Rapport

MedMij

Grip op je eigen gezondheidsgegevens

Consultatiedocument voor juridische afspraken MedMij

Auteur Theo Hooghiemstra
Versie Def-2016
Datum 16 december 2016

Dit consultatiedocument is het vertrekpunt voor de consultatie over juridische afspraken die deel worden van het MedMij-afsprakenstelsel.

MedMij

Grip op je eigen gezondheidsgegevens

Inhoudsopgave

Inhoudsopgave **2**

1. Inleiding: Meer regie over gezondheid **4**

2. Belangrijkste begrippen **6**

3. Rollen, scenario's, push en pull **11**
3.1. Rollen 11
3.2. Scenario's 11
3.3. Push en Pull 12

4. Huidige en komende juridische kader **13**
4.1. Huidige juridisch kader 13
4.2. Komend juridisch kader 14

5. Thema's **17**
5.1. Zeggenschap, regie en toegang 17
5.1.1. Zeggenschap in plaats van eigendom 17
5.1.2. Verantwoordelijke 17
5.1.3. Individuele persoon als verantwoordelijke? 17
5.1.4. Bewerker (verwerker in de AVG) 18
5.1.5. Zeggenschapsscenario's in de praktijk 19
5.2. Dossier 19
5.2.1. Inleiding 19
5.2.2. Scenario's voor het dossier 20
5.3. Toestemming 20
5.3.1. Inleiding 20
5.3.2. Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (cliëntenrechten bij elektronische uitwisseling van gegeven) 20
5.3.3. Toestemming op grond van de Wbp / AVG in de praktijk van persoonlijke gezondheidsomgevingen bij zorgaanbieders 21
5.3.4. Geen toestemming nodig voor rechtstreeks bij de behandeling betrokkenen 21
5.4. Vertrouwensketen: identificatie, authenticatie, autorisatie (incl. eID-stelsel) 22
5.4.1. Identificatie 22
5.4.2. Authenticatie 23
5.4.3. Autorisatie 24
5.5. Aansprakelijkheid 24
5.5.1. Aansprakelijkheidsvragen algemeen 24
5.5.2. Aansprakelijkheidsvragen hosting providers 25
5.6. Vertegenwoordiging 26
5.7. Medische apps 26
5.8. Inrichting & governance, Toezicht & handhaving 27
5.9. ACM Juridische vraagstukken om nader te regelen in het afsprakenstelsel 27
5.10. Specifieke juridische vraagstukken 27
5.10.1. Erfelijkheidsgegevens in een persoonlijke gezondheidsomgeving 27

MedMij

Grip op je eigen
gezondheidsgegevens

MedMij
Grip op je eigen gezondheidsgegevens

1. Inleiding: Meer regie over gezondheid

Het MedMij-programma (voorheen: programma Meer regie over gezondheid) streeft naar het beschikbaar komen van een persoonlijke gezondheidsomgeving voor iedere willekeurige persoon in 2020. De verwachting is dat met de beschikking over en meer regie op de eigen gezondheidsgegevens er meer mogelijkheden zijn om regie te voeren over de eigen gezondheid. De persoon gebruikt hiervoor zelf gekozen functionaliteit die met behulp van deze gegevens die gewenste regiemogelijkheden biedt, geheel afgestemd op de situatie van de persoon. Het afsprakenstelsel MedMij is erop gericht de persoon te kunnen laten beschikken over gegevens die elders over hem/ haar zijn vastgelegd, dan wel zelf vastgelegde gegevens te kunnen delen met anderen of andere functies. Het afsprakenstelsel is erop gericht de barrières te doorbreken die hierbij spelen tegen de randvoorwaarden die daarvoor gelden.

De persoonlijke gezondheidsomgeving
In het stuk hanteren we de volgende definitie van de persoonlijke gezondheidsomgeving:
Een universeel toegankelijk, voor leken begrijpelijk, gebruiksvriendelijk en levenslang hulpmiddel om relevante gezondheidsinformatie te verzamelen, te beheren en te delen, en om regie te kunnen nemen over gezondheid en zorg en om zelfmanagement te ondersteunen via gestandaardiseerde gegevensverzamelingen voor gezondheidsinformatie en geïntegreerde digitale zorgdiensten.

