Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

27 529 **Informatie- en Communicatietechnologie (ICT) in de Zorg**

32 761 **Verwerking en bescherming persoonsgegevens**

Nr. 190 **BRIEF VAN DE MINISTER VOOR MEDISCHE ZORG**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 1 oktober 2019

Op 29 januari 2019 heb ik u de position paper «Het Patiëntgeheim» van Patiëntenfederatie Nederland (hierna: de Patiëntenfederatie) gestuurd[1]. Ik heb in het Algemeen Overleg (AO) van 30 januari 2019 inzake «Gegevensuitwisseling in de zorg / gegevensbescherming» in reactie op die position paper gezegd dat ik gegevensuitwisseling in de zorg heel belangrijk vind, maar dat dit alleen maar gaat werken als patiënten zeker weten dat hun gegevens veilig zijn. Ik kan mij dan ook heel goed voorstellen dat de Patiëntenfederatie voor een patiëntgeheim aandacht vraagt. U heeft mij gevraagd voor het AO Gegevensuitwisseling en gegevensbescherming begin oktober te komen met een reactie op dit position paper en te onderzoeken of de bescherming van patiëntgegevens afdoende is en of er geen witte vlekken zijn. In deze brief ga ik in hoofdlijnen in op het beleid inzake bescherming van gezondheidsgegevens en gebruikers van applicaties (apps) waarin gezondheidsgegevens worden opgeslagen. In de bijlage bij deze brief treft u de analyse aan en mijn reactie op de voorstellen van de Patiëntenfederatie.

Digitalisering in de zorg

In eerdere debatten met uw Kamer ben ik al ingegaan op het belang van een goede digitale infrastructuur in de zorg en digitale uitwisseling van gegevens zowel tussen zorgprofessionals onderling als tussen zorgprofessional en de patiënt.[2] Digitalisering verandert echter niet alleen de uitwisseling van gezondheidsgegevens tussen en met zorgprofessionals binnen de zorg.

Digitalisering heeft ook tot gevolg dat mensen steeds vaker buiten de zorgcontext de beschikking krijgen over hun eigen gezondheidsgegevens via het gebruik van allerlei gezondheidsapps, draagbare technologie

[1] Kamerstuk 27 529, nr. 169
[2] Kamerstuk 27 529, nr. 180

kst-27529-190
ISSN 0921 - 7371
's-Gravenhage 2019

(wearables[3]) en persoonlijke gezondheidsomgevingen (PGO's). Via met name PGO's krijgen mensen meer inzicht in en controle over hun gezondheid omdat PGO's mensen in staat stellen om via een website of app alle relevante gezondheidsgegevens, die verspreid liggen opgeslagen bij bijvoorbeeld huisartsen, ziekenhuizen of apotheken in te zien en aan te vullen met zelf gegenereerde (meet)gegevens van bijvoorbeeld een stappenteller of glucosemeter. Met een PGO kan iemand daarom meer regie krijgen over zijn gezondheid en zijn gezondheidsgegevens. Ik ben daar een groot voorstander van en met mij een groot aantal branchepartijen in de zorg en de Patiëntenfederatie. Ik stimuleer dan ook de ontwikkeling van PGO's door marktpartijen door deelname aan MedMij[4]. Ook stimuleer ik het gebruik van PGO's met een MedMij keurmerk via een aankomende tijdelijke financieringsregeling zodat iedere Nederlander die dat wil kosteloos een PGO kan kiezen en gebruiken. Via de VIPP-programma's[5] stimuleer ik bovendien de implementatie van de MedMij-standaarden in diverse sectoren, waaronder de huisartsenzorg, ziekenhuiszorg, GGZ, langdurige zorg en geboortezorg.

Position paper Patiëntenfederatie

De ontwikkeling dat mensen steeds meer de beschikking krijgen over hun eigen gezondheidsgegevens versterkt hun positie en maakt dat zij meer grip kunnen krijgen op hun gezondheid. Dit brengt echter ook nieuwe vraagstukken met zich, bijvoorbeeld op het terrein van privacy. Gezondheidsgegevens van een persoon worden in verschillende omvang en samenstelling op steeds meer plaatsen buiten de zorg bewaard, onder meer bij de private aanbieders van apps en in PGO's. Dit is het punt waar de Patiëntenfederatie aandacht voor vraagt. De Patiënten-federatie vraagt extra maatregelen om te waarborgen dat de gegevens bij deze leveranciers veilig zijn, en dat mensen beschermd worden tegen druk van (machtige) derden om de gezondheidsgegevens te delen. De Patiëntenfederatie stelt onder meer voor om het medisch beroepsgeheim, dat alleen geldt voor hulpverleners, te verbreden naar leveranciers van PGO's en andere beheerders van gezondheidsgegevens, zoals Google, Philips, Apple of Samsung. Dit «patiëntgeheim» zou ertoe leiden dat ook de leveranciers een wettelijke zwijgplicht hebben. Deze zwijgplicht dient volgens de Patiëntenfederatie vergezeld te gaan van een verschoningsrecht voor leveranciers en gebruikers van PGO's en andere apps wanneer zij voor de rechter komen te staan.

