PELS RIJCKEN

Landsadvocaat

Rapport

voor	Ministerie van Volksgezondheid, Welzijn en Sport
van	(kantoor landsadvocaat)
datum	10 juni 2020
inzake	Rapport inzake patiëntgeheim
zaaknr	11012595

1 Inleiding

1.1 De Minister voor Medische Zorg en Sport (**de minister**) heeft op 1 oktober 2019 een schriftelijke reactie gegeven op het position paper van de Patiëntenfederatie Nederland (**Patiëntenfederatie**) over het zgn. patiëntgeheim. De Patiëntenfederatie wijst in haar position paper op de ontwikkelingen die zich voordoen bij de verwerking van gegevens betreffende de gezondheid van personen (**gezondheidsgegevens**), meer in het bijzonder het toenemend gebruik van (gezondheids)apps, wearables en persoonlijke gezondheidsomgevingen (**PGO's**). Als gevolg daarvan worden steeds meer gezondheidsgegevens verwerkt door de aanbieders (leveranciers, beheerders) van deze gezondheidsapps, wearables en PGO's.

1.2 De Patiëntenfederatie meent dat deze ontwikkeling nieuwe risico's met zich mee brengt, onder meer doordat de gezondheidsgegevens hierdoor niet worden beschermd door het medisch beroepsgeheim van de zorgverlener. De Patiëntenfederatie stelt zich op het standpunt dat de risico's dusdanig zijn dat het (in aanvulling op de bestaande relevante wettelijk kader) wenselijk is om een nieuw 'patiëntgeheim' te introduceren. Dit patiëntgeheim is enerzijds erop gericht meer juridische bescherming te bieden aan de gezondheidsgegevens die worden verwerkt buiten de behandelrelatie. Anderzijds is het patiëntgeheim gericht op het verhogen van de bewustwording van patiënten van de privacyrisico's die gepaard gaan met gezondheidsapps, wearables en PGO's én het verbeteren van de handhaving van eventuele overtredingen van de relevante privacywetging door aanbieders van deze gezondheidsapps, wearables en PGO's.

1.3 De minister heeft zich in zijn brief van 1 oktober 2019 op het standpunt gesteld dat met de huidige wetgeving, aangevuld met het MedMij afsprakenstelsel voor PGO's, reeds een voldoende mate van bescherming van gezondheidsgegevens wordt geboden. In de bijlage bij deze brief heeft de minister zijn standpunt onderbouwd.[1]

[1] Zie Bijlage bij Kamerbrief van 1 oktober 2019 kenmerk 1540335-191826-PZO.

1.4 De minister heeft ons gevraagd te analyseren in hoeverre de huidige relevante wet- en regelgeving, aangevuld met het MedMij afsprakenstelsel voor PGO's, inderdaad een voldoende mate van bescherming biedt tegen risico's die zich voordoen bij de verwerking van gezondheidsgegevens die buiten de behandelrelatie worden verzameld en opgeslagen, zoals in gezondheidsapps, wearables en PGO's en voor zover de bescherming onvoldoende is, wat de voor- en nadelen zijn van het (wettelijk) regelen van extra bescherming ten aanzien van deze risico's. De minister wil deze analyse gebruiken om vast te stellen of voldoende reden bestaat tot de introductie van een patiëntgeheim. Dit rapport voorziet in deze analyse.

1.5 Dit rapport is als volgt opgebouwd:

- In hoofdstuk 2 zetten wij uiteen op welke wijze de huidige relevante wet- en regelgeving (privacy)bescherming biedt bij de verwerking van gezondheidsgegevens die worden verzameld en opgeslagen buiten de behandelrelatie.

- In hoofdstuk 3 bespreken wij de in de relevante literatuur geïdentificeerde risico's die zich voor kunnen doen met betrekking tot het buiten de behandelrelatie verzamelen en opslaan van gezondheidsgegevens.

- In hoofdstuk 4 analyseren wij in hoeverre de relevante wet- en regelgeving de in hoofdstuk 3 genoemde risico's verminderen of wegnemen.

- In hoofdstuk 5 bespreken we, in geval van eventuele restrisico's[2] voor de privacybescherming van gebruikers, welke voor- en nadelen bestaan bij het door de Patiëntenfederatie voorgestelde introduceren van een nieuw wettelijke patiëntgeheim.

1.6 Een en ander resulteert in een conclusie waarbij de voor- en nadelen van het invoeren van het patiëntgeheim worden afgewogen tegen het vasthouden aan de huidige wet- en regelgeving.

2 Op welke wijze biedt de huidige relevante wet- en regelgeving (privacy)bescherming bij de verwerking van gezondheidsgegevens die worden verzameld en opgeslagen buiten de behandelrelatie?

2.1 De verwerking van gezondheidsgegevens wordt — afhankelijk van de aard van de verwerking — beheerst door de algemene regels van de Algemene Verordening Gegevens (**AVG**) en de Uitvoeringswet AVG (**UAVG**) (tezamen: **(U)AVG**), eventuele bijzondere sectorale wetgeving met betrekking tot de verwerking van

[2] Met 'restrisico' wordt bedoeld: het privacyrechtelijke risico dat patiënten lopen zonder de nadere door de Patiëntenfederatie voorgestelde wetgeving.

gezondheidsgegevens, het medisch beroepsgeheim en tot slot de nadere regels die zijn opgenomen in afsprakenstelsels, zoals MedMij.

2.2 Hieronder geven wij een beschrijving van de wijze waarop gezondheidsgegevens in de huidige wet- en regelgeving worden beschermd. Wij maken daarbij een onderscheid tussen de verwerking van gezondheidsgegevens (1) in het kader van een behandelrelatie, (2) buiten de behandelrelatie, door middel van een PGO en (3) buiten de behandelrelatie door middel van andere (gezondheids)apps en wearables.

(1) Privacybescherming bij de verwerking van gezondheidsgegevens in het kader van een behandelrelatie

2.3 De verwerking van gezondheidsgegevens van een patiënt in het kader van een behandelrelatie door een zorgverlener is gebonden aan een strikt wettelijk stelsel. De privacybescherming in het kader van een behandelrelatie is als volgt vormgegeven.

(a) Het medisch beroepsgeheim

2.4 Zorgverleners[3] en zorgaanbieders zijn allereerst gebonden aan het medisch beroepsgeheim van artikel 7:457 van het Burgerlijk Wetboek (**BW**) en artikel 88 de Wet op de beroepen in de individuele gezondheidszorg (**Wet BIG**).[4] Het medisch beroepsgeheim houdt kortgezegd in dat zorgverleners vertrouwelijke informatie over een patiënt in beginsel alleen met uitdrukkelijke toestemming van die patiënt aan een ander kenbaar mogen maken. Het beroepsgeheim van de zorgverlener is niet beperkt tot medische informatie, maar ziet op alle informatie die de patiënt aan de zorgverlener heeft toevertrouwd. Het beroepsgeheim strekt zich eveneens uit tot de medewerkers van de zorgverlener (zoals assistenten en secretaresses).[5] Voor hen geldt een zgn. afgeleid beroepsgeheim.