Een persoonlijke gezondheidsomgeving is een digitale omgeving die je in staat stelt om al je relevante gezondheidsgegevens, die verspreid staan opgeslagen bij zorgverleners, zorgaanbieders en overheden, overzichtelijk en veilig in te zien, aan te vullen met zelf gegenereerde gegevens en te delen met wie je dat wilt.

Inhoudelijke functionaliteiten zijn optioneel en zullen per persoon verschillen op basis van persoonlijke behoefte en situatie. Een persoon moet daarbij kunnen kiezen voor één persoonlijke gezondheidsomgeving en niet gedwongen worden meerdere omgevingen bij te houden. Leveranciers van persoonlijke gezondheidsomgevingen maken gebruik van informatie uit achterliggende systemen van zorgaanbieders en kunnen daar functionaliteit aan toevoegen. Ook zullen er aanbieders van losse functionaliteit zijn die via het MedMij-afsprakenstelsel gegevens kunnen uitwisselen.

Grip op je eigen gezondheidsgegevens en toegang tot digitale functionaliteit stellen je in staat op je zelfgekozen manier aan je eigen gezondheid te werken en je zorgproces te laten ondersteunen.

De waarde van het Afsprakenstelsel MedMij voor de gebruiker
Door een persoonlijke gezondheidsomgeving te gebruiken die het MedMij-stempel draagt, kan

een persoon erop vertrouwen, dat deze is aangesloten op het MedMij-afsprakenstelsel en via dit afsprakenstelsel op een veilige manier gegevens kan uitwisselen met zorgaanbieders. Aansluitvoorwaarden borgen dat een persoonlijke gezondheidsomgeving met het MedMij-stempel op een veilige manier omgaat met gegevens.

Een persoonlijke gezondheidsomgeving met het MedMij-stempel is een waarborg voor betrouwbare grip op je gezondheidsgegevens. En dat biedt toegevoegde waarde voor de persoon. MedMij zegt dus iets over Integriteit, validiteit, actualiteit en interoperabiliteit, maar niet over de inhoudelijke functionaliteit. Het gebruik van aanvullende functionaliteit stelt mensen in staat om gezonder te leven en actiever bij te dragen aan een behandeling.

De inrichting van een persoonlijke gezondheidsomgeving zal net zo zijn gepersonaliseerd met aanvullende functionaliteiten als een smartphone dat is met apps. Mensen zullen zelf de functionaliteiten en apps gebruiken en kiezen die zij goed vinden. Op die manier wordt ingespeeld op de behoefte van gebruikers via marktwerking.

De markt van aanvullende functionaliteiten en apps is bovendien een internationale markt, waarbij het niet realistisch is te verwachten, dat deze zich laten sturen door lokale (MedMij) voorschriften. De partijen in het MedMij stelsel lossen dit voor die partijen op. MedMij zegt om deze redenen niets over inhoudelijke functionaliteit en apps.

Het Afsprakenstelsel MedMij
Via het afsprakenstelsel kunnen persoonsgebonden, gevoelige en vertrouwelijke gegevens op een veilige en gebruiksvriendelijke wijze aangeboden worden aan persoonlijke gezondheidsomgevingen en hun personen en uitgewisseld worden met zorgaanbieders.

MedMij streeft naar het realiseren van interoperabiliteit voor het uitwisselen van persoonlijke gezondheidsgegevens tussen patiënten en zorgaanbieders. Hiertoe wordt een afsprakenstelsel overeengekomen, bestaande uit afspraken op juridisch, organisatorisch, financieel, semantisch en technisch gebied, zodat personen en zorgaanbieders op een veilige manier gegevens kunnen uitwisselen. Partijen die deelnemen aan het MedMij-afsprakenstelsel committeren zich aan de afspraken, en kunnen op basis van de reeds overeengekomen afspraken, diensten aanbieden. Deze partijen, deelnemers in het stelsel en daarmee intermediaire partijen, ontzorgen vervolgens de gebruiker en de zorgprofessional door voor hen deze ingewikkelde invulling van eisen te regelen op een eenduidige manier. Het stelsel kan deze rol alleen vervullen mits deze is voorzien van een transparante besturingsstructuur waarin de belangrijkste partijen zijn vertegenwoordigd met een rol voor toezicht en een helder juridisch kader.