1. Bescherming onder huidig recht voldoende

Ik ben het met de Patiëntenfederatie eens dat het heel belangrijk is dat gebruikers van PGO's en apps zeker weten dat hun gegevens veilig zijn. Enerzijds omdat de privacy van de gebruikers geborgd moet zijn en anderzijds omdat de gebruikers het vertrouwen moeten hebben om apps daadwerkelijk te gebruiken. Ook uw Kamer acht het van belang dat gegevens voldoende worden beschermd. De motie van het lid Hijink[6] vraagt om te voorkomen dat de gegevens in het PGO gebruikt worden voor commercieel gewin. Uit de analyse, opgenomen in de bijlage bij deze brief, blijkt dat met de huidige wetgeving, aangevuld met het MedMij

---

[3] Voorbeeld van een wearable is een horloge dat onder meer het aantal gezette stappen kan meten, evenals de bloeddruk, de hartslag, en het slaapritme van een persoon.

[4] MedMij is een samenwerkingsverband van brancheorganisaties, verenigingen van huisartsen, ziekenhuizen, apothekers, thuisorganisaties, verpleeghuizen, zorgverzekeraars, patiënten en lokale overheden. MedMij stelt spelregels op voor de manier waarop PGO's gegevens uitwisselen.

[5] VIPP= Versnellingsprogramma Patiënt en Professional. Beleidsregels subsidiëring Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional, Stcrt. 2019, nr. 27176

[6] Kamerstuk 27 529, nr. 178

afsprakenstelsel voor PGO's, er al veel geregeld is voor de bescherming van gezondheidsgegevens of gebruikers van PGO's en gezondheidsapps.

Zo volgt uit de Algemene Verordening Gegevensbescherming (AVG) dat niet meer persoonsgegevens mogen worden verwerkt dan noodzakelijk en dat persoonsgegevens niet zonder meer voor andere (commerciële) doelen kunnen worden gebruikt. Ook regelt de AVG bijvoorbeeld dat toestemming van een betrokkene een uitdrukkelijke, vrije, specifieke, geïnformeerde en ondubbelzinnige uiting van de wens van de betrokkene moet zijn en dat de verwerkingsverantwoordelijke moet kunnen aantonen dat er toestemming is gegeven. Bovendien kunnen PGO-leveranciers onder voorwaarden al een afgeleid verschoningsrecht[7] hebben als het gegevens betreft die tot stand zijn gebracht in de vertrouwelijke relatie tussen arts en de patiënt, zoals gegevens uit het medisch dossier.

Gelet op het bovenstaande is aanvullende wet- en regelgeving dan ook niet nodig.

2. Accent op toepassing bestaande regels en bewustwording

Om de gezondheidsgegevens van de patiënt te beschermen, moet het accent liggen op een goede toepassing van de al bestaande regels. In dat kader hebben onlangs de eerste PGO's het MedMij keurmerk gekregen, wat betekent dat na een uitvoerig toetsings- en auditproces met zekerheid is vastgesteld dat deze PGO's aan alle afspraken en eisen van MedMij voldoen. Door de toetsing aan deze afspraken is geborgd dat deze PGO's veilig met de gezondheidsgegevens omgaan, dat gegevens alleen worden gedeeld als daar door de desbetreffende persoon in de PGO expliciet toestemming voor gegeven is en dat data door de PGO-leverancier niet kunnen worden doorverkocht. De verwachting is dat in de loop van jaar meer PGO's het MedMij keurmerk zullen krijgen, mits zij de strenge toetsing doorstaan. Met het afsprakenstelsel van MedMij loopt de zorgsector voorop in het waarborgen van kaders voor een veilige en betrouwbare uitwisseling van gegevens, maar dat wil niet zeggen dat het hier ophoudt.

Bewustwording

Om te waarborgen dat de huidige wettelijke regels goed werken, is het van belang dat iedereen op de hoogte is van zijn rechten en plichten op het gebied van het delen van gezondheidsgegevens. Dat geldt niet alleen voor burgers, maar ook voor personen die werken bij organisaties die gezondheidsgegevens verwerken. Bewustwording van de rechten en plichten leidt tot vertrouwen in het gebruik van ondersteunende diensten. Dat vind ik, net als de Patiëntenfederatie, heel belangrijk. Dat geldt voor mij specifiek daar waar het gaat om vertrouwen in PGO's, gezien de hierboven genoemde positieve effecten.

