Grip op je eigen
gezondheidsgegevens

MedMij: veilige en betrouwbare uitwisseling van gezondheidsgegevens

In dit factsheet lees je meer over:

- MedMij
- hoe de uitwisseling van gezondheidsgegevens via MedMij werkt
- hoe veilig het gebruik van een persoonlijke gezondheidsomgeving is
- het MedMij Afsprakenstelsel en veiligheid
- hoe MedMij veilige gegevensuitwisseling bevordert
- concrete voorbeelden rondom MedMij en privacy en veiligheid
- eigen verantwoordelijkheid
- veelgestelde vragen

Wat is MedMij?

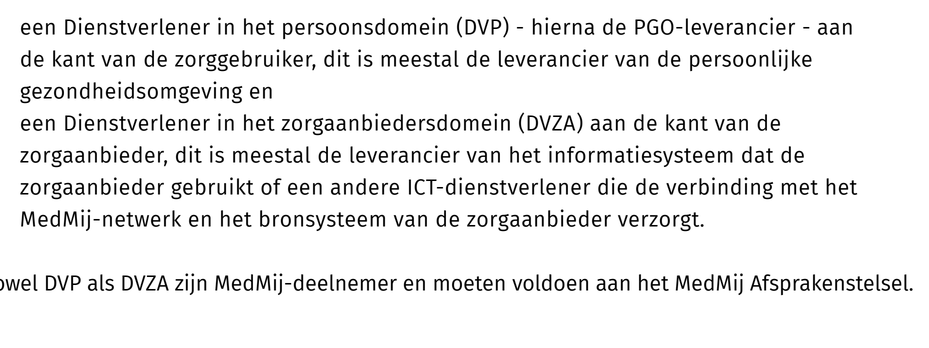
MedMij is dé Nederlandse standaard voor het veilig uitwisselen van gezondheidsgegevens tussen zorggebruiker en zorgverlener. Deze uitwisseling vindt plaats via het MedMij-netwerk tussen een persoonlijke gezondheidsomgeving (PGO) en een bronsysteem van een zorgaanbieder.

Met een PGO kan iedereen (vanaf 16 jaar) die dat wil gezondheidsgegevens op één plek verzamelen, beheren en delen. MedMij maakte de spelregels voor deze gegevensuitwisseling, het **MedMij Afsprakenstelsel**. Alle MedMij-deelnemers moeten zich aan deze spelregels houden. Zo kunnen zij met elkaar op een door MedMij goedgekeurde manier veilig en betrouwbaar gegevens uitwisselen. MedMij-deelnemers zijn te herkennen aan het **MedMij-label**. **Hier** kun je controleren of een PGO-leveranciers MedMij-deelnemer is.

Hoe werkt de uitwisseling van gezondheidsgegevens via MedMij?

Een van de uitgangspunten van MedMij is dat iedereen zijn/haar eigen PGO kan kiezen. Personen verzamelen, in een PGO naar keuze, veilig en betrouwbaar informatie die de zorgverlener ter beschikking stelt. Om via MedMij gegevens aan te bieden vragen zorgaanbieders aan de ICT-leverancier(s) van hun zorginformatiesysteem, of een andere dienstverlener als tussenpartij, deelnemer aan het MedMij-netwerk te worden. Hiervoor worden deze leveranciers MedMij-deelnemer.

Er zijn twee soorten dienstverleners die de informatie-uitwisseling tussen zorggebruikers en zorgverleners mogelijk maken:



- een Dienstverlener in het persoonsdomein (DVP) - hierna de PGO-leverancier - aan de kant van de zorggebruiker, dit is meestal de leverancier van de persoonlijke gezondheidsomgeving en
- een Dienstverlener in het zorgaanbiedersdomein (DVZA) aan de kant van de zorgaanbieder, dit is meestal de leverancier van het informatiesysteem dat de zorgaanbieder gebruikt of een andere ICT-dienstverlener die de verbinding met het MedMij-netwerk en het bronsysteem van de zorgaanbieder verzorgt.

Zowel DVP als DVZA zijn MedMij-deelnemer en moeten voldoen aan het MedMij Afsprakenstelsel.

Hoe veilig is het gebruik van PGO's?