In de kern is het streven naar een minimale set van afspraken die nodig zijn om alle partijen voldoende vertrouwen te geven in hetgeen het stelsel hen biedt en tegelijkertijd zoveel mogelijk ruimte te laten voor innovatie in de functionaliteit aan personen.

2. Belangrijkste begrippen

1. Afsprakenstelsel MedMij: minimale set van afspraken op juridisch, organisatorisch, financieel, semantisch en technisch gebied om alle partijen voldoende vertrouwen te geven in hetgeen het stelsel hen biedt. Partijen die deelnemen aan het MedMij-afsprakenstelsel committeren zich aan de afspraken, en kunnen op basis van de reeds overeengekomen afspraken, diensten aanbieden.

2. Het MedMij-netwerk: de infrastructuur dat de gezamenlijke toegangsverleners leveren om gegevens over uit te wisselen conform de afspraken uit het afsprakenstelsel.

3. Persoonlijke gezondheidsomgeving: Een persoonlijke gezondheidsomgeving is een digitale omgeving die je in staat stelt om te beschikken over al je relevante gezondheidsgegevens, die verspreid staan opgeslagen bij zorgverleners, zorgaanbieders en overheden, aan te vullen met zelf gegenereerde gegevens en te delen met wie je dat wilt.

4. Persoon: degene op wie de persoonlijke gezondheidsomgeving betrekking heeft. Synoniem voor: individu, gebruiker, betrokkene, patiënt, cliënt, zorgconsument.

5. Persoonsgegeven: gegeven “betreffende een geïdentificeerde of identificeerbare natuurlijke persoon”. Een persoon is identificeerbaar “indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden” (artikel 1, onder a, Wbp)

6. Gezondheidsgegeven: gegeven betreffende de geestelijke en/of lichamelijke gesteldheid van een persoon (artikel 21 Wbp).

7.Verantwoordelijke (AVG: Verwerkingsverantwoordelijke): de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1, onder d, Wbp)

8. Bewerker: De bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen..(artikel 1, onder e, Wbp)

9. Derde: ieder, niet zijnde de betrokkene, die ten behoeve van de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken (artikel 1, onder g, Wbp)

10. Zorgverlener: een natuurlijke persoon die beroepsmatig zorg verleent (artikel 1 Wggz).

11. Zorgaanbieder een instelling dan wel een solistisch werkende zorgverlener (overeenkomstig de Wet kwaliteit, klachten en geschillen zorg (artikel 1 Wkkgz).

12. Overheden: alle instellingen die het recht hebben om burgers verplichtingen op te leggen en juist rechten toe te kennen, de overheid is onder te verdelen in de rijksoverheid, dat wil zeggen de centrale overheid zoals regering en ministers, en in decentrale overheden zoals provincies, gemeenten en waterschappen.

13. Hosting provider: het leveren van een dienst van de informatiemaatschappij [die] bestaat in de opslag van de door een afnemer van de dienst verstrekte informatie (Art. 14. Lid 1, Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ("Richtlijn inzake elektronische handel"), PbEG nr. L 178 van 17/07/2000: 1-16).

14. Elektronische communicatiedienst: “een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische-communicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt, doch niet de dienst waarbij met behulp van elektronische-communicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd. Hij omvat niet de diensten van de informatiemaatschappij zoals omschreven in artikel 1 van Richtlijn 98/34/EG, die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronische-communicatienetwerken”.

15. Dossier zorgaanbieder: een dossier in met betrekking tot de behandeling van de patiënt. Hij houdt in het dossier aantekening van de gegevens omtrent de gezondheid van de patiënt en de te diens aanzien uitgevoerde verrichtingen en neemt andere stukken, bevattende zodanige gegevens, daarin op, een en ander voor zover dit voor een goede hulpverlening aan hem noodzakelijk is. alle informatie over de patiënt die noodzakelijk is voor de behandeling (artikel 7:454 lid 1 BW):.