Gezien de signalen van de Patiëntenfederatie en de reacties op dit position paper, wil ik nog steviger inzetten op bewustwording. Daarom ben ik voornemens om financiële middelen ter beschikking te stellen om een bewustwordingscampagne te starten om mensen verder bekend te maken met hun rechten ten aanzien van het gebruik van hun gezondheidsgegevens. Ik betrek de Patiëntenfederatie bij de verdere vormgeving hiervan. Meer specifiek gaat het om een campagne om burgers en

[7] Het kenmerk van het afgeleide verschoningsrecht is dat de houder hiervan niet zelfstandig kan beoordelen of het beroepsgeheim mag worden doorbroken. Deze beoordelingsbevoegdheid komt als uitgangspunt slechts de »primaire» houder van het beroepsgeheim toe, dus aan de hulpverlener.

zorgverleners te informeren over de toegevoegde waarde van PGO's en e-health. Ik wil in die campagne mensen ook wijzen op het belang van het zorgvuldig omgaan met gezondheidsgegevens.

Ten slotte zoek ik, waar mogelijk, aansluiting bij campagnes die op andere terreinen worden voorbereid of uitgevoerd en die betrekking hebben op digitale bewustwording (zoals die de Autoriteit Persoonsgegevens in mei van dit jaar is gestart) en vaardigheden van mensen. Zo ben ik aangesloten bij een interdepartementaal actieplan om digitale basisvaardigheden van mensen te vergroten, mede met het oog op digitale ontwikkelingen in de samenleving. Dit actieplan is op 18 maart 2019 naar uw Kamer gestuurd[8].

Beleidsbrief Regie op gegevens

Het onder regie van de burger zelf digitaal delen van gegevens met andere organisaties speelt niet alleen op het terrein van de gezondheidsgegevens, maar op veel meer terreinen, zoals het terrein van financiële gegevens, mobiliteitsgegevens of woongegevens. Daarom is het Ministerie van BZK het overheidsbrede programma Regie op Gegevens gestart, waarin ook mijn ministerie participeert. Het uitgangspunt van dit programma is dat het digitaal kunnen delen van gegevens een grote bijdrage kan leveren aan meerdere maatschappelijke doelen, zoals meer autonomie van de burger, een betere publieke en private dienstverlening, en minder administratieve rompslomp. Het digitaal kunnen delen van gegevens biedt echter niet alleen kansen, maar vergt ook spelregels waar alle betrokken partijen aan moeten voldoen.

De Staatssecretaris van BZK schetst in zijn beleidsbrief Regie op Gegevens van 11 juli jongstleden de wenselijkheid van deze ontwikkeling, maar ook de wenselijkheid hiervoor, aanvullend op bestaande wetgeving (en dan met name de AVG), overheidsbrede kaders vast te stellen en deze wettelijk te verankeren, bijvoorbeeld in de Wet digitale overheid.[9] Dit kader vormt daarmee een fundament onder de (zorgspecifieke) kaders die voor MedMij zijn en worden ontwikkeld.

Ik ben aangesloten bij het programma Regie op Gegevens om vanuit dat kader te bezien of er vanuit het perspectief van de zorg nog iets mist.

Ik hoop u met deze brief voldoende te hebben geïnformeerd en acht de motie Hijink met deze brief ook afgedaan.

De Minister voor Medische Zorg,
B.J. Bruins

[8] Kamerstuk 28 760, nr. 84
[9] Kamerstuk 32 761, nr. 147

BIJLAGE

Deze bijlage betreft de analyse van de position paper van Patiëntenfederatie Nederland (hierna: de Patiëntenfederatie) van 17 januari 2019. De bijlage bestaat uit vier onderdelen.

- In onderdeel A wordt een samenvatting gegeven van de position paper van de Patiënten federatie.
- In onderdeel B wordt ingegaan op de waarborgen in het huidige recht voor de bescherming van gezondheidsgegevens. In onderdeel B1 wordt ingegaan op waarborgen voor de bescherming van gezondheidsgegevens bij hulpverleners en in onderdeel B2 op de waarborgen wanneer gezondheidsgegevens in beheer bij anderen dan hulpverleners zijn.
- In onderdeel C wordt ingegaan op de waarborgen in het huidige recht tegen druk van derden. In onderdeel C1 wordt ingegaan op het uitgangspunt toestemming bij gegevensuitwisseling en in onderdeel C2 op de grenzen die de huidige wet- en regelgeving stelt.
- In onderdeel D wordt ingegaan op technische waarborgen.