In een PGO verzamelen gebruikers gezondheidsgegevens, waaronder gegevens vanuit het medisch dossier bij een of meerdere zorgverlener(s). Denk hierbij aan: medicijngebruik, vaccinatiegegevens, bloeddruk, bloedwaarden, mentale gezondheid, operaties of (chronische) aandoeningen. Allemaal privacygevoelige gegevens. MedMij-deelnemers die volgens de MedMij-afspraken gegevens uitwisselen voldoen dan ook aan strenge privacy- en informatiebeveiligingsregels.

Het MedMij Afsprakenstelsel en veiligheid

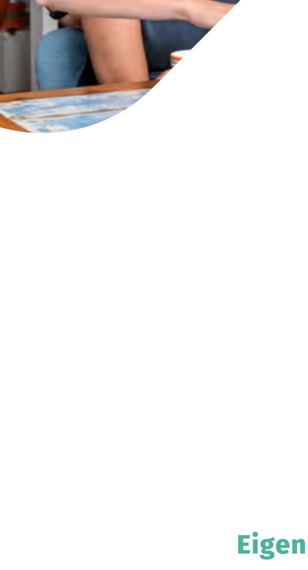
Als aanvulling op bestaande wet- en regelgeving zorgen we op twee manieren voor veilige gegevensuitwisseling aan de hand van het MedMij Afsprakenstelsel:

- We stellen strenge eisen aan de privacy en informatiebeveiliging van MedMij-deelnemers (zie factsheet Normenkader Informatiebeveiliging).
- We toetsen of deelnemers de (privacy- en informatiebeveiligings)afspraken nakomen wanneer zij MedMij-deelnemer worden en dit blijven we doen tijdens hun deelname (zie onder meer Toetredingsbeleid en Nalevingsbeleid).

Hoe zorgt MedMij voor veilige gegevensuitwisseling?

Hieronder vind je een aantal voorbeelden hoe MedMij zorgt voor veilige gegevensuitwisseling:

1. Het MedMij Afsprakenstelsel bevat verantwoordelijkheden en verplichte afspraken over veiligheid.
2. We toetsen deelnemers tijdens kwalificatie en acceptatie hoe zij deze afspraken implementeren.
3. Een onafhankelijke certificatie-organisatie moet een auditverklaring afgeven op de beheersings-maatregelen die elke deelnemer moet nemen (zie factsheet Normenkader Informatiebeveiliging).
4. MedMij-deelnemer worden kan alleen onder strenge voorwaarden. Zo vereisen we onder meer een KvK-inschrijving in Europa en een ondertekende intentieverklaring.
5. MedMij heeft een incidentenbeleid waarin we samenwerking faciliteren om tot een oplossing van een incident te komen, en hier gezamenlijk van te leren.
6. Het MedMij Afsprakenstelsel kent een Juridisch Kader en een Nalevingsbeleid met verplichtingen voor MedMij-deelnemers. Elke gebruiker van een PGO met MedMij-label kan erop vertrouwen dat wij deelnemers hieraan houden.



Wat betekent dit concreet – een aantal voorbeelden

- Gegevens worden te allen tijde versleuteld en gestructureerd uitgewisseld, uitsluitend door partijen die onderdeel zijn van het MedMij-netwerk. Hiervoor gebruiken we PKIo-certificaten: een gewaarmerkt, digitaal paspoort, waarmee systemen kunnen vaststellen met wie ze communiceren.
- MedMij-deelnemers moeten het hoogst beschikbare betrouwbaarheidsniveau (momenteel DigiD) gebruiken om toegang te krijgen tot de medische data bij de zorgverlener. Daarom moeten zorginstellingen die gegevens uitwisselen via MedMij een DigiD-aansluiting hebben. Zonder deze aansluiting is gegevensuitwisseling niet mogelijk. Vanuit MedMij adviseren we zorgaanbieders aan te sluiten op de Toegangsverleningservice (TVS), zie ook dit dit factsheet. Uitgebreide informatie voor zowel zorgaanbieders als ICT-leveranciers vind je op de website van DICTU.
- Voor gegevensuitwisseling van gezondheidsgegevens van partijen binnen het MedMij-netwerk wordt het BSN-nummer niet gecommuniceerd of opgeslagen. Lees meer over het gebruik van het BSN-nummer bij de veelgestelde vragen[*].
- We vereisen meerfactorauthenticatie voor toegang tot het dossier in een PGO.
- Om misbruik te voorkomen is de toestemming voor het ophalen van gegevens bij een zorgaanbieder door een PGO-gebruiker maximaal een kwartier (15 minuten).
- MedMij volgt de wet- en regelgeving rondom privacy en veiligheid van de Nederlandse overheid. Eventuele nieuwe maatregelen voeren wij altijd uit.
- De overeenkomst die MedMij met haar deelnemers sluit is streng en duidelijk. Zo mogen persoonsgegevens en gegevens in de PGO nooit worden doorverkocht.
- Alle partijen houden zich aan de Algemene verordening gegevensbescherming (AVG) en de Wet op de geneeskundige behandelovereenkomst (WGBO).