2.5 In de rechtspraak is bevestigd dat een wettelijk geregeld beroepsgeheim, zoals dat van advocaten en het medisch beroepsgeheim, een maatschappelijk belang dient, namelijk:

> "het maatschappelijk belang dat een ieder zich vrijelijk en zonder vrees voor openbaarmaking van het toevertrouwde om bijstand en rapport tot de verschoningsgerechtigde c.q. zwijgplichtige moet kunnen wenden."[6]

2.6 Daarnaast dient het medisch beroepsgeheim ook een, in de literatuur geïdentificeerd, individueel belang. Dat betreft het privacybelang dat bepaalde gevoelige informatie

---

[3] Een zorgverlener kan zowel een natuurlijke persoon als een rechtspersoon zijn die een geneeskundig beroep of bedrijf uitoefent. Voorbeelden van natuurlijke personen die een geneeskundig beroep uitoefenen zijn een arts, tandarts, verloskundige, psychotherapeut en paramedicus. Voorbeelden van een rechtspersoon die een geneeskundig bedrijf uitoefent zijn ziekenhuizen, verpleeghuizen of andere zorginstellingen.

[4] Het medische beroepsgeheim in artikel 7:457 BW is ruimer dan het beroepsgeheim uit de Wet BIG, aangezien ook niet-geregistreerde zorgverleners onder de reikwijdte van deze bepaling vallen.

[5] Zie onder meer HR 30 juni 2017, ECLI:NL:HR:2017:1205.

[6] Zie bijv. HR 19 november 1985, ECLI:NL:HR:1985:AC9105, *NJ* 1986, 533 m.nt. 't Hart.

niet bij anderen terecht komt en daarnaast het gezondheidsbelang dat intieme informatie moet kunnen worden verstrekt om zo goed mogelijk te worden behandeld.[7]

2.7 Het medisch beroepsgeheim kent een aantal strikt omschreven uitzonderingsgronden.[8] De belangrijkste is de mondelinge of schriftelijk gegeven toestemming van de patiënt. Voor zover het medisch beroepsgeheim wordt doorbroken met toestemming, is vereist dat de patiënt voorafgaand aan het verlenen van toestemming is ingelicht over het doel, de inhoud en de mogelijke consequenties van de gegevensverstrekking. In bepaalde gevallen kan worden uitgegaan van veronderstelde toestemming van de patiënt, bijvoorbeeld (i) als de patiënt op de hoogte is van de gegevensverstrekking en daartegen geen bezwaren heeft geuit of (ii) als de patiënt niet in staat is om zijn toestemming te geven voor de gegevensverstrekking.

2.8 Het medisch beroepsgeheim dient, als gezegd, ook een maatschappelijk belang. Dit brengt met zich dat de zorgverlener een eigen afweging moet maken of hij zijn/haar medisch beroepsgeheim doorbreekt. Deze afweging kan als resultaat hebben dat de zorgverlener, ondanks toestemming van de patiënt, ervoor kiest om toch géén informatie te verstrekken.

2.9 De zorgverlener komt met betrekking tot de onder hem berustende informatie een verschoningsrecht toe tegenover de rechter, de rechter-commissaris, de officier van justitie en de politie. Dit verschoningsrecht houdt in dat de zorgverlener mag weigeren om een getuigenis af te leggen of vertrouwelijke informatie over de patiënt te verstrekken. Het verschoningsrecht geldt in het strafrecht,[9] het civiele recht,[10] bestuursrecht[11] en tuchtrechtelijke procedures.[12] Aan de medewerkers van de zorgverlener (zoals assistenten, secretaresses, medewerkers van de IT-afdeling)[13] komt een afgeleid verschoningsrecht toe. Dit afgeleide verschoningsrecht volgt met name uit de hulppositie waarin zij verkeren ten opzichte de verschoningsgerechtigde zorgverlener verkeren. Als er een verzoek wordt gedaan om verstrekking van patiëntinformatie staat het degene(n) met een afgeleid verschoningsrecht niet vrij om daarover zelfstandig te beslissen. De zorgverlener blijft als oorspronkelijke verschoningsgerechtigde de zeggenschap behouden of en zo ja, in hoeverre een beroep wordt gedaan op het verschoningsrecht.

---

7 T. Hooghiemstra, *Informationele zelfbeschikking in de zorg*, Tilburg University 2018, p. 152; S. Nouwt, *Zorg voor privacy. Informatietechnologie en informationele privacy in de gezondheidszorg*, Den Haag: NV Sdu 1997, p. 95.

8 De zorgverlener kan een uitzondering maken op zijn beroepsgeheim indien (i) hij bij of krachtens de wet tot verstrekking van informatie aan derden is verplicht (art. 7:457 lid 1, laatste volzin), (ii) gegevens worden verstrekt aan (rechts)personen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst (art. 7:457 lid 2 BW), (iii) het verstrekken van informatie aan de vertegenwoordigers van een patiënt die niet goed zelf zijn eigen belangen kan waarnemen (art. 7:457 lid 3 BW); (iv) de zorgverlener twijfelt of hij de gegevens aan de patiënt mag onthouden en in dat kader eerst een andere hulpverlener wil consulteren en op grond daarvan gerechtigd is de zorgverlener te informeren (laatste zin van lid 3 van art. 7:448), (v) de aanwezigheid van een noodtoestand, in de zin van een conflict van plichten of (vi) de doorbreking van het beroepsgeheim gerechtvaardigd is in geval van zwaarwegende belangen (of in het strafrecht 'zeer uitzonderlijke omstandigheden').

9 Artikel 218 Sv.

10 Artikel 191, tweede lid, sub b, Wetboek van Burgerlijke rechtsvordering (Rv).

11 Artikel 8:33, derde lid, Algemene wet bestuursrecht (Awb).

12 Artikel 68, vijfde lid, Wet BIG.

13 Ook de raad van bestuur van een zorginstelling komt een afgeleid verschoningsrecht toe.

2.10 Het verschoningsrecht rust bovendien op de vertrouwelijke communicatie tussen de zorgverlener en zijn patiënt, zelfs indien deze informatie zich onder een derde (bijvoorbeeld een cloudopslagprovider) of de patiënt bevindt.[14] In de strafrechtelijke context[15] leidt dit ertoe dat brieven of andere geschriften, maar ook USB-sticks en e-mails, zijn uitgesloten van inbeslagneming voor zover deze informatie bevatten waarop het verschoningsrecht rust.[16] Ook voor doorzoekingen[17], met inbegrip van doorzoekingen van geautomatiseerde werken of gegevens, gelden beperkingen.[18] De rechter-commissaris oordeelt hierover.[19] [20]

2.11 Van belang is dat het verschoningsrecht slechts een rol speelt bij de verstrekking van medische informatie of vertrouwelijke communicatie aan de rechter, de officier van justitie of de politie (of de inbeslagneming of doorzoeking daarvan door een officier van justitie of politie). Het verschoningsrecht vormt geen beletsel voor het delen van (medische) informatie met derden. In een dergelijk geval is slechts het medisch beroepsgeheim van toepassing. De patiënt kan – voor zover hij over zijn eigen medische informatie beschikt - naar eigen inzicht besluiten om medische informatie met derden (eventueel door middel van een wearable of een PGO) te delen.