16. Anonimiseren: verwisseling van persoonsgegevens in gegevens die niet langer gebruikt kunnen worden om een natuurlijk persoon te identificeren, daarbij in ogenschouw nemende ‘alle middelen die hiervoor redelijkerwijs gebruikt kunnen worden’ door zowel een verantwoordelijke als een derde partij. Een belangrijke factor hierbij is dat de verwerking onomkeerbaar moet zijn. (Artikel 29 Werkgroep, 2014, zie ook overweging 26 bij de AVG: De gegevensbeschermingsbeginselen dienen derhalve niet van toepassing te zijn op anonieme gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is. Deze verordening heeft derhalve geen betrekking op de verwerking van dergelijke anonieme gegevens, onder meer voor statistische of onderzoeksdoeleinden).

17. Toegangsverleners: beheerders van systemen die kunnen zorgen voor de (technische) uitwisseling van gegevens tussen beheerders van persoonlijke gezondheidsomgevingen en zorgaanbieders.

18: Datalek: is niet wettelijk gedefinieerd. Het betreft een inbreuk op de beveiliging (artikel 13 Wbp). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden. De Autoriteit Persoonsgegevens heeft beleidsregels opgesteld in het kader van de meldplicht datalekken in het kader van artikel 34a Wbp.[1]

19. PIA: Een Privacy Impact Assessment (PIA) is een instrument dat helpt bij het identificeren van privacy risico's en levert de handvaten om deze risico's te verkleinen tot een acceptabel niveau. Op grond van de Algemene Verordening Gegevensbescherming worden PIA's verplicht voor processen die 'likely high risk' vormen. Bij gezondheidsgegevens waarop een beroepsgeheim rust zal daarvan snel sprake zijn.

20. Persoonlijke werkaantekening in dossier zorgaanbieder: is bedoeld voor de eigen voorlopige gedachtevorming, van tijdelijke aard en moet na afloop worden vernietigd. Moet ook echt persoonlijk blijven (Zie Handreiking omgaan met medisch gegevens, KNMG, 2016).

21. eIDAS: Europese verordening, van kracht is sinds 1 juli 2016 die gaat over elektronische identificatie en het opbouwen van een Europees vertrouwenstelsel waarbinnen elkaars identificatiemiddelen worden geaccepteerd om toegang te krijgen tot (grensoverschrijdende) overheidsdienstverlening.

Definities in de Algemene Verordening Gegevensbescherming (AVG)

1) „persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

2) „verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

[1] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf

3)„profilering”: 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;

4) „pseudonimisering”: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

5) „bestand”: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

6) „verwerkingsverantwoordelijke”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

7) „verwerker”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

8) „ontvanger”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk 4.5.2016 L 119/33 Publicatieblad van de Europese Unie NL persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;

9) „derde”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;

10) „toestemming” van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een

ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;

11) „inbreuk in verband met persoonsgegevens”: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

12) „genetische gegevens”: persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon;

13) „biometrische gegevens”: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens;

14) „gegevens over gezondheid”: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;

15) „vertegenwoordiger”: een in de Unie gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in verband met hun respectieve verplichtingen krachtens deze verordening;

16) „onderneming”: een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met inbegrip van maatschappen en persoonsvennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen;

3. Rollen, scenario's, push en pull

3.1. Rollen

De volgende juridisch relevante rollen voor persoonlijke gezondheidsomgevingen zijn te onderscheiden:

- Verantwoordelijke
- Bewerker
- Derde
- Aanbieder persoonlijke gezondheidsomgeving

3.2. Scenario's

Binnen het MedMij-afsprakenstelsel zijn er verschillende scenario's voor gegevensverwerking bij persoonlijke gezondheidsomgevingen te onderscheiden:

1. Data blijft bij de bron/zorgaanbieder, recht op inzage door de persoon.

2. Zelf opslaan en bewerken door de persoon is mogelijk in de persoonlijke gezondheidsomgeving.

3. Uitwisseling tussen persoon en zorgaanbieder en zorgaanbieder en persoon.

4. Beschikbaar stellen van gegevens voor secundaire doelen.
Voorbeelden van relevante, te verwachten secundaire doelen waar gegevens uit een persoonlijke gezondheidsomgeving voor ter beschikking kunnen en zullen worden gesteld zijn wetenschappelijk onderzoek, onderwijs, beleid en statistiek.
Daarbij zal tenminste sprake dienen te zijn van pseudonimisering en als het kan zelfs anonimisering (bijvoorbeeld in het geval van het verzamelen van big data voor collectieve doeleinden die niet tot individuen traceerbaar hoeven te zijn, zoals bij big data om epidemieën mee te kunnen voorspellen). De begrippen pseudonimisering en anonimisering zijn opgenomen in de begrippenlijst. Wat betreft pseudonimisering en versleuteling is Werkgroep 29 (waaraan alle Europese toezichthouders gegevensbescherming deelnemen) en de onze eigen Autoriteit Persoonsgegevens van oordeel dat pseudonimisering weliswaar een goede en vaak noodzakelijke beschermingsmaatregel is, maar nog steeds leidt tot persoonsgegevens en daarmee toepasselijkheid van de Wbp en straks de AVG.

Alleen inzien (scenario 1) past niet binnen de definitie van MedMij. Binnen MedMij wordt

uitgegaan dat de persoon de mogelijkheid heeft om te bewerken dan wel te sturen. In de praktijk zullen alle scenario's voorkomen en dus zullen we hier rekening mee moeten houden in het afsprakenstelsel.

Bij elk van deze scenario's is verder het onderscheid van belang tussen fysieke opslag (bijvoorbeeld op een smartphone, zonder kopie naar de provider) of opslag ergens in 'the cloud'.

3.3. Push en Pull

Bij elektronische gegevensuitwisseling kan bovendien een onderscheid worden gemaakt tussen push- en pull-verkeer.[2]

Push-verkeer : Bij push-verkeer ligt het initiatief voor de gegevensuitwisseling bij de verzender. Dat is degene die het dossier in bewaring heeft. Hij verstuurt gericht gegevens naar één of enkele ontvangers. Voorbeelden van push-verkeer zijn Edifactberichten, e-mail en het gebruik van WhatsApp en andere applicaties waarmee berichten en foto's kunnen worden uitgewisseld met derden.

Pull-verkeer: Bij pull-verkeer stelt een zorgaanbieder zijn dossiergegevens beschikbaar voor raadpleging door andere zorgaanbieders (dossierraadplegers). Op voorhand staat niet vast wie uiteindelijk de gegevens zullen raadplegen. Het initiatief voor de daadwerkelijke gegevensuitwisseling ligt bij de dossierraadpleger. Een voorbeeld hiervan is het Landelijk Schakelpunt (LSP).

Potentieel zijn voor elk van de scenario's - en per scenario het onderscheid tussen fysieke opslag en opslag in de cloud - en afhankelijk van push- of pull-verkeer, afzonderlijke juridische afspraken noodzakelijk, afhankelijk van de architectuur die ontwikkeld wordt.

[2] Zie KNMG Richtlijn omgaan met medische gegevens (2016)

4. Huidige en komende juridische kader

Als algemeen kader voor de verwerking van persoonsgegevens bij persoonlijke gezondheidsomgevingen hanteren we de Wet bescherming persoonsgegevens (Wbp). Vanaf 25 mei 2018 zal de Algemene Verordening Gegevensbescherming (AVG) van toepassing zijn. Dan worden de Wbp en de Richtlijn bescherming persoonsgegevens (Richtlijn 95/46/EG) ingetrokken. Naast de AVG zal ook een nieuwe uitvoeringswetgeving van toepassing zijn. Daarnaast is 4 oktober 2016 de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (cliëntenrechten elektronische gegevens) aangenomen. Zodra deze wet inwerking treedt is er een overgangsperiode van 3 jaar om de elektronische inzage en de gespecificeerde toestemming uit deze wet in de praktijk te regelen.

4.1. Huidige juridisch kader

Wbp

Op dit moment dient de verantwoordelijke voor een persoonlijke gezondheidsomgeving niet alleen het doel van de gegevensverwerking vast te stellen en te specificeren, maar ook een rechtmatige grondslag voor de gegevensverwerking te hebben. De wet kent een limitatief aantal grondslagen. Op grond van de Wbp dienen de volgende toetsen te worden doorlopen om de rechtmatigheid van een gegevensverwerking te beoordelen:

(i) er dient sprake te zijn van een uitdrukkelijk omschreven en rechtmatig doel (*doelspecificatie*)
(ii) er mogen niet meer gegevens worden verzameld (en langer worden bewaard) dan nodig voor dat doel (*data minimalisatie*);
(iii) er dient sprake te zijn van een *grondslag voor de verwerking* (zie hierna)
(iv) voor *bijzondere persoonsgegevens, zoals gezondheidsgegevens*: dient een specifieke grondslag voor verwerking
te bestaan; en
(v) de verdere verwerking van de gegevens mag niet onverenigbaar zijn met het oorspronkelijke doel van verzameling (*verenigbaar gebruik)*.