A. Samenvatting position paper Patiëntenfederatie

De Patiëntenfederatie geeft in de position paper aan dat er steeds meer plekken komen waar gezondheidsgegevens door anderen dan hulpverleners worden bewaard, zoals in Persoonlijke Gezondheidsomgevingen (PGO's). De Patiëntenfederatie betwijfelt of deze gegevens bij deze partijen voldoende beschermd zijn.
Daarnaast merkt de Patiëntenfederatie op dat de patiënt of consument (hierna: de zorggebruiker) door deze ontwikkelingen steeds meer zelf de beschikking krijgt over deze gegevens. De Patiëntenfederatie vraagt in de position paper aandacht voor het gevaar van het onder druk zetten van een zorggebruiker om toestemming te geven om medische gegevens te delen. Bijvoorbeeld door (semi-) overheden, verzekeraars, hypotheekverstrekkers, justitie, inlichtingendiensten of commerciële partijen. De Patiëntenfederatie vraagt zich af of de zorggebruiker altijd sterk genoeg is om deze druk te weerstaan. De Patiëntenfederatie merkt daarbij op dat gegevens die buiten de zorgsector worden opgeslagen niet onder het medisch beroepsgeheim vallen.

Om te waarborgen dat degenen die de gezondheidsgegevens van zorggebruikers bewaren prudent met deze gegevens omgaan, en om zorggebruikers te sterken in het weerstaan van druk, stelt de Patiëntenfederatie maatregelen voor.

Deze hebben enerzijds betrekking op het inzetten op bewustwording van zorggebruikers. Anderzijds stelt de Patiëntenfederatie voor om wettelijk vast te leggen:
- een medisch beroepsgeheim voor de beheerder van gezondheidsgegevens, bestaande uit een geheimhoudingsplicht, een verschoningsrecht en toezicht en handhaving daarop (in de position paper «het patiëntengeheim» genoemd);
- een verbod op het onder druk zetten van een zorggebruiker om medische gegevens te delen, en toezicht en handhaving daarop;
- technische normen:
  - alle organisaties die gezondheidsgegevens verwerken moeten voldoen aan de norm voor informatiebeveiliging NEN 7510; en
  - er moet een verplichte NEN-norm komen die gaat over de consequenties van de verplichting dat systemen ontworpen moeten worden met privacy als uitgangspunt.

B. Waarborgen bescherming gezondheidsgegevens

Omwille van de leesbaarheid is hieronder een samenvatting opgenomen van de juridische analyse van de bescherming van gezondheidsgegevens:

Gezondheidsgegevens in:	Zijn gegevens voldoende beschermd	Hoe	Geregeld in:
Medische dossiers van hulpverleners	Ja	Via het medisch beroepsgeheim en de Algemene Verordening Gegevensbescherming (hierna: AVG)	– Artikel 457 van boek 7 van het Burgerlijk Wetboek (Wet op de geneeskundige behandelingsovereenkomst, oftewel Wgbo) – artikel 88 van de Wet beroepen in de individuele gezondheidszorg – de AVG
PGO's	Ja	Via de AVG, aangevuld met Afsprakenstelsel Medmij en, voor zover het gegevens betreft die tot stand zijn gebracht in het kader van de vertrouwelijke relatie tussen arts en patiënt, via het afgeleid verschoningsrecht	– de AVG – het Afsprakenstelsel Medmij – jurisprudentie
Gezondheidsapps	Ja	Via de AVG	– de AVG

B1. Waarborgen bescherming gegevens bij hulpverlener

Het medisch beroepsgeheim houdt in dat een hulpverlener in beginsel moet zwijgen over alles dat aan hem door de patiënt wordt toevertrouwd. Het medisch beroepsgeheim is geregeld in artikel 457 van de Wgbo en artikel 88 van de Wet beroepen in de individuele gezondheidszorg (hierna: Wet BIG). Het belang van het wettelijk beroepsgeheim wordt onderstreept door de strafbaarstelling van schending ervan.[10] In het verlengde van het medisch beroepsgeheim ligt het verschoningsrecht[11]. Dit houdt kort gezegd in het recht van een getuige om vragen van een rechter niet te hoeven beantwoorden. Onderdeel van verschoningsrecht van de getuige is dat de justitiële autoriteiten in beginsel geen kennis kunnen nemen van datgene wat in het contact tussen de verschoningsgerechtigde hulpverlener en hulpzoekende schriftelijk is vastgelegd.[12]

Het medisch beroepsgeheim is ontwikkeld ter bescherming van zowel het individu als de samenleving en garandeert de vrije toegang tot de zorg voor iedereen. Dat wil zeggen dat iedereen zich vrijelijk en zonder vrees voor openbaarmaking medische hulp kan zoeken. Gezien het doel van het medisch beroepsgeheim richt het beroepsgeheim zich tot specifieke beroepsbeoefenaars. Het medisch beroepsgeheim in de Wgbo richt zich tot hulpverleners die een handeling op het gebied van de geneeskunst verrichten. Het medisch beroepsgeheim in de Wet BIG richt zich tot een

[10] Artikel 272 van het Wetboek van Strafrecht.
[11] Vastgelegd in artikel 218 van het Wetboek van Strafvordering (Sv), artikel 5:20 van de Algemene wet bestuursrecht (Awb) en 165, tweede lid, Wetboek van Burgerlijke Rechtsvordering (Rv).
[12] Vastgelegd in de artikelen 96a en 98 Sv en artikel 843a, derde lid, Rv.

ieder die een beroep op het gebied van de individuele gezondheidszorg uitoefent.