(b) Doorbrekingsgrond voor de verwerking van gezondheidsgegevens (AVG)

2.12 Persoonsgegevens over gezondheid of gezondheidsgegevens zijn 'bijzondere persoonsgegevens' in de zin van artikel 9, eerste lid, AVG. Voor deze gegevens geldt een verwerkingsverbod, dat door middel van een doorbrekingsgrond kan worden doorbroken.[21] Zo een doorbrekingsgrond betreft de uitdrukkelijke toestemming van de patiënt (art. 9, tweede lid, aanhef en onderdeel a, AVG). De toestemming moet, zo

---

[14] Doordat het verschoningsrecht van de zorgverlener op de vertrouwelijke communicatie blijft rusten, bepaalt de zorgverlener (en dus niet de patiënt) of de informatie onder zijn verschoningsrecht valt en/of deze informatie aan de officier van justitie of de rechter mag worden verstrekt. Achtergrond daarvan is dat het verschoningsrecht strekt ter bescherming van het algemene maatschappelijke belang dat men zich vrijelijk en zonder vrees voor openbaarmaking van het aan hem toevertrouwde tot hem als vertrouwenspersoon kan wenden en niet in het individuele belang van de patiënt. Hoewel in zoverre gesproken zou kunnen worden van een afgeleid verschoningsrecht, benadrukken wij dat de positie van de patiënt verschilt van de positie van een willekeurige derde met een afgeleid verschoningsgerechtigde. Doordat het verschoningsrecht ziet op informatie van de patiënt, heeft de patiënt een persoonlijk belang bij het oordeel van de zorgverlener. De patiënt kan – bijvoorbeeld door middel van het verlenen van toestemming – het oordeel van de zorgverlener (pogen te) beïnvloeden. Hoewel een dergelijke toestemming van de patiënt het verschoningsrecht niet zonder meer opheft, zal de zorgverlener die toestemming wel dienen te betrekken bij zijn afweging of hij de gevraagde gegevens zal verstrekken (zie HR 26 mei 2009, ECLI:NL: HR:2009:BG5979).

[15] Het (strafrechtelijke) verschoningsrecht is opgenomen in artikel 218 van het Wetboek van Strafvordering (**Sv**).

[16] Zie artikel 98, eerste lid, Sv.

[17] Artikel 98, vijfde lid, Sv.

[18] Artikel 125i Sv bepaalt dat artikel 98 Sv van overeenkomstige toepassing is in geval van de doorzoeking van een plaats ter vastlegging van gegevens die op een gegevensdrager zijn vastgelegd of opgeslagen.

[19] Tegen het oordeel van de rechter-commissaris staat beklag open. Zolang niet onherroepelijk op dit beklag is beslist, mag niet tot kennisneming van de brieven of geschriften worden overgegaan. Zie artikel 98, derde lid, Sv. Tegen de beslissing van de beklagrechter kan de verschoningsgerechtigde zorgverlener in cassatie gaan (artikel 552a Sv jo. artikel 552d Sv).

[20] Uit de consultatieversie van het nieuwe Boek 2 Sv blijkt dat de wetgever voornemens is om artikel 98 Sv te verduidelijken, door te expliciteren dat het verschoningsrecht ook betrekking heeft op gegevens van de verschoningsgerechtigde; zie Consultatie Wetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering, artikel 2.7.6.2.2.2. p. 52

[21] De algemene doorbrekingsgronden staan beschreven in artikel 9 AVG en de artikelen 22 tot en met 33 van de Uitvoeringswet AVG ('UAVG'). In aanvulling hierop bevatten sectorale wetten veelal bijzondere doorbrekingsgronden voor specifieke gevallen.

blijkt uit artikel 7 AVG en overwegingen 32, 42 en 43 uit de preambule van de AVG, vrijelijk, specifiek en geïnformeerd zijn gegeven. De toestemming dient bovendien op een ondubbelzinnige wijze (aantoonbaar) te zijn gegeven door middel van een actieve handeling én moet gemakkelijk weer in te trekken zijn.[22]

(c) Wettelijke grondslag voor de verwerking van gezondheidsgegevens (AVG)

2.13 In aanvulling op het vereiste dat er een doorbrekingsgrond is, geldt dat de verwerking moet kunnen worden gebaseerd op een wettelijke grondslag als bedoeld in artikel 6, eerste lid, AVG.[23] De verwerking van persoonsgegevens door een zorgverlener in het kader van de behandelrelatie zal vaak zijn gebaseerd op toestemming van de betrokkene (art. 6, eerste lid, aanhef en onderdeel a, AVG) of de noodzaak om uitvoering te geven aan de behandelovereenkomst (art. 6, eerste lid, aanhef en onderdeel b, AVG jo. art. 7:446 BW). Ook is het mogelijk dat de verwerking wordt gebaseerd op het gerechtvaardigde belang van een derde (art. 6, eerste lid, aanhef en onderdeel f, AVG).

(d) Overige vereisten van de (U)AVG

2.14 In aanvulling op de hiervoor besproken vereisten stelt de AVG nog een aantal overige relevante vereisten. Dit betreffen vereisten voortvloeiend uit onder andere:

- het doelbindingsbeginsel (art. 5, eerste lid, aanhef en onderdeel b, AVG jo. art. 6, vierde lid, AVG);
- het beginsel van minimale gegevensverwerking (art. 5, eerste lid, aanhef en onderdeel c, AVG);
- het beveiligingsbeginsel (artikel 5, eerste lid, aanhef en onderdeel f, AVG);
- de beginselen van gegevensbescherming door ontwerp en door standaardinstellingen (zgn. privacy by design & default) (art. 25 AVG);
- het verbod op geautomatiseerde besluitvorming, waaronder profilering (art. 22 AVG).[24]

(e) Voorwaarden die voortvloeien uit andere bijzondere wetten of afsprakenstelsels

2.15 Op grond van artikel 9, vierde lid, AVG heeft de wetgever de bevoegdheid om te voorzien in bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van gezondheidsgegevens. Een voorbeeld daarvan is te vinden in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (**Wabvpz**). Daarin wordt de beschikbaarstelling van medische dossiers door artsen onderling via een

[22] Andere mogelijke doorbrekingsgronden die in een behandelrelatie uitkomst zouden kunnen bieden zijn onder meer artikel 9, tweede lid, aanhef en onder c, AVG dat bepaald dat de verwerking plaats mag vinden indien dat noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven; artikel 9, tweede lid, aanhef en onder h, AVG jo. artikel 30, tweede lid, aanhef en onder a, UAVG dat bepaalt dat hulpverleners en instellingen of voorzieningen voor gezondheidszorg gezondheidsgegevens mogen verwerken en tot slot: artikel 9, tweede lid, aanhef en onder j, AVG jo. artikel 24 UAVG dat bepaalt dat gezondheidsgegevens onder voorwaarden mogen worden verwerkt voor onder meer wetenschappelijk onderzoek.