Ad (iii**)** – *grondslag* voor de verwerking.
De Wbp kent – limitatief – de volgende grondslagen (waarvan de **vetgedrukte** primair relevant zijn voor een persoonlijke gezondheidsomgeving):

a. toestemming betrokkene
b. uitvoering van de overeenkomst
c. nakomen wettelijke verplichting
d. vitaal belang betrokkene

e. goede vervulling publiekrechtelijke taak
f. behartigen *gerechtvaardigd belang*

Wat betreft de begrippen van de Wbp, zie de in de begrippenlijst. Relevante begrippen voor persoonlijke gezondheidsomgevingen zijn onder andere ‘persoonsgegeven’, ‘gezondheidsgegeven’, ‘verantwoordelijke’ en bewerker.

In beginselen samengevat gaat het bij de Wbp om:

1) Transparantie;
2) Doelbinding (noodzakelijkheidsbeginsel)
3) Beveiliging
4) Dataminimalisatie (proporionaliteitsbeginsel)
5) Rechten van betrokkenen (inzage, correctie, verwijdering. Aanvullend vanuit de Wgbo onder andere ook: vernietiging, aanvulling)

Wgbo en overige gezondheidsrechtelijke wetten

In de Wgbo, diverse gezondheidsrechtelijke wetten en professionele standaarden zoals de Richtlijn omgaan met medische gegevens van de KNMG staat op welke wijze zorgaanbieders met inachtneming van hun medisch beroepsgeheim (o.a. artikel 7:457 BW), medische gegevens mogen verwerken. De Wgbo is een behandelingsovereenkomst tussen een zorgaanbieder en een persoon en vastgelegd in het Burgerlijk Wetboek. Het is vooral een patiëntenrechtenwet, waarin onder andere het recht op inzage, vernietiging, aanvulling, niet weten en medisch beroepsgeheim zijn geregeld.

Daarnaast is ook de kwaliteit van zorg ten dele in de Wgbo in relatie tot andere wetten en professionele standaarden geregeld. Zo kent de Wgbo een bepaling over ‘Goed hulpverlenerschap’ gericht op de kwaliteit van de zorgverlening. Overigens zijn er naast de Wgbo ook andere wetten die betrekking hebben op de kwaliteit van zorg zoals de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) en de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG). Daarnaast hebben de beroepsgroepen diverse kwaliteitsrichtlijnen opgesteld, waaronder het KNMG Kwaliteitskader medische zorg ‘Staan voor kwaliteit’(april 2012).

4.2. Komend juridisch kader

AVG

Voor persoonlijke gezondheidsomgevingen bevat de AVG onder andere de volgende relevante aanvullingen op de Wbp:

- Verantwoordingsplicht (accountability: documenteren en implementeren: kunnen laten zien dat AVG wordt nageleefd);

- Extra rechten (vergeetrecht, dataportabiliteit,…);

- Privacy by design en default;

Privacy by Design houdt in dat privacy één van de ontwerpeisen is door passende technische en organisatorische beschermingsmaatregelen te nemen. Mogelijke technische maatregelen:
1. Beperk gegevensverwerking (dataminimalisatie);
2. Bewaar gegevens gescheiden;
3. Abstraheer datgene wat je nodig hebt/relevant is voor het doel dat je met de gegevens wil bereiken;
4.Bescherm de gegevens die je beheert.

Mogelijke organisatorische maatregelen
1.Informeer begrijpelijk;
2.Geef controle aan de betrokkene;
3. Maak een privacybeleid en zorg ervoor dat dit intern wordt nageleefd.
4.Toon aan dat je persoonsgegevens op een privacyvriendelijke manier verwerkt. Uit de AVG volgt namelijk dat je als organisatie verantwoordelijk bent voor de naleving van deze beginselen en dat je deze moet kunnen aantonen (de 'verantwoordingsplicht').

