Veilig gebruik van PGO's met MedMij-label

Hoe veilig is het gebruik van een persoonlijke gezondheidsomgeving (PGO) met MedMij-label? Waarvoor zorgt MedMij en waarop moet ik letten als zorgaanbieder? In dit factsheet gaan we dieper in op een aantal belangrijke thema's, zoals datagebruik, privacy en toestemming.

Vraag 1.

Van wie zijn de gegevens in de PGO van mijn patiënt/cliënt?
De gegevens in de PGO zijn eigendom van de gebruiker *(patiënt/cliënt)* van de PGO.

Vraag 2.

Kunnen anderen/derden meekijken in iemands PGO?
De meeste PGO's maken het voor gebruikers mogelijk om anderen toegang te geven tot hun gegevens. Het ophalen van gegevens bij de zorgaanbieder volgens MedMij is alleen mogelijk door de PGO-eigenaar of iemand die daarvoor is gemachtigd *(een vertegenwoordiger)* op basis van een machtiging of een wettelijke basis. Via DigiD-machtigen en DigiD-volmacht *(vanaf december 2022 beschikbaar)* kan ook aan mantelzorgers, ouders en wettelijke vertegenwoordigers, vrijwillig of op wettelijke basis, toegang verleend worden tot de PGO van een ander.

Vraag 3.

Mag een PGO-leverancier data in PGO's aan derden verkopen?
Nee, dit is verboden. De PGO-leverancier mag de gegevens in de PGO niet inzien en moet zich daarnaast houden aan de Deelnemersovereenkomst, die zij tekenen wanneer zij MedMij-deelnemer worden. In paragraaf 5.7 van de Deelnemersovereenkomst staat hierover:
De Deelnemer verstrekt geen persoonsgegevens van de Persoon aan anderen dan degenen waaraan de Deelnemer uit hoofde van de Overeenkomst gegevens mag verstrekken c.q. op grond van een wettelijke verplichting moet verstrekken. Het is de Deelnemer uitdrukkelijk verboden om data betreffende de Persoon te verkopen.

Vraag 4.

Wanneer mag of moet een PGO-leverancier data verstrekken uit hoofde van de overeenkomst, zoals genoemd in vraag 3?
De PGO-leverancier mag alleen informatie uitwisselen wanneer daarvoor toestemming is verleend door de PGO-gebruiker. Van die toestemming moet aangetoond kunnen worden:
a. Dat en waarvoor de PGO-gebruiker toestemming verleend
b. Dat de toestemming vrijelijk, specifiek, geïnformeerd en ondubbelzinnig is gegeven, en
c. Wie de verwerkingsverantwoordelijke is, wat de specifieke doeleinden/ het specifieke doel van de verwerking is, wie de ontvangers van de persoonsgegevens zijn en het recht om de toestemming te allen tijde weer in te trekken.

Hiervoor moet de PGO-leverancier een Verklaring van Toestemming opstellen, die begrijpelijk, gemakkelijk en toegankelijk is qua vorm en duidelijke taal bevat. Bij het geven van de toestemming moet de PGO-gebruiker hiervoor een actieve handeling uitvoeren *(bijvoorbeeld het zetten van een vinkje)*.

Vraag 5.

Mag een PGO-leverancier data gebruiken voor andere doeleinden dan het beschikbaar stellen van deze data in de PGO? Voor welke doeleinden dan?
Voor het antwoord op deze vragen verwijzen we naar vraag 4.

Vraag 6.

Regelt en borgt het MedMij Afsprakenstelsel dat PGO-leveranciers niets mogen doen met de medische gegevens in PGO's en deze dus ook niet mogen inzien, delen, gebruiken voor andere eigen (commerciële) doelen *(zoals bv een platform)*, verstrekking aan derden, etc ?
Zie ook vraag 4. In het MedMij Afsprakenstelsel en dan met name in het normenkader staan de eisen die gesteld worden om geheimhouding te waarborgen. Het maakt ook deel uit van de **deelnemersovereenkomst**.

Artikel 5.7 De Deelnemer verstrekt geen persoonsgegevens van de Persoon aan anderen dan degenen waaraan de Deelnemer uit hoofde van de Overeenkomst gegevens mag verstrekken c.q. op grond van een wettelijke verplichting moet verstrekken. Het is de Deelnemer uitdrukkelijk verboden om data betreffende de Persoon te verkopen.

Vraag 7.

Mag een PGO-leverancier data verstrekken aan anderen, bv een dochter- of moeder-onderneming?
Nee, de informatie mag alleen gebruikt worden waarvoor toestemming is gegeven door de PGO-gebruiker. Bij de toestemming is duidelijk aangegeven wie de ontvanger van de informatie is. Die informatie mag niet naar andere ontvangers gestuurd worden.

Vraag 8.

Hoelang bewaart een PGO-leverancier gegevens van de PGO-gebruiker?
Hoe wordt omgegaan met updates in het zorginformatiesysteem?
De gegevens blijven in het dossier van de PGO zolang de gebruiker dat wil. Als er updates zijn in het HIS, dan kunnen die door de gebruiker worden toegevoegd aan de bestaande informatie in de PGO. Het is afhankelijk van het zorginformatiesysteem of de gebruiker hierover een notificatie ontvangt. Het is niet de bedoeling dat updates automatisch naar de PGO gestuurd worden, het zal altijd een actieve handeling van de gebruiker vragen om informatie toe te voegen. Alleen daarmee wordt de regiefunctie van de gebruiker gewaarborgd.

Vraag 9.

Hoe borgt het MedMij Afsprakenstelsel dat de PGO-leverancier gegevens van een gebruiker wist wanneer zij de overeenkomst met deze leverancier beëindigen?
De PGO-leverancier moet zich naast de MedMij Deelnemersovereenkomst ook houden aan de **AVG** in de rol van verwerker en verwerkingsverantwoordelijke. Daarbij hoort ook het "recht op vergeten". Dus het verwijderen van informatie op verzoek van de gebruiker. Een bijzonder geval is het verwijderen van informatie na het overlijden van een gebruiker. De regels zijn niet gelijk aan de richtlijnen die gelden voor een arts met het medische dossier. Het PGO-dossier is onderwerp van de overeenkomst tussen PGO-gebruiker en PGO-leverancier. Hierin moet bepaald zijn hoe met deze informatie wordt omgegaan na overlijden. Ook toegang door familieleden of mantelzorgers moet vooraf geregeld zijn via machtigingen.

Vraag 10.

Worden patiënt -medische gegevens 'opgeslagen' door de PGO-leveranciers?
In de PGO verzamelt de gebruiker een kopie van gegevens uit het medisch dossier van zijn zorgverlener(s). Het is de gebruiker die bepaalt welke informatie hij wel of niet opslaat en dus ook of informatie verwijderd moet worden. De gebruiker heeft zelf een overeenkomst met de PGO-leverancier. Deze leverancier is in termen van **AVG** de verwerkersverantwoordelijke. Om MedMij-deelnemer te kunnen worden moet de PGO-leverancier ook voldoen aan **NEN 7510**. *[Zie ook vraag 12]*

Vraag 11.

Hoe zorgt MedMij ervoor dat dat de persoonlijke (medische) gegevens van mijn patiënten/cliënten niet in verkeerde handen terechtkomen?
Naast het uitdrukkelijke verbod op het verkopen van data in PGO's aan derden in de Deelnemersovereenkomst *(zie vraag 3)* moeten MedMij-deelnemers ook een **NEN 7510**-accreditatie hebben voor zij MedMij-deelnemer mogen worden. *[Zie ook vraag 12]*

Vraag 12.

Wat is NEN 7510?
NEN 7510 is de Nederlandse norm voor informatiebeveiliging in de zorg, gebaseerd op de internationale kwaliteitsnorm ISO 27001. NEN 7510 werd ontwikkeld voor de zorgsector en bevat een aantal specifieke beheersmaatregelen, gericht op de bescherming van persoonlijke zorggegevens zoals patiëntdata en behandelgegevens.
Het NEN 7510-certificaat is drie jaar geldig, daarna volgt opnieuw certificering. Verder wordt er, door een onafhankelijke organisatie, jaarlijks een controle uitgevoerd om te toetsen of het informatiesysteem nog voldoet aan alle certificeringseisen.

Vraag 13.

Waar kan ik mij melden wanneer ik misbruik vermoed *(bv data aan derden verkopen en het niet op de juiste manier naleven van de NEN 7510)* ?
De PGO-gebruiker heeft een overeenkomst met zijn PGO-leverancier. Als de eindgebruiker een klacht heeft over zijn PGO-leverancier dan moet hij die klacht indienen bij die leverancier. Als zorgaanbieder speel je hierin geen rol. Je kunt wel een melding doen bij het MedMij-loket via **info@medmij.nl**.
Het NEN 7510-certificaat gaat verder dan de MedMij-uitwisseling. MedMij kan alleen handhaven in relatie tot de MedMij-eisen en -uitwisselingen en niet over de complete productrange van de PGO-leverancier. Controle en handhaving geschieden altijd reactief op basis van signalen.

Vraag 14.