[23] De wettelijke grondslagen 'wettelijke verplichting' (artikel 6, eerste lid, aanhef en onder c, AVG) en 'noodzakelijk voor de uitvoering van een publieke taak' (artikel 6, eerste lid, aanhef en onder e, AVG) dienen overeenkomstig artikel 6, derde lid, AVG te worden vastgesteld bij een unierechtelijke of nationale grondslag dat op de verwerkingsverantwoordelijke van toepassing is.

[24] Voor zover noodzakelijk zullen deze vereisten nader worden uitgewerkt in hoofdstuk 4 van dit rapport.

elektronisch uitwisselingssysteem beperkt tot die gevallen waarin de patiënt daarvoor uitdrukkelijke toestemming heeft gegeven.[25]

(2) Privacybescherming bij de verwerking van gezondheidsgegevens door middel van een PGO, buiten een behandelrelatie

2.16 Het is ook mogelijk dat de verwerking van gezondheidsgegevens buiten een behandelrelatie worden verwerkt, bijvoorbeeld door middel van een PGO, een website of gezondheidsapp waarmee de betrokkene toegang heeft tot de eigen gezondheidsgegevens.[26] Een PGO stelt de betrokkene in staat om regie te houden over zijn of haar eigen gezondheidsgegevens, waar het gaat om het verzamelen, beheren en het delen ervan met derden.[27] De natuurlijke persoon op wie de gegevens betrekking hebben, de betrokkene, kan in zijn of haar PGO gegevens van verschillende zorgverleners combineren. De aanbieder van de PGO zal in de meeste gevallen toegang hebben tot de gegevens van de betrokkene en deze gegevens ten behoeve van die betrokkene verwerken.

2.17 Indien gezondheidsgegevens worden verwerkt door middel van een PGO valt een deel van de in het voorgaande beschreven (randnr. 2.3) privacybescherming weg. Zo is de aanbieder van een PGO niet gebonden aan het medisch beroepsgeheim. Het vereiste van een doorbrekingsgrond, het vereiste van een wettelijke grondslag en de overige vereisten van de AVG gelden evenwel onverkort voor de aanbieder van een PGO.[28]

Voor de PGO's is het MedMij-label ontwikkeld. MedMij is een afsprakenstelsel waarin technische standaarden en juridische richtlijnen zijn opgenomen die een nadere invulling geven aan de wijze waarop de privacy van gebruikers van een PGO worden beschermd. Indien een PGO voldoet aan de gestelde eisen kan de PGO in aanmerking komen voor het MedMij-label.[29] De voorwaarden van het MedMij-label vormen een relevante factor bij de beoordeling van risico's van het gebruik van een PGO. Voor zover noodzakelijk zullen wij bij de bespreking van de risico's in hoofdstuk 4 nader ingaan op de relevante voorwaarden van het MedMij-label. Daarbij merken wij op dat deelname aan MedMij geschiedt op vrijwillige basis, wat impliceert dat deze voorwaarden dus niet van toepassing op *alle* PGO's.[30]

---

25 Zie artikel 15a, eerste lid, Wabvpz.

26 Op Medmij.nl wordt de volgende definitie gehanteerd: "Een persoonlijke gezondheidsomgeving (PGO) is een website of app, waarin je informatie over je eigen gezondheid bij kan houden en actief aan de slag kan gaan met je gezondheid. Zo kan je jouw medische gegevens verzamelen en beheren, maar deze ook delen met anderen. Op deze manier houd je grip op je gezondheidsgegevens. Van behandeling tot lab-uitslagen, medicatie en inentingen. En deze gegevens blijven je hele leven bereikbaar."

27 Een PGO dient te worden onderscheiden van een patiëntenportaal. Een patiëntenportaal is een specifiek aan een zorgverlener gekoppeld zorgverlenerssysteem die aldus ook gebonden is aan de strikte privacybescherming die in het kader van de behandelrelatie geldt (zie het hiervoor besproken onderdeel i).

28 Zie onderdeel (1), sub (b) tot en met (c) van deze notitie. Voor de procedure van het verkrijgen van het MedMij-label wordt onderscheid gemaakt tussen twee soorten dienstverleners. Ten eerste zijn er dienstverleners in het zorgaanbiedersdomein: ze werken samen met zorgaanbieders en leveren de informatiesystemen in een zorginstelling (Dienstverlener zorgaanbieder). Daarnaast zijn er dienstverleners in het persoonlijke domein: zij leveren de PGO's als dienst aan de Persoon, zodat hij regie op zijn gezondheidsgegevens kan uitoefenen (Dienstverlener persoon).

29 Voorbeelden van PGO's die reeds een MedMij-label hebben ontvangen zijn onder meer Zorgkluis B.V., MGP PRO, Careweb, PGO Zwanger, Zodos, MedApp, Icarus en Zorgdoc.

30 Het MedMij-label is bovendien niet van toepassing op gezondheidsapps en wearables (zie hierna).

(3) Privacybescherming bij de verwerking van gezondheidsgegevens door middel van gezondheidsapps of wearables, buiten een behandelrelatie

2.18 De gezondheidsgegevens kunnen ook worden verwerkt door middel van gezondheidsapps of wearables, zijnde draagbare technologie zoals een Fitbit of Apple Watch. Met behulp van deze wearables kunnen gegevens over gezondheid en fitness worden vastgelegd en bijgehouden (denk aan: het aantal stappen dat iemand zet of trappen dat omhoog is gelopen, bloeddruk, hartslag of slaapritme, etc.).[31] Het gaat daarbij niet alleen om het verzamelen van deze gezondheidsgegevens maar ook om de verdere verwerking daarvan, bijvoorbeeld ten behoeve van het doen van suggesties ter verbetering van de gezondheid van de betrokkene.[32] Wij benadrukken dat het aantal gezondheidsapp aanzienlijk hoger is dan het aantal PGO's. Reeds in februari 2018 bestonden er naar schatting 325.000 gezondheidsapps.[33]

2.19 Een aanbieder van een gezondheidsapp of wearable is niet gebonden aan het medisch beroepsgeheim, maar dient wel te beschikken over een doorbrekingsgrond, een wettelijke grondslag en de overige vereisten van de AVG.[34] Het MedMij label is niet van toepassing op de verwerking die plaatsvindt via de gezondheidsapp of wearable. Het MedMij label kan echter wel van toepassing zijn op de via wearable verkregen gegevens die in een PGO worden opgeslagen, althans voor zover de PGO zich heeft aangesloten bij het MedMij-label.