- Privacy Impact Assessment (PIA);

- Hogere boetes.

Het begrip 'bewerker' wordt in de AVG 'verwerker' genoemd.

Voor de verwerker in de AVG gelden ten opzichte van de bewerker in de Wbp de volgende aanvullende specifieke verplichtingen:

•Bewerkers worden verplicht een overzicht bij te houden van alle categorieën persoonsgegevens die zij verwerken in opdracht van een verantwoordelijke;
•Bewerkers mogen niet langer nieuwe sub-bewerkers inschakelen zonder toestemming van de verantwoordelijke;
•Bewerkers moeten de verantwoordelijke onverwijld op de hoogte stellen van een datalek. De termijn voor 'onverwijld' moet nog worden vastgesteld; in Nederlandse wetgeving is deze termijn met de introductie van de Wet Meldplicht datalekken door de Autoriteit Persoonsgegevens (AP) vastgesteld op 72 uur na ontdekking van het incident. Of deze termijn wordt aangehouden is onduidelijk;
•Bewerkers zijn verplicht medewerking te verlenen bij een verzoek daartoe van de toezichthouder (in Nederland de AP) in het kader van de uitoefening van diens taken;
•In bepaalde gevallen moet de bewerker, voorafgaand aan de verwerking van persoonsgegevens, de AP consulteren omtrent de effectieve bescherming van de rechten en vrijheden van betrokkenen of een Privacy Impact Assessment uitvoeren;

•Bewerkers dienen in bepaalde gevallen zelf een privacy officer (of data officer) aan te stellen. Dit is bijvoorbeeld het geval wanneer de bewerker een publieke organisatie is, bij de verwerking sprake is van op grote schaal reguliere en systematische monitoring van betrokkenen of wanneer de primaire activiteiten van de verwerking bestaan uit het op grote schaal verwerken van bijzondere persoonsgegevens.

Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (cliëntenrechten elektronische gegevens)

Het wetsvoorstel cliëntenrechten bij elektronische gegevensuitwisseling in de zorg is 4 oktober jl. door de Eerste Kamer aangenomen en dient na de inwerkingtreding op 1 juli 2017 overeenkomstig artikel 25 van die wet te worden aangehaald als Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Deze wet is een aanvulling op onder andere de Wbp/AVG, de Wgbo, de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet. Door deze wet kan de patiënt 3 jaar na de inwerkingtreding zelf bepalen wie zijn medisch dossier kan inzien. In het rapport Patiëntauthenticatie van PrivacyCare en PBLQ, dat voor de Minister van VWS onder andere ten behoeve van deze wet is geschreven, staat dat voor patiëntauthenticatie minimaal niveau ‘substantieel’ en voor veel situaties betrouwbaarheidsniveau ‘hoog’ (eIDAS) is vereist. Niveau ‘hoog’ is vereist indien er sprake is van een combinatie van het verwerken van gezondheidsgegevens, het BSN en het medisch beroepsgeheim. De minister en de Kamerleden hebben tijdens de behandeling van deze wet aangegeven dat het daarbij belangrijk is dat de burger beschikt over veilige authenticatiemiddelen op voldoende hoog betrouwbaarheidsniveau waarmee hij zijn gegevens in kan zien en opslaan. Daarom laat zij de bepalingen ten aanzien van elektronische inzage en elektronisch afschrift pas in werking treden op het moment dat een authenticatiemiddel op hoog niveau beschikbaar is voor veilige elektronische inzage en afschrift.

Voor wat betreft toestemming bevat deze wet de bepaling dat voor beschikbaarstelling van gegevens via een elektronisch uitwisselingssysteem de zorgaanbieder de voorafgaande toestemming van de betreffende cliënt behoeft (art. 15a lid 1). Hij dient voorts een registratie bij te houden van de door cliënten verleende toestemming waarbij wordt aangetekend vanaf welk moment de toestemming van kracht is geworden. Bij dit alles gaat het om zogenaamde ‘gespecificeerde toestemming’, dat wil zeggen toestemming voor het beschikbaar stellen van alle of bepaalde gegevