechtigd zelf het BSN te verwerken. Authenticatiemiddelen die resulteren in een BSN (bijvoorbeeld DigiD) zijn daarom niet te gebruiken. Kortom: als er gegevensuitwisseling plaats vindt, moet de identiteit van een persoon onomstotelijk worden vastgesteld door de zorgaanbieder. MedMij zorg ervoor dat deze spelregels vastgelegd worden in het MedMij Afsprakenstel.

Begrippenlijst

Authenticatie
De controle van een geclaimde identiteit van een persoon en de set van zijn geclaimde attributen op een bepaald betrouwbaarheidsniveau, zodat kan worden aangetoond dat degene die zich identificeert ook daadwerkelijk degene is die zich als zodanig voorgeeft.

Autorisatie
Het verlenen van toestemming (een bevoegdheid) aan een geauthentiseerde partij om toegang te krijgen tot een bepaalde dienst of toestemming om een bepaalde actie uit te voeren.

eID-stelsel
Het eID-stelsel is een Nederlands stelsel en stelt burgers en bedrijven in staat om veilig online (overheids)diensten af te nemen of hun zaken (met de overheid) digitaal te regelen.

eIDAS
Met eIDAS wordt de eIDAS-verordening bedoeld. eIDAS is de Europese Verordening voor elektronische identiteiten en vertrouwensdiensten die sinds 1 juli 2016 van kracht is. Deze Verordening brengt door de invoering van nieuwe verplichtingen belangrijke veranderingen voor aanbieders van elektronische identificatiemiddelen en bepaalde vertrouwensdiensten teweeg.
Op basis van de eIDAS-verordening is ook een platform beschikbaar dat organisaties in de toekomst de mogelijkheid biedt om gebruikers, uit alle Europese lidstaten, op een betrouwbare manier te identificeren. Deze identificatie maakt het mogelijk om aan alle Europeanen, vanuit elke Europese lidstaat, online diensten te verlenen.

Identificatie
Het bekend maken van de identiteit van personen, organisaties of IT-voorzieningen.

Wilt u meer informatie over identificatie, authenticatie en autorisatie?
Stuurt u ons dan een e-mail via **info@medmij.nl**.

Disclaimer:
Het MedMij Afsprakenstelsel en de architectuur die daar onderdeel van is, blijft zich in de loop van 2017 ontwikkelen. Deze factsheet is opgesteld met de kennis tot en met augustus 2017.

MedMij

WWW.MEDMIJ.NL