3 Welke risico's voor de privacybescherming van gebruikers worden in de relevante literatuur geïdentificeerd met betrekking tot het buiten de behandelrelatie verzamelen en verwerken van gezondheidsgegevens?

3.1 Er is, als gevolg van digitalisering, sprake van een toename van de mate waarin gezondheidsgegevens buiten een behandelrelatie worden verwerkt. De vraag rijst dan welke risico's het toenemende gebruik van PGO's, gezondheidsapps en wearables met zich meebrengen voor de privacybescherming van patiënten. In dit hoofdstuk bespreken wij eerst de door de Patiëntenfederatie geïdentificeerde risico's. Vervolgens bespreken wij enkele aanvullende in de relevante literatuur geïdentificeerde risico's.

3.2 De Patiëntenfederatie noemt in haar position paper een viertal risico's die gepaard gaan met het in toenemende mate verwerken van gezondheidsgegevens door middel van PGO's, gezondheidsapps of wearables.[35] In de literatuur worden nog een tweetal andere risico's genoemd. We bespreken deze achtereenvolgens. Daarbij merken wij op

---

31 Zie T. Mulder, 'Health apps, their privacy policies and the GDPR', *European Journal of Law and Technology,* 2019, vol. 10.
M. Sax, N. Helberger en N. Bol, 'Health as a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices', Journal of Consumer Policy 2018/41, p. 103-134.

33 NOS, 'Zorgen over wildgroei van gezondheidsapps' van 23 juni 2019. Het betreft een schatting van het National eHealth Living Lab ('NeLL').

34 Zie onderdeel (1), sub (b) tot en met (c) van deze notitie.

35 Zie tevens *Kamerstukken II* 2019/20, 27529, 190.

dat gezondheidsgegevens in de meeste gevallen buiten de behandelrelatie lijken te worden verwerkt door middel van gezondheidsapps of wearables.[36]

Eerste risico – geen medisch beroepsgeheim: aanbieders van PGO's, gezondheidsapps of wearbles worden onder druk gezet om gezondheidsgegevens te delen met derden.

3.3 De Patiëntenfederatie noemt als eerste risico dat de aanbieder van de PGO of de wearable (in veel gevallen) geen gebruik kan maken van een verschoningsrecht en evenmin gebonden is aan een geheimhoudingsplicht.[37] De Wet BIG en de WGBO kennen geen geheimhoudingsplicht voor verwerkingsverantwoordelijken die geen medische hulpverleners zijn. Het verschoningsrecht (van onder meer artikel 218 Sv) is evenmin van toepassing.[38]

3.4 Het ontbreken van het medisch beroepsgeheim brengt met zich mee, vreest de Patiëntfederatie, dat de commerciële partijen die ten behoeve van de gebruiker de gezondheidsgegevens in de PGO of de wearable verwerken, onder druk kunnen worden gezet om de gegevens te verstrekken aan derden. Er is het risico dat een opsporingsdienst via de aanbieder van een PGO of gezondheidsapp het medisch beroepsgeheim kan omzeilen, als een patiënt ervoor kiest gegevens beschikbaar te stellen in zo'n PGO of gezondheidsapp.[39] Ook wordt erop gewezen dat schade- en levensverzekeraars, financiële instellingen, ICT-bedrijven, (semi)overheden zo een aanbieder onder druk kunnen zetten om hen toegang te geven tot deze gegevens.[40]

3.5 Ook de Raad voor de Volksgezondheid en Zorg (**RVZ**) identificeerde in 2015 dit risico. De raad merkte op dat:

> "zonder bescherming door het medisch beroepsgeheim [..] politie, justitie en inlichtingendiensten zoals de National Security Agency (NSA) gegevens [kunnen] vorderen zonder dat er sprake is van een verschoningsrecht."[41]

Tweede risico – patiënten worden onder druk gezet om gegevens te delen.

3.6 Het tweede risico dat volgens de Patiëntenfederatie bestaat bij de verwerking van gezondheidsgegevens buiten de behandelrelatie is het risico dat patiënten onder druk worden gezet om gegevens te delen. Een en ander kan leiden tot een verminderd vertrouwen van de patiënt in de veiligheid van de verwerking van zijn gegevens.

3.7 Van dit risico kan vooral sprake zijn in ongelijkwaardige relaties, waarin iemand afhankelijk is van (semi)overheden, uitkeringsinstanties, verzekeraars of commerciële

---

[36] Reeds in februari 2018 bestonden er naar schatting 325.000 gezondheidsapps. Zie paragraaf 2.18 van dit rapport.
[37] Dit in tegenstelling tot zorgverleners die gebonden zijn aan het medisch beroepsgeheim, zie paragrafen 2.4 tot en met 2.11 van dit rapport.
[38] Zie T. Hooghiemstra, *Informationele zelfbeschikking in de zorg*, Tilburg University 2018, p. 66 en 68 en 155 en 168.
[39] Zie T. Hooghiemstra, *Informationele zelfbeschikking in de zorg*, Tilburg University 2018, p. 66.
[40] Zie hierover Raad voor de Volksgezondheid en Zorg, Patiënteninformatie. Informatievoorziening rondom de patiënt, Den Haag: 2014.
[41] Zie Raad voor de Volksgezondheid en Zorg, *Consumenten-eHealth*, Den Haag: 2015.

partijen. De Patiëntenfederatie heeft de zorg dat die druk toeneemt als individuen hun gezondheidsgegevens zelf beheren. Voor de hand ligt dat de verwerking van gezondheidsgegevens in een PGO of via een wearable is gebaseerd op de uitdrukkelijke toestemming van de betrokkene (patiënt)[42], maar de vraag is of gebruikers van de gezondheidsapps voldoende overzien waarvoor ze toestemming geven (bijvoorbeeld omdat de aanbieder van de PGO of de wearable onvoldoende transparantie betracht over de verdere verwerkingen die vervolgens plaatsvinden).[43] Ook is er het risico dat patiënten te gemakkelijk akkoord gaan met de voorwaarden, omdat zij anders niet van de dienst gebruik kunnen maken.[44] Er is bovendien een risico – zo begrijpen wij de Patiëntenfederatie – dat commerciële partijen en (semi)overheden op deze wijze zonder veel moeite gezondheidsgegevens kunnen verkrijgen en deze vervolgens ten behoeve van commerciële doeleinden verder kunnen verwerken. Een en ander zou kunnen resulteren in ondermijning van het vertrouwen van de patiënt.

Derde risico – de autonomie van de patiënt komt in gevaar.

3.8 De Patiëntenfederatie ziet ook een risico voor de autonomie van de patiënt. De autonomie van een persoon in het kader van gegevensverwerking ziet erop dat een persoon over zijn eigen gegevens kan beschikken en inzicht heeft in wat er met zijn gegevens gebeurd. Het recht op bescherming van persoonsgegevens is een expressie van de autonomie en menselijke waardigheid. En dat kan worden aangetast als de desbetreffende persoon niet meer over de eigen gegevens kan beschikken en inzicht heeft in wat daarmee gebeurt.[45]

Vierde risico – Risico's van verdere verwerking (profilering, stigmatisering).

