Vertrouwen, veiligheid & privacy

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. Daarin staat één duidelijke set kwaliteitseisen en informatiestandaarden waar de ICT-leveranciers van de persoonlijke gezondheidsomgevingen en de zorginformatiesystemen aan moeten voldoen om aangesloten te zijn op het MedMij-netwerk. Om veiligheid en privacy te borgen, staan een aantal uitgangspunten en ontwerpprincipes aan de basis van het MedMij Afsprakenstelsel.

Uitgangspunten & ontwerpprincipes

Veel van de regels op het gebied van veiligheid en privacy zijn wettelijk vastgelegd, bijvoorbeeld in de Wet bescherming persoonsgegevens (Wbp) en (vanaf 2018) de Europese algemene verordening gegevensbescherming (AVG). Dat geldt ook, in toenemende mate, voor de regels rondom de digitale identiteit van burgers. MedMij wil dat gebruikers uitwisseling via het MedMij-netwerk kunnen vertrouwen en hanteert daarom de volgende uitgangspunten en ontwerpprincipes:

a. **Gegevensbescherming door ontwerp (privacy-by-design).**
Dit houdt – onder meer – in dat de verwerking van persoonsgegevens door technische en organisatorische maatregelen wordt beschermd. Het concept van Privacy-by-Design houdt nauw verband met het principe van ‘dataminimalisatie’: niet meer persoonsgegevens verwerken dan noodzakelijk. De manier waarop dit gebeurt is transparant en personen kunnen controle uitoefenen op de gegevensverwerking.

b. **Gegevensbescherming door standaardinstellingen.** Dit houdt in dat er nooit méér persoonsgegevens worden opgeslagen dan nodig is en waarvoor toestemming is verleend. De standaardinstellingen zorgen er ook voor dat persoonsgegevens niet langer worden bewaard dan noodzakelijk of toegestaan en dat ze niet automatisch voor een onbeperkt aantal personen toegankelijk kunnen worden gemaakt.

c. **Zo veilig als nodig.** Gezondheidsgegevens zijn doorgaans van een hoog betrouwbaarheidsniveau en moeten om die reden goed beveiligd worden. De ‘Wet bescherming persoonsgegevens’ (vanaf 2018 de ‘Algemene verordening gegevensbescherming’) schrijft voor dat er passende beveiligingsmaatregelen moeten worden getroffen om deze bijzondere persoonsgegevens te beschermen. Dat betekent onder andere dat de toegang voor patiënten tot hun gezondheidsgegevens en de gegevensuitwisseling op een substantieel of hoog betrouwbaarheidsniveau (in de zin van de eIDAS-verordening) geregeld moeten worden. De maatregelen die hiervoor als passend worden bestempeld binnen MedMij, volgen later dit jaar uit een risicoanalyse op het stelsel en worden verwerkt in het normenkader beveiliging. Dit normenkader maakt onderdeel uit van het MedMij Afsprakenstelsel.

Hoe passen de gekozen ontwerpprincipes in een architectuurmodel?

Een ICT-architectuurmodel creëert samenhang tussen de doelstellingen van een organisatie en een technisch ontwerp dat bijdraagt aan het realiseren van deze doelstellingen. Een goed architectuurmodel helpt MedMij om orde te brengen in het grote aanbod van gegevens en systemen die potentieel onderdeel uitmaken van, of in verbinding staan met, een persoonlijke gezondheidsomgeving.
De volgende twee perspectieven op het architectuurmodel geven een goed beeld van de beoogde privacy- en beveiligingsmaatregelen:

1. De functionele architectuur laat zien welke functies nodig zijn om de uitwisseling van gezondheidsgegevens mogelijk te maken. Functies die bijdragen aan de veiligheid en privacy zijn:

a. **Authenticeerfunctie.** Deze controleert of patiënten die gezondheidsgegevens opvragen daadwerkelijk zijn wie zij beweren te zijn. Het is de verantwoordelijkheid van de zorgaanbieder om de patiënt op hoog betrouwbaarheidsniveau (eIDAS) te identificeren aan de hand van het BSN. Wilt u hier meer over weten? Zie de factsheet ‘Identificatie, authenticatie en autorisatie’.

b. **Toestemmingsfunctie.** Hiermee verlenen patiënten toestemming aan zorgaanbieders voor het beschikbaar stellen van gezondheidsgegevens ten behoeve van hun persoonlijke gezondheidsomgeving;

c. **Logfunctie.** Deze functie zorgt ervoor dat handelingen in het netwerk herleidbaar zijn.

2. De technische architectuur toont de informatiemodellen, applicaties, en IT-infrastructuur elementen en laat zien hoe het persoonlijke domein van een patiënt en het domein van een zorgaanbieder met elkaar in verbinding staan. De technische architectuur bevat, als aanvulling op het functionele perspectief, een aantal MedMij-netwerkfuncties dat bijdraagt aan veiligheid en privacy:

a. **Een veilige dataverbinding.** MedMij ziet erop toe dat gegevens tussen aangesloten partijen alleen via beveiligde verbindingen uitgewisseld kunnen worden en dat alleen door MedMij vertrouwde partijen toegang hebben tot het netwerk;

b. **Geen centraal register van gegevens.** Gezondheidsgegevens worden niet op een centrale plek opgeslagen, maar blijven op de huidige plek opgeslagen, zoals bijvoorbeeld bij een huisarts.

Privacy en veiligheid krijgt aandacht binnen MedMij

Privacy en veiligheid krijgt binnen MedMij de hoogst mogelijke aandacht. Al in een vroeg ontwikkelstadium is een privacy gap assessment uitgevoerd om de opzet van het stelsel te toetsen. Ook zijn gedurende het ontwikkeltraject privacy- en veiligheidsexperts betrokken. De uiteindelijke privacy- en beveiligingsmaatregelen voor MedMij worden nog vastgesteld aan de hand van een risicoanalyse op het stelsel. Deze analyse levert een normenkader op dat MedMij gaat hanteren voor toetreders. Hierbij wordt zoveel mogelijk uitgegaan van gangbare normen binnen het zorglandschap.

Wilt u meer informatie over veiligheid en privacy?
Of ervaart u privacy- en/of veiligheidsproblemen in de toepassing van MedMij? 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