Eigen verantwoordelijkheid blijft essentieel

Geen enkel stelsel kan 100% veiligheid garanderen. Het gebruik van de gegevens in de PGO is uiteindelijk de verantwoordelijkheid van de gebruiker. Elke PGO met MedMij-label is verplicht die gebruikers daarop te wijzen. Wanneer het vermoeden bestaat dat er oneigenlijk gebruik van gezondheidsgegevens wordt gemaakt, kunnen zowel zorgverleners als zorggebruikers hiervan melding maken bij de Toezichthouder: Autoriteit Persoonsgegevens. Ook kunnen zij een melding bij Stichting MedMij doen. Wij starten dan het Nalevingsproces waarbij altijd sprake zal zijn van hoor en wederhoor.

Vragen?

Heb je nog vragen over MedMij en veiligheid na het lezen van dit factsheet?
Neem dan contact op met het MedMij-loket via info@medmij.nl.

Veelgestelde vragen

Waarvoor geven PGO-gebruikers toestemming en kunnen zij die weer intrekken?
Allereerst geeft de PGO-gebruiker toestemming aan zijn/haar PGO-leverancier om persoonsgegevens te verwerken. Wanneer de gebruiker zorggegevens gaat verzamelen en delen, geeft hij/zij aanvullende toestemming aan de ICT-leverancier van de zorgverlener voor het verzamelen of delen van specifieke informatie. Deze toestemming is alleen geldig voor dat moment en die specifieke gegevensuitwisseling. Bij elke volgende gegevensuitwisseling moet opnieuw om toestemming worden gevraagd.

Pas wanneer de gebruiker zelf besluit gegevens te verzamelen krijgt een zorgaanbieder van deze gebruiker toestemming om gegevens te versturen naar zijn/haar PGO. Dit is noodzakelijk, omdat de PGO-leverancier een dienstverlener is die namens de persoon de gegevens bij de zorgverlener verzamelt of met hem/haar deelt.

Let op: Voor de toestemming van gegevens is van de zorgverlener geen enkele actie vereist. De toestemming gaat automatisch omdat beschikbaar stellen van gegevens al impliciet is verankerd in de WGBO. Zorgverleners hoeven dus niet nogmaals actief toestemming te geven wanneer patiënten gegevens verzamelen of delen.

Hoelang blijven gegevens zichtbaar in de PGO van de gebruiker?
De gegevens blijven zichtbaar zolang de gebruiker de PGO wil gebruiken; dit kan vanaf het moment van ingebruikname levenslang zijn. Uiteraard kan de gebruiker ook zelf zijn/haar gegevens wissen in de eigen PGO. Dit is geen selectief proces om te voorkomen dat slechts een gedeelte van de waarheid gedeeld kan worden met een zorgverlener. Bij beëindiging van de overeenkomst tussen gebruiker en de PGO worden de gegevens ook gewist. In de gebruikersovereenkomst van de PGO-leverancier staat hoelang de gegevens bewaard blijven.

Kunnen zorgaanbieders via MedMij informatie delen met andere zorgaanbieders?
Nee, zorgaanbieders kunnen onderling geen informatie uitwisselen via MedMij. Wanneer de ICT-leverancier van de zorgaanbieder deelnemer is van MedMij, kan de gebruiker zijn/haar gegevens in de toekomst zelf wel delen met andere zorgaanbieders als hij/zij dat wil.