3.9 Een ander risico dat in de literatuur wordt geïdentificeerd, is het risico dat de aanbieder van de PGO of de wearable de gezondheidsgegevens verder verwerkt, verrijkt en verhandelt,[46] en daarmee profielen opstelt op basis waarvan bijvoorbeeld gepersonaliseerde advertenties worden aangeboden aan de patiënt.[47] Hooghiemstra wijst erop dat het delen van gegevens met derden veel voorkomt bij gezondheidsapps en ook dat individuen op basis van profilering kunnen worden gestigmatiseerd.[48]

---

42 Artikel 9(1) jo. (2)(a) AVG.

43 Zie voor de overheidsinstantie die gezondheidsgegevens verzamelen d.m.v. een PGO: T. Hooghiemstra, *Informationele zelfbeschikking in de zorg*, Tilburg University 2018, p. 56.

44 T. Hooghiemstra, *Informationele zelfbeschikking in de zorg*, Tilburg University 2018, p. 54.

45 Zie hierover: Kamerstukken II 1975-1976,13 872, nr. 3 en T. Hooghiemstra, *Informationele zelfbeschikking in de zorg*, Tilburg University 2018, p. 107.

46 Zie T. Hooghiemstra, *Informationele zelfbeschikking in de zorg*, Tilburg University 2018, p. 53.

47 Profilering houdt volgens artikel 4, onderdeel 4, AVG in: "elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen"

48 Zie T. Hooghiemstra, *Informationele zelfbeschikking in de zorg*, Tilburg University 2018, p. 49; zie bijv. Q. Grundy e.a., 'Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content and network analysis', *the BMJ*, 2019;364;l920.

Vijfde risico – Risico's voor verdere verwerking (nudging).

3.10 Een ander in de literatuur geïdentificeerd risico betreft het risico op verdere verwerking dat leidt tot 'nudging', oftewel de mogelijkheid om het gedrag van individuen te beïnvloeden. De Raad voor de Volksgezondheid stelt vast dat de toegenomen mogelijkheden om gepersonaliseerde adviezen te geven ertoe kan leiden dat individuen worden geconfronteerd met een (morele) verplichting om gezondheidsgegevens over zichzelf te gaan verzamelen en beschikbaar te stellen:

> "Zelfmetingen (medicatietherapietrouw, dieet, beweging, slaap, bloedsuikerspiegels) als objectiveerbare maat voor therapietrouw zouden voorwaardelijk gemaakt kunnen worden voor bepaalde vergoedingen op grond van het verzekerde pakket. Onder deze eis van gegevensverzameling ligt de morele verwachting voor mensen om zich aan bepaalde adviezen te committeren en zich volgens een bepaalde norm te gedragen."[49]

3.11 Ook bestaat bij het gebruik van gezondheidsapps het gevaar van beïnvloeding van het economisch gedrag van personen. Inspelend op de wens van app-gebruikers om gezond te eten, kunnen de aanbieders van gezondheidsapps bijvoorbeeld gaan samenwerken met ondernemingen die gezond eten aanbieden. Het is dan denkbaar dat gebruikers worden aangemoedigd om de diensten van dergelijke ondernemingen af te nemen of om hun websites te bezoeken.[50]

4 In hoeverre kan de huidige relevante wet- en regelgeving de in hoofdstuk 3 geconstateerde risico's verminderen of wegnemen?

4.1 De vraag is in hoeverre de in hoofdstuk 2 beschreven wet- en regelgeving de in hoofdstuk 3 geconstateerde risico's voldoende mitigeert. In dit hoofdstuk analyseren wij per risico welke concrete wettelijke bepalingen reeds een effect hebben, of kunnen hebben, op de gevreesde negatieve gevolgen. Er kan dan per risico een inschatting worden gegeven van het (rest)risico dat zich voordoet als aanvullende wettelijke bescherming, in de vorm van het voorgestelde patiëntgeheim, uitblijft.

Eerste risico – geen medisch beroepsgeheim: aanbieders van PGO's, gezondheidsapps of wearables worden onder druk gezet om gezondheidsgegevens te delen met derden

4.2 Het eerste door de Patiëntenfederatie aangedragen risico is dat de gezondheidsgegevens in een PGO, gezondheidsapp of wearable niet vallen onder de bescherming van het medisch beroepsgeheim. De aanbieder kan dan door derden (bijv. politie, zorgverzekeraars) onder druk worden gezet om gezondheidsgegevens van de patiënt te verstrekken.

---

[49] Raad voor de Volksgezondheid en Zorg, *Consumenten-eHealth*, Den Haag: 2015, p. 36; zie ook M. Sax, N. Helberger en N. Bol, 'Health as a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices', *Journal of Consumer Policy* 2018/41, p. 103-134.

[50] Zie M. Sax, N. Helberger en N. Bol, 'Health as a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices', *Journal of Consumer Policy* 2018/41, p. 103-134.

4.3 De volgende reeds bestaande wettelijke bepalingen mitigeren dit specifieke risico:

(a) De aanbieder is weliswaar niet gebonden aan een medisch beroepsgeheim, maar mag niettemin de gegevens alleen verstrekken als daarvoor een doorbrekingsgrond (onder meer art. 9, tweede lid, AVG) én een wettelijke grondslag (art. 6, eerste lid, AVG) bestaat. Dit impliceert dat, als er geen sprake is van een bijzondere wettelijke grondslag, er uitdrukkelijke toestemming van de betrokkene (patiënt) moet worden verkregen voor een dergelijke verstrekking en verdere verwerking. Deze uitdrukkelijke toestemming moet specifiek zijn en moet door de patiënt kunnen worden geweigerd. Het vragen van (uitdrukkelijke) toestemming tot het verwerken van bijzondere persoonsgegevens als voorwaarde voor de uitvoering van een overeenkomst of het aanbieden van een dienst, leidt er overigens toe dat niet langer gesproken kan worden van vrijelijke toestemming.

(b) Voor zover de verstrekking plaatsvindt op basis van een bijzondere wettelijke grondslag – die de verstrekking van bijzondere persoonsgegevens toelaat – heeft de wetgever de verstrekking blijkbaar toelaatbaar geacht (zie art. 9, eerste lid, aanhef en onderdeel g, AVG);

(c) In aanvulling daarop geldt dat een dergelijke verstrekking zal worden aangemerkt als een verdere verwerking in de zin van artikel 6, vierde lid, AVG. Vereist is dan ofwel (i) toestemming van de patiënt, ofwel (ii) wettelijke grondslag die noodzakelijk en evenredig is voor één van de in artikel 23, eerste lid, AVG genoemde doelstellingen, ófwel (iii) dat er sprake is van een verenigbare verwerking, hetgeen niet voor de hand ligt al was het maar omdat deze verdere verwerking betrekking heeft op bijzondere persoonsgegevens.[51] Een en ander betekent een vergaande beperking van de mogelijkheden voor de aanbieder om zelfstandig te besluiten tot het verstrekken van de gezondheidsgegeven.