B2. Waarborgen bescherming gezondheidsgegevens in beheer bij anderen dan hulpverleners

B2a. Algemeen

De AVG biedt al veel waarborgen voor de bescherming van gezondheidsgegevens en stelt eisen aan de verwerking ervan. Hieronder wordt ingegaan op een aantal van deze waarborgen en eisen.

Rechtmatigheid gegevensverwerking

Volgens de AVG is het verwerken (zoals verzamelen, gebruiken of verstrekken) van gegevens over de gezondheid van iemand is in beginsel verboden. Dit is alleen anders als een van de limitatieve[13] uitzonderingsgronden van toepassing is (artikel 9, tweede lid, van de AVG).
Eén van die uitzonderinggronden betreft «uitdrukkelijke toestemming», waaraan de AVG specifieke eisen stelt. Zo moet uitdrukkelijke toestemming een vrije, specifieke, geïnformeerde en ondubbelzinnige uiting van de wens van de betrokkene zijn en moet de verwerkingsverantwoordelijke ook kunnen aantonen dat er toestemming is gegeven (artikel 7 van de AVG). Hierbij is ook van belang dat in geval van een schriftelijke verklaring, het verzoek om toestemming in begrijpelijke en gemakkelijk toegankelijke vorm aangeboden moet worden, en in duidelijke en eenvoudige taal. Daarnaast kan de betrokkene de toestemming te allen tijde intrekken zonder opgaaf van redenen en dient het intrekken van de toestemming net zo eenvoudig te zijn als het geven. Vanaf het moment van intrekken is de verwerking niet rechtmatig meer (tenzij die op een andere grondslag kan worden gebaseerd).

Plichten verwerkingsverantwoordelijke

Op grond van artikel 5 van de AVG moet elke verwerking van persoonsgegevens voldoen aan onder meer de volgende beginselen:
- de verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn («rechtmatigheid, behoorlijkheid en transparantie»);
- de verwerking moet gebonden zijn aan specifieke verzameldoelen («doelbinding»);
- de persoonsgegevens moeten toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is («minimale gegevensverwerking»); en
- gegevens moeten goed beveiligd zijn en vertrouwelijk blijven («integriteit en vertrouwelijkheid»).

De verwerkingsverantwoordelijke moet kunnen aantonen dat een verwerking van gegevens voldoet aan de beginselen uit de AVG (de verantwoordingsplicht).

Tevens stelt de AVG specifieke eisen aan de doorgifte van persoonsgegevens naar landen buiten de Europese Unie. Derde landen moeten ten minste een «passend» beschermingsniveau bieden. Wanneer een land niet als adequaat is aangemerkt, dan is doorgifte alleen mogelijk wanneer sprake is van «passende waarborgen» of in «afwijkende specifieke situaties». In dat laatste geval moeten betrokkenen uitdrukkelijke met de doorgifte instemmen en moeten betrokkenen zijn ingelicht over de risico's.

[13] Sommige onderdelen van de opsomming geven de nationale wetgever wel de ruimte om zelf nieuwe uitzonderingen te creëren.

Transparantie en informatieplicht

Het hierboven genoemde beginsel van transparantie is in de AVG uitgewerkt. Zo moet een betrokkene op de hoogte worden gesteld van het feit dat er verwerking van zijn persoonsgegevens plaatsvindt, en wat de doeleinden van deze verwerking zijn (artikel 12 van de AVG). Bovendien moet de verwerkingsverantwoordelijke in een beknopte en transparantie, begrijpelijke vorm informeren over:

– wanneer persoonsgegevens bij de betrokkene worden verzameld (artikel 13 van de AVG);
– wanneer de persoonsgegevens niet van de betrokkene zijn verkregen (artikel 14 van de AVG);
– de rechten van de betrokkene: recht op inzage, recht op rectificatie, recht om te worden vergeten, recht op beperking van de verwerking, kennisgevingsplicht, recht op overdraagbaarheid van gegevens (artikelen 15 tot en met 22 van de AVG).

Passende technische en organisatorische maatregelen

Tevens dienen er technische en organisatorische maatregelen genomen te worden dat een passende beveiliging is gewaarborgd en dat de gegevens zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (artikel 32 van de AVG). Dit betekent onder meer dat bij het inrichten van verwerkingen rekening moet worden gehouden met het principe van privacy door ontwerp en standaardinstellingen (*privacy by design & default* (artikel 25 van de AVG)) en passende maatregelen moeten worden getroffen met het oog op de bescherming van persoonsgegevens.

Toezicht en handhaving

In de AVG staan veel waarborgen voor de bescherming van bijzondere gegevens, zoals gezondheidsgegevens. De Autoriteit Persoonsgegevens (hierna: AP) houdt toezicht op de naleving van deze voorschriften.

Het toezicht houden op gegevensverwerkingen door verwerkingsverantwoordelijken is de *core business* van de AP. Daarbij beziet de AP of verwerkingsverantwoordelijken niet meer gegevens verzamelen dan noodzakelijk (waarbij onder meer gekeken wordt naar proportionaliteit en evenredigheid) en zich houden aan het doelbindingsbeginsel.

Zorggebruikers kunnen klachten bij de AP indienen als ze vinden dat een partij zich niet houdt aan de privacyregels. Zo kan iemand een klacht indienen jegens een PGO-leverancier, een leveranciers van andere gezondheidsapps of een zorginstelling[14], omdat er onzorgvuldig wordt omgegaan met gezondheidsgegevens. Ook kan een klacht worden ingediend als iemand onder druk gezet wordt om toestemming te geven voor het delen van zijn gezondheidsgegevens.

De AP moet elke klacht behandelen. Soms kunnen klachten ertoe leiden dat de AP een controlerend onderzoek doet. Uit zo'n onderzoek kan blijken dat er sprake is van een overtreding van de AVG. De AP kan dan handhavend optreden en een boete, last onder dwangsom of verwerkingsverbod opleggen. In de AVG, de Uitvoeringswet AVG en de Awb is geregeld welke bevoegdheden de AP heeft. Overigens kan de AP ook

[14] In het toezichtkader van de AP voor 2018–2019 staat dat de AP bij zorginstellingen extra focus legt op de beveiliging van medische gegevens en op de vraag of de verwerking gebaseerd is op de juiste grondslag. Zie https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezichtkader_autoriteit_persoonsgegevens_2018–2019.pdf, pagina 8

onderzoeken instellen naar aanleiding van berichten in de media. De AP ontvangt klachten die onder meer gaan over het door verwerkingsverantwoordelijke opvragen van meer persoonsgegevens dan noodzakelijk is. De AP onderzoekt deze klachten en daar waar sprake blijkt te zijn van het uitoefenen van druk en bewust meer opvragen van persoonsgegevens, kan dit een verzwarende omstandigheid zijn bij het kiezen van het instrument van handhaving en het handhavingstraject.

De AP houdt zich ook bezig met bewustwording van het publiek over vraagstukken die spelen rond gegevensbescherming. Zo is de AP onlangs een publiekscampagne gestart die burgers meer bewust moet maken van hun privacyrechten[15] (zie ook hulpbijprivacy.nl).
Ook hebben de gezamenlijke Europese toezichthouders, verenigd in de EDPB, in een richtlijn meer informatie gegeven over toestemming en welke randvoorwaarden daarbij gelden. Die richtlijn biedt meer waarborgen voor een goede toepassing van de AVG. Deze richtlijn is op de website van de AP te raadplegen.[16]

B2b. Afgeleid verschoningsrecht

Naast de AVG en het toezicht daarop door de AP, kan onder omstandigheden (voor leveranciers van PGO's en patiënten) een afgeleid verschoningsrecht gelden. Dit kan wanneer het gaat om gegevens:
– die tot stand zijn gebracht in de vertrouwelijke communicatie tussen arts en patiënt; én
– waarvan met de verstrekking de vertrouwelijkheid niet is opgegeven.

Het eerste criterium brengt met zich dat gegevens uit bijvoorbeeld een medisch dossier onder het afgeleid verschoningsrecht kunnen vallen, maar gegevens die op een andere manier zijn gegenereerd (bijvoorbeeld in een stappenteller) niet. Ook niet als zij in een PGO worden opgeslagen. Het tweede criterium houdt in dat als de vertrouwelijkheid is opgegeven, niet meer kan worden gesteld dat het verschoningsrecht zich over de informatie aangetroffen bij de derde uitstrekt. Van het opgeven van de vertrouwelijkheid is sprake als een patiënt besluit informatie breder te verspreiden dan noodzakelijk is in verband met de bijstand en advies die hij nodig heeft en daarmee de vertrouwelijkheid van de informatie prijsgeeft. In dit verband kan worden gedacht aan gevallen waarin ook anderen dan de patiënt en zijn hulpverleners toegang hebben tot de gegevens. De vertrouwelijkheid wordt niet geacht te zijn opgeheven als de gegevens uit een medisch dossier met toestemming van de patiënt alleen in een PGO zijn opgenomen en alleen de patiënt zelf en zijn hulpverleners toegang hebben tot die gegevens.
Met «afgeleid» wordt bedoeld dat het in beginsel de primair verschoningsgerechtigde (de hulpverlener) is die beslist of het verschoningsrecht in het geding is en of daarop een beroep wordt gedaan. Dit betekent dat het de (oorspronkelijke) verschoningsgerechtigde degene is die beslist of er een beroep wordt gedaan op het verschoningsrecht en dat de afgeleid verschoningsgerechtigde dus niet zelfstandig kan beslissen van een beroep daarop af te zien.

Als geen sprake is van een (afgeleid) verschoningsrecht, waarop een beroep kan worden gedaan, betekent dat overigens nog niet dat gezond-

[15] Zie ook: www.hulpbijprivacy.nl
[16] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht#hoe-kan-ik-aantonen-dat-ik-toestemming-heb-ontvangen-6160

heidsgegevens zonder meer kunnen worden gevorderd.[17] De verstrekking van deze gegevens kan alleen worden gevorderd door de officier van justitie:
– bij verdenking van een misdrijf ter zake waarvan voorlopige hechtenis mogelijk is, en het betreffende misdrijf een ernstige inbreuk oplevert op de rechtsorde[18];
– als het onderzoeksbelang dat dringend vordert;
– als daartoe een voorafgaande schriftelijke[19] machtiging van de rechter-commissaris is gegeven.[20]

Een vordering tot het verstrekken van gezondheidsgegevens kan niet worden gericht aan de verdachte.[21]

B2c. Medmij

De vraag van de Patiëntenfederatie is ingegeven doordat steeds meer mensen laagdrempelig en digitaal beschikken over hun eigen gezondheidsgegevens. Bijvoorbeeld doordat men zelf gegevens verzamelt in stappentellers en gezondheidsapps en door de opkomst van patiëntportalen en PGO's.
Voor PGO's is het MedMij-programma ontwikkeld. In het MedMij-programma, waarin ook de Patiëntenfederatie participeert, is een afsprakenstelsel en een reeks standaarden ontwikkeld die veilige en betrouwbare gegevensuitwisseling tussen zorgverleners en zorggebruikers mogelijk maakt. Een PGO en een zorgaanbiedersysteem dat voldoet aan de strenge eisen van het afsprakenstelsel, krijgt een MedMij-label en kan vervolgens gegevens uitwisselen met andere deelnemers van het stelsel. De zorggebruiker bepaalt welke gegevens hij wil verzamelen, beheren en eventueel delen. Een zorggebruiker weet dan dat de PGO veilig en betrouwbaar is.

Het afsprakenstelsel gaat uit van de wettelijke kaders, zoals de AVG en de Wgbo. Aanvullend op de wettelijke kaders is binnen MedMij in de standaard verwerkingsovereenkomst (tussen zorgaanbieder en het ICT-bedrijf dat gegevens verstuurt naar de PGO-aanbieder) een geheimhoudingsclausule voor het ICT-bedrijf opgenomen.[22] Er is dus sprake van een contractuele geheimhoudingsplicht.[23]
Ook is – aanvullend op de wettelijke kaders – in het afsprakenstelsel een normenkader voor informatiebeveiliging[24] opgenomen, op grond waarvan de PGO-leverancier verplicht is jegens de Stichting MedMij om aan te tonen dat hij voldoet aan de voor hem geldende eisen op het gebied van privacy- en informatiebeveiligingsbeleid evenals het normenkader informatiebeveiliging van het MedMij Afsprakenstelsel. In het normenkader informatiebeveiliging worden naast versleuteling, eisen gesteld aan de authenticatie en autorisatie en classificatie van informatie.

Er is geen verplichting voor PGO-leveranciers om mee te doen met het MedMij afsprakenkader, maar deelname wordt gestimuleerd via financiële prikkels. Alleen leveranciers die MedMij gecertificeerd zijn, komen voor een vergoeding in aanmerking. En daarmee is de PGO voor de gebruiker gratis.

---

[17] Zie artikel 126nd, tweede lid, tweede volzin, Sv. In civiele procedures zal het afstuiten op gewichtige redenen vanwege de vertrouwelijkheid van de opgevraagde gegevens.
[18] Zoals moord en ernstige zedenmisdrijven.
[19] Wanneer sprake is van dringende noodzaak, dan kan de machtiging eerst mondeling worden verleend en later op schrift worden gesteld.
[20] Artikel 126nf Sv.
[21] Artikel 126nf, tweede lid, Sv en artikel 843a Rv.
[22] https://afsprakenstelsel.medmij.nl/display/PUBLIC/Modelverwerkersovereenkomst
[23] Aan de contractuele geheimhoudingsplicht is geen verschoningsrecht gekoppeld.
[24] https://afsprakenstelsel.medmij.nl/display/PUBLIC/Normenkader+informatiebeveiliging

PGO-leveranciers die meedoen met het MedMij afsprakenkader moeten aantonen dat zij zich houden aan afspraken uit het MedMij Afsprakenstelsel. Daarbij kan toetsing plaatsvinden. Er wordt toezicht gehouden op de naleving door een van de deelnemers onafhankelijke partij, die over een proportioneel en effectief sanctie-instrumentarium beschikt.[25] Daarnaast houdt de AP er toezicht op dat PGO-leveranciers voldoen aan de AVG.