Wie is verantwoordelijk voor de gedeelde data van de zorgverlener als de PGO-gebruiker deze in zijn/haar PGO heeft staan?
De zorgverlener stuurt op verzoek van de gebruiker een (gedeeltelijke) kopie van het medisch dossier digitaal vanuit het zorginformatiesysteem naar de PGO. Zodra de gebruiker de data in de PGO heeft ontvangen, is het onderdeel van zijn/haar persoonlijk dossier. Zorgverleners zijn niet verantwoordelijk voor dat persoonlijke dossier. De PGO-leverancier beheert deze in opdracht van de PGO-gebruiker.

Wat betekent het voor zorgverleners als een gebruiker van PGO wisselt?
De gebruiker kiest via welke PGO hij/zij gegevens uitwisselt. Dit heeft geen invloed op de zorgaanbieder. Wanneer een gebruiker overstapt naar een andere PGO met MedMij-label merkt de zorgaanbieder daar niets van.

Kunnen anderen/derden meekijken in iemands PGO?
De meeste PGO's maken het voor gebruikers mogelijk dat zij anderen inzage bieden. Voor het ophalen van je gegevens bij je zorgaanbieder is het, volgens de eisen van MedMij, op dit moment uitsluitend mogelijk dat de eigenaar van de PGO kan inloggen. Ook kunnen alleen met de eigen DigiD gegevens worden verzameld of gedeeld met zorgaanbieders. MedMij wil het in de toekomst mogelijk maken dat gebruikers deze functie van de PGO ook aan iemand anders kunnen uitbesteden (bijvoorbeeld mantelzorgers, via een geregistreerde machtiging).

Hebben PGO-gebruikers recht op alle gegevens uit het zorginformatiesysteem?
Nee. De zorgverlener is wettelijk gezien verplicht het medisch dossier ter inzage aan te bieden en sinds juli 2020 op verzoek ook digitaal te delen. Persoonlijke werkaantekeningen vallen hier niet onder. Daarnaast kunnen nog niet alle gegevens op de MedMij-manier met PGO's worden uitgewisseld maar er wordt continu gewerkt aan nieuwe gegevensdiensten waardoor steeds meer beschikbaar komt. Daarnaast is het verstrekken van het medisch dossier aan regels gebonden. Zo gelden er bijvoorbeeld specifieke regels voor inzage door minderjarigen (onder de 16 jaar) en kan een arts afhankelijk van een situatie tot een andere afweging komen, wat ertoe kan leiden dat de gegevens mogelijk niet beschikbaar zijn via de MedMij-manier van uitwisseling. Met de zogeheten beschikbaarheidstoets wordt vastgesteld dat aan de voornoemde voorwaarden is voldaan voordat informatie uitgewisseld wordt.

Wat als een patiënt vindt dat het medisch dossier bij de zorgverlener niet helemaal op orde is?
De PGO-gebruiker kan de gegevens ophalen zoals die in het zorginformatiesysteem staan. Als de PGO-gebruiker daarin fouten of onvolledigheden ontdekt, kan hij/zij contact opnemen met zijn/haar zorgverlener en daar een verzoek indienen om de gegevens aan te passen. Een gebruiker kan gegevens zelf nooit rechtstreeks in het medisch dossier bij de zorgverlener wijzigen.

Kan een PGO-gebruiker zelf gegevens toevoegen aan of verwijderen uit het medische dossier bij de zorgverlener?
Nee, de PGO-gebruiker kan alleen gegevens in zijn/haar PGO verzamelen uit het medische dossier. Alleen de zorgverlener kan het medisch dossier corrigeren. Een patiënt kan bijvoorbeeld niet zelf in het EPD inloggen.

Waar bewaart mijn PGO-leverancier mijn data?
Dit is afhankelijk van de inrichting door de PGO-leverancier.
Vanzelfsprekend moet die omgeving voldoen aan de eisen die MedMij stelt.

september 2021

---

[*] **MedMij en het BSN-nummer**
MedMij maakt onderscheid tussen het Persoonsdomein en het Zorgaanbiedersdomein. Voor MedMij valt de verwerking van persoonsgegevens in het Zorgaanbiedersdomein onder de verwerkingsverantwoordelijkheid van de zorgaanbieder. In dit domein is het verwerken van het BSN voor de identificatie van personen wettelijk verplicht. In het Persoonsdomein valt de verwerking van persoonsgegevens onder de verwerkingsverantwoordelijkheid van de Dienstverlener persoon (DVP). Het is wettelijk bepaald dat de DVP in de rol als MedMij-deelnemer, het BSN niet mag verwerken.