(d) Ook het noodzakelijkheidsbeginsel (art. 5, eerste lid, aanhef en onderdeel c, AVG) en de verantwoordingsplicht (art. 5, tweede lid, AVG) zijn relevant. De verstrekking mag slechts plaatsvinden voor zover zowel de aanbieder als de ontvangende derde kunnen aantonen (verantwoordingsplicht) dat de gezondheidsgegevens strikt noodzakelijk en ter zake dienend zijn voor het doel waarvoor de gegevens worden uitgewisseld (noodzakelijkheidsbeginsel). Als deze noodzakelijkheid niet kan worden aangetoond kan de door de Patiëntenfederatie gevreesde verstrekking aan derden geen doorgang vinden.

(e) Verder verlangen de beginselen van gegevensbescherming door ontwerp en standaardinstellingen (privacy by design & by default) (art. 25 AVG) en beveiligingsverplichtingen (art. 32 AVG) dat de aanbieder technische en

[51] Zie art. 6, vierde lid, aanhef en onderdeel c, AVG.

organisatorische maatregelen neemt die bescherming bieden tegen toegang van de gezondheidsgegevens voor derden.

4.4 Tot slot is van belang dat, voor zover de PGO voldoet aan het MedMij-label, de eventuele risico's voor de PGO nog verder worden beperkt. In het MedMij-afsprakenstelsel is tot uiting gebracht dat de deelnemer (aanbieder van PGO) alleen persoonsgegevens aan derden mag verstrekken voor zover dat in de deelnemersovereenkomst is toegestaan of voor zover de wet daartoe verplicht. Het is bovendien uitdrukkelijk verboden om data betreffende de persoon te verkopen.[52] Ook is in het MedMij-afsprakenstelsel een aanvullend normenkader informatiebeveiliging opgenomen, dat eveneens ertoe leidt dat de beveiliging van de gezondheidsgegevens niet zomaar doorbroken mag worden.[53]

4.5 De verschillende reeds bestaande wettelijke bepalingen beperken dus het risico van het ontbreken van het medisch beroepsgeheim. Er is, menen wij, niettemin een restrisico voor de privacybescherming van de betrokkene. Het medisch beroepsgeheim – en het daaraan verbonden (afgeleide) verschoningsrecht – vormt inderdaad een aanvullende drempel om (op verzoek van een derde) over te gaan tot het verstrekken van medische informatie. Daarmee is overigens niet gezegd dat de noodzaak tot het introduceren van aanvullende wettelijke bescherming in de vorm van een nieuw patiëntgeheim is aangetoond. Als de van toepassing zijnde bepalingen goed worden nageleefd, en zo nodig strikt worden gehandhaafd, kan er geen, of alleen in heel beperkte mate, sprake zijn van de door de Patiëntfederatie gevreesde gegevensverstrekkingen. Zeker als sprake is van een PGO waarop ook het MedMij-afsprakenstelsel van toepassing is.

Tweede en derde risico – patiënten onder druk worden gezet om gegevens te delen met mogelijk gevolg dat de autonomie van de patiënt in gevaar komt.

4.6 Ook voor zover het gaat om het risico dat mensen onder druk worden gezet om gegevens te delen, menen wij dat de hiervoor achter (a) tot en met (e) genoemde wettelijke bepalingen het risico in belangrijke mate verkleinen. In aanvulling daarop stellen wij vast dat de zorg dat patiënten onder druk worden gezet en vervolgens overgaan tot verstrekking, in belangrijke mate verband lijkt te houden met het in onvoldoende mate informeren van de betrokkene (patiënt) over de verwerking. De gebrekkige informatiepositie van de patiënt – in combinatie met het gebrek aan juridische kennis - kan ertoe leiden dat de patiënt onbedoeld toestemming geeft. Er zijn evenwel verschillende wettelijke bepalingen en instrumenten beschikbaar die dit risico beperken:

(a) Allereerst dient de patiënt goed en uitvoerig te zijn geïnformeerd over de verwerkingen die plaatsvinden voordat toestemming wordt gegeven (art. 12 en 13 AVG jo. art. 6, eerste lid, aanhef en onder a, AVG). Uit het vereiste van

[52] Zie Afsprakenstelsel MedMij, Afsprakenset 1.1.2, Juridische context, Toelichting AVG-normen, nr. 12.
[53] *Ibidem* nr. 19.

geïnformeerde toestemming volgt bovendien dat de patiënt ook goed moet zijn geïnformeerd over de verwerkingen waarvoor de toestemming wordt gevraagd.

(b) Het vereiste van vrijelijke toestemming sluit uit dat een patiënt onder druk wordt gezet om tegen zijn zin toestemming te geven voor het delen van zijn persoonsgegevens. Als de patiënt onder druk wordt gezet, is er geen sprake van vrijelijk gegeven toestemming. Verder brengt het vereiste van vrijelijke toestemming met zich mee dat toestemming in beginsel niet mag worden ingeroepen als er sprake is van een afhankelijkheidsrelatie tussen de verwerkingsverantwoordelijke en de betrokkene. Ook het vragen om toestemming in ruil voor fikse kortingen of premies kan betekenen dat toestemming niet geacht wordt 'vrijelijk' te zijn.

(c) VWS, de Autoriteit persoonsgegevens (**AP**) en ook de Patiëntenfederatie, kunnen patiënten voorlichting geven en hen informeren dat zij bij het gebruik van een PGO, een wearable of een gezondheidsapp niet zomaar verplicht kunnen worden om toestemming voor de verstrekking van persoonsgegevens aan derden te verlenen (zou een dergelijke verstrekking verplicht zijn, dan zou ook niet om toestemming van de patiënt worden gevraagd).

(d) de AP kan van haar toezichtsbevoegdheden gebruik maken om zo nodig aanbieders van PGO's, wearables en gezondheidsapps te bewegen zich te houden aan het vereiste van geïnformeerde en in vrijheid gegeven toestemming.

4.7 Uit het voorgaande blijkt dat er reeds is voorzien in diverse wettelijke bepalingen bestaan ter bescherming van de patiënt. Waar deze bescherming toch te kort schiet, is aannemelijk dat dit kan worden verholpen door verscherpte toezicht op de naleving van de AVG.

Vierde risico – risico's van verdere verwerking (profilering).

4.8 Voor wat betreft het risico op verdere verwerking, ten behoeve van profileringsdoeleinden, wordt ook dit beperkt door de specifieke regeling die de AVG daarvoor geeft. Voor zover profilering uitsluitend plaatsvindt op geautomatiseerde wijze, dus zonder menselijke tussenkomst, mogen daarbij alleen gezondheidsgegevens worden verwerkt met uitdrukkelijke toestemming van de patiënt (art. 22, vierde lid, AVG) of op basis van een specifieke wettelijke grondslag (als bedoeld in art. 9, tweede lid, aanhef en onderdeel g, AVG). Verwezen wordt naar de in het voorgaande gemaakte opmerkingen over geïnformeerde en vrijelijk gegeven toestemming.

4.9 Wij beoordelen dit door de Patiëntfederatie genoemde privacyrechtelijke risico, gelet op de strikte regels voor profilering, als beperkt.

Vijfde risico – risico's voor verdere verwerking (nudging).

4.10 Voor het risico op nudging gelden in beginsel dezelfde mitigerende wettelijke bepalingen als omschreven bij het eerste risico. Verwezen wordt naar de in randnr. 4.3 van dit rapport genoemde bepalingen. Voor zover het gaat om een PGO die is aangesloten bij het MedMij-label, gelden uiteraard aanvullend de strikte MedMij-afspraken.

4.11 Ook hier achten wij het restrisico voor de privacybescherming van de patiënt beperkt.

5 Voor zover zich eventuele restrisico's voor de privacybescherming van gebruikers blijven voordoen, welke voor- en nadelen heeft de introductie van) patiëntgeheim ten opzichte van het vasthouden aan de huidige wet- en regelgeving?

5.1 De Patiëntenfederatie doet het voorstel om de bestaande wet- en regelgeving genoemd in hoofdstuk 2 van dit rapport aan te vullen met het zogenoemde patiëntgeheim, zodat de in hoofdstuk 3 genoemde risico's bij de verwerking van gezondheidsgegevens buiten de behandelrelatie worden weggenomen.

5.2 Het patiëntgeheim zou volgens de Patiëntenfederatie kunnen inhouden dat de aanbieder van een PGO, een gezondheidsapp of een wearable wordt gebonden aan een verschoningsrecht of een geheimhoudingsplicht ten aanzien van de gezondheidsgegevens die de aanbieder ten behoeve van de patiënt verwerkt en toezicht en handhaving daarop. Het patiëntgeheim zou bovendien kunnen regelen dat een patiënt niet onder druk kan worden gezet om zijn gegevens te delen. Meer concreet zou het patiëntgeheim volgens de Patiëntenfederatie de volgende vormen kunnen aannemen:

- aanpassing van het Wetboek van Strafrecht (Boek 2), zodat ook PGO-aanbieders en andere aanbieders van gezondheidsgegevens onder het verschoningsrecht vallen;
- aanpassing van het bestuursrecht (Awb, sociale zekerheidswetgeving bijv. rond uitkeringsorganisaties) om daarin een patiëntgeheim op te nemen in situaties waarbij er sprake is van verzoeken om gezondheidsgegevens vanuit de overheid;
- aanpassing van het privaatrecht, voor verzoeken om gezondheidsgegevens door private partijen;
- verplichtstelling van de informatiebeveiligingsnorm NEN7510 voor alle organisaties die gezondheidsgegevens verwerken.

5.3 Vastgesteld is dat de geïdentificeerde risico's grotendeels al worden weggenomen of beperkt door bestaande wet- en regelgeving. Om deze reden achten wij het niet zonder meer aangetoond dat het invoeren van een wettelijk patiëntgeheim, in de zin

van het introduceren van nieuwe wettelijke waarborgen, noodzakelijk is. De vraag is of zo een wettelijk patiëntgeheim werkelijk zal leiden tot het oplossen of verminderen van deze risico's, dat er geen minder bezwarende alternatieven zijn, én dat de kosten en lasten daarvan gerechtvaardigd worden door de ernst van het probleem.[54] Er is weliswaar vastgesteld dat er restrisico's voor patiënten zijn, maar vooralsnog is niet aangetoond dat minder vergaande alternatieven deze restrisico's niet voldoende zouden kunnen mitigeren. Alternatieven waaraan zou kunnen worden gedacht omvatten (i) het verhogen van de weerbaarheid en de informatiepositie van de patiënt door informatiecampagnes, (ii) het intensiveren van het toezicht op beheerders van PGO's, gezondheidsapps en wearables en (iii) het introduceren van (met het MedMij-label vergelijkbare) certificeringsmechanismen voor gezondheidsapps en wearables. Als blijkt dat deze alternatieven onvoldoende effect sorteren, kan dit aanleiding vormen om nieuwe wetgeving in overweging te nemen.

5.4 Het voorgestelde wettelijk patiëntgeheim heeft als voordeel dat een extra wettelijke bescherming wordt gecreëerd die de aanbieder van PGO's, gezondheidsapps en wearables en de patiënt zelf meer en vooral duidelijkere mogelijkheden biedt om de verstrekking van medische informatie te weigeren. Er zijn echter ook nadelen. De belangrijkste daarvan is, naar onze mening, dat het, in termen van privacybescherming, per saldo weinig toevoegt en tegelijkertijd verwachtingen wekt die uiteindelijk niet reëel kunnen blijken te zijn. Aannemelijk is immers dat het patiëntgeheim – net als het medisch beroepsgeheim – niet absoluut zal zijn. Ook het patiëntgeheim zal in voorkomende gevallen met toestemming van de patiënt kunnen worden doorbroken. Als zodanig beperkt de introductie van het patiëntgeheim niet de risico's die ermee verband houden dat patiënten onvoldoende geïnformeerd en/of niet in vrijheid deze toestemming geven.

5.5 Een belangrijke factor daarbij is dat de extra bescherming die het beroepsgeheim en het verschoningsrecht bieden, afhankelijk is van de eigen afweging van de zorgverlener. Deze afweging kán erin resulteren dat de zorgverlener met het oog op goed hulpverlenerschap – ondanks toestemming van de patiënt – weigert informatie te verstrekken. Dit motief ontbreekt bij een commerciële beheerder van een PGO, een gezondheidsapp of een wearable. Dit doet wederom de vraag opkomen of een patiëntgeheim in de praktijk wel echt tot hoger bescherming zal leiden.

5.6 Er is nog een ander nadeel. De wetgever dient rekening te houden met de nadelige gevolgen die het invoeren van het patiëntgeheim zou kunnen hebben. Het medisch beroepsgeheim en het daaruit voortvloeiende verschoningsrecht kunnen in de weg staan aan de waarheidsvinding. De wetgever acht dit acceptabel gezien de maatschappelijke en persoonlijke belangen dat een patiënt zich vrijelijk en zonder vrees voor openbaarmaking van zijn medische situatie om bijstand en advies kan

[54] Zie artikel 2.2 van de Aanwijzingen voor regelgeving. Een relevante factor bij de lasten van de invoering van het patiëntgeheim is dat het introduceren van het patiëntgeheim in zijn huidige vorm zal moeten leiden tot diverse wetswijzigingen, die naar verwachting tot een langdurig wetgevingstraject zullen leiden.

wenden tot een arts. Van dergelijke belangen is niet zonder meer sprake waar het gaat om aanbieders van gezondheidsapps, PGO’s of wearables.

****