Wordt het privacyreglement van PGO-leveranciers gecontroleerd door MedMij? Bijvoorbeeld om te kijken of de bepalingen conform het MedMij-stelsel zijn? En wat te doen bij 'rare of vage' teksten?
MedMij reviewt/verifieert de overeenkomsten en privacystatements van PGO-leveranciers niet. Dit blijft te allen tijde de verantwoordelijkheid van de deelnemers, omdat zij naast MedMij-functionaliteit ook andere functionaliteit aanbieden.
Controle en handhaving geschieden altijd reactief op basis van signalen. De voorwaarden zijn omschreven in de deelnemersovereenkomst. Alles wat mogelijk schadelijk kan zijn voor het imago van MedMij, is niet toegelaten in de context van de MedMij-PGO.

Vraag 15.

Wie ziet toe op een juiste inhoud van de gebruikersovereenkomst van de PGO-leverancier?
De gebruikersovereenkomst maakt geen onderdeel uit van de toetsing bij aansluiting en/of de periodieke toetsing.

Vraag 16.

Mag een PGO-leverancier in de eigen toestemmingsverklaring een brede toestemming opnemen (direct informed consent) waarmee de PGO-gebruiker aan de PGO-leverancier toestemming geeft voor het gebruiken van iemands persoonlijke gezondheidsgegevens?
Dat is niet toegestaan. Voor het uitwisselen van gezondheidsgegevens is een uitdrukkelijke en specifieke toestemming noodzakelijk. Deze kan dus geen deel uitmaken van een brede toestemming.
De PGO-leverancier moet kunnen aantonen dat voor de uitwisseling die specifieke toestemming is gegeven. De eisen aan die toestemming staan in het **afsprakenstelsel**:
(Als een PGO-gebruiker alleen met JA of NEE kan antwoorden is dit juridisch onjuist, omdat de PGO-gebruiker dan gedwongen wordt om toch JA te antwoorden om de PGO te kunnen gebruiken. Daarnaast zijn er allerlei voorwaarden aan het geven van toestemming voor het delen en verwerken van (bijzondere) persoonsgegevens. De gebruiker moet hierover duidelijk en expliciet geïnformeerd worden en moet de toestemming zonder dwang kunnen geven en de toestemming ook op elk moment weer kunnen intrekken.)

Vraag 17.

Er is een verschil tussen generieke persoonsgegevens en bijzondere persoonsgegevens. Maakt de gegeven toestemming bij het aanmaken van het account hier onderscheid in?
Alle informatie waaruit direct of indirect informatie over de gezondheid van een persoon uit kan worden afgeleid heeft in het MedMij **Informatieclassificatiebeleid** het vertrouwelijkheidsniveau 'zeer hoog'. Voor de classificaties sluit het MedMij Afsprakenstelsel aan bij NEN 7512:2015. Andere informatie heeft een lagere vertrouwelijkheid. De gegeven toestemming is onderdeel van de overeenkomst tussen PGO-leverancier en PGO-gebruiker. De leverancier moet zich voor wat betreft de gezondheidsinformatie te allen tijde houden aan het vertrouwelijkheidsniveau zeer hoog.

Vraag 18.

Hoe controleert MedMij of PGO-leveranciers zich aan de afspraken houden?
MedMij handhaaft op basis van signalen. In eerste instantie gebeurt de naleving zo veel mogelijk in goed onderling overleg tussen partijen in het afsprakenstelsel. In tweede instantie kan het noodzakelijk voor een goede naleving te zorgen door tussenkomst van MedMij. Op basis daarvan wordt de procedure opgestart. Stichting MedMij is verantwoordelijk voor de uitvoering van het Nalevingsbeleid.
Het MedMij Nalevingsbeleid vind je **hier** in het MedMij Afsprakenstelsel:

Vraag 19.

Welke informatie verzamelt MedMij zelf?
Om het gebruik van MedMij inzichtelijk te maken worden maandelijks managementrapportages opgesteld. De informatie in deze rapportages is op geen enkele wijze te herleiden tot personen en voldoet aan alle eisen die het afsprakenstelsel stelt aan privacy en beveiliging. Exacte details welke informatie MedMij verzamelt in de managementrapportage staan in het hoofdstuk **Managementinformatie** van het MedMij Afsprakenstelsel.

Vraag 20.

Als zorgverlener ben ik gehouden aan mijn beroepsgeheim. Is er ook zoiets als een 'patiëntgeheim' en wat is daarover geregeld?
Patiëntenfederatie Nederland biedt richtlijnen aan voor het **Patiëntgeheim**.
MedMij maakt hier geen afspraken over.

NB. Waar staat PGO-leverancier bedoelen we de MedMij-deelnemer in de rol van dienstverlener persoon (DVP).
Waar staat PGO-gebruiker bedoelen we een patiënt/cliënt (burger > 16 jaar) met een persoonlijke gezondheidsomgeving.

november 2022

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**.