C. Waarborgen tegen druk van derden

C1. Uitgangspunt toestemming bij gegevensuitwisseling

Bij de vormgeving van het inzagerecht van medische gegevens staat de wilsuiting van de zorggebruiker voorop. Dit volgt zowel uit de AVG als de Wgbo. Er wordt van uitgegaan dat de zorggebruiker in beginsel voldoende in staat is aan te geven met wie en in hoeverre hij zijn gegevens wil delen.[26] Er bestaat dan ook geen verbod op het vragen om toestemming.

C2. Grenzen in wet- en regelgeving

Een zorggebruiker mag niet onder druk gezet worden om gegevens te delen. De wet- en regelgeving stelt daar grenzen aan.

Hierboven is al gewezen op de waarborgen uit de AVG. Toestemming kan niet worden afgedwongen. De toestemming moet uitdrukkelijke zijn en een vrije, specifieke, geïnformeerde en ondubbelzinnige uiting van de wens van de betrokkene zijn. Betrokkene moet dus goed geïnformeerd zijn en vrij tot een beslissing kunnen komen. Er mogen geen – al dan niet gepercipieerde – negatieve consequenties zijn als geen toestemming wordt gegeven. Bovendien bepaalt de AVG dat niet meer gegevens mogen worden gevraagd dan voor het doel noodzakelijk is (artikel 5 van de AVG). Hierboven is al aangegeven dat de AP toezicht houdt op bepalingen uit de AVG.

Voor een aantal specifieke situaties worden in de wet- en regelgeving aanvullend op de AVG grenzen gesteld. Zo mogen gegevens over de gezondheid van de betrokkene of van zijn of haar bloedverwanten door verzekeraars[27] bijvoorbeeld alleen verwerkt worden onder de voorwaarden van artikel 30, derde lid, onder b, van de UAVG. Verzekeraars mogen enkel gezondheidsgegevens verwerken voor zover de verwerking noodzakelijk is voor de beoordeling van het door de verzekeraar te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt; of voor zover dit noodzakelijk is voor de uitvoering van de verzekeringsovereenkomst dan wel het assisteren bij het beheer en de uitvoering van de verzekeringsovereenkomst. Deze gegevens mogen alleen verwerkt worden door personen die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht (artikel 30, vierde lid, van de UAVG). Verder zijn bijvoorbeeld in de Wet op de medische keuringen specifiek bij keuringen grenzen gesteld aan de medische gegevens die een verzekeraar mag vragen en verwerken.

Zoals hiervoor al aan de orde kwam, kunnen gezondheidsgegevens op grond van het Wetboek van Strafvordering niet zomaar worden gevorderd. Er gelden strenge eisen voor de officier van justitie bij het

---

[25] https://afsprakenstelsel.medmij.nl/display/PUBLIC/Principes

[26] Hierbij wordt uitgegaan van wilsbekwame patiënt van 16 jaar of ouder.

[27] Als bedoeld in artikel 1:1 van de Wet op het financieel toezicht of financiële dienstverleners die bemiddelen in verzekeringen als bedoeld in artikel 1:1 van die wet

vorderen van dit soort gegevens (hoog verdenkingscriterium, proportionaliteit en subsidiariteit en een voorafgaande machtiging van de rechter-commissaris). Uit de strafvorderlijke regeling volgt dat gebruik moet worden gemaakt van de vorderingsbevoegdheden en dat het de opsporing in beginsel niet is toegestaan om te verzoeken om op vrijwillige basis gegevens die onder het regime van de AVG vallen te verstrekken. Personen aan wie een verschoningsrecht toekomt, mogen weigeren aan de vordering te voldoen.[28] Dat geldt ook voor personen aan wie een afgeleid verschoningsrecht toekomt, waaronder de patiënt wiens gegevens het betreft, voor zover deze het door het verschoningsrecht beschermde vertrouwelijke verkeer tussen verschoningsgerechtigde en zijn patiënt betreffen. Een vordering mag niet worden gericht aan een verdachte.[29]

D. Technische waarborgen

De Patiëntenfederatie stelt voor technische eisen in de wet op te leggen. De AVG stelt echter al technische eisen aan het verwerken aan gegevens. De AVG verplicht zoals gezegd onder meer dat bij het inrichten van verwerkingen rekening moet worden gehouden met het principe van privacy door ontwerp en standaardinstellingen (*privacy by design & default)* en passende maatregelen moeten worden getroffen met het oog op de bescherming van persoonsgegevens. Voor PGO's binnen het MedMij-afsprakenkader geldt bovendien – aanvullend op de AVG – een normenkader voor informatiebeveiliging. In het normenkader informatiebeveiliging worden naast versleuteling, ook eisen gesteld aan de authenticatie en autorisatie en classificatie van informatie. Een regeling die nadere technische eisen stelt is daarom niet noodzakelijk.

[28] Zie artikel 126nf, derde lid, jo. artikel 96a Sv.
[29] Zie artikel 126nf, derde lid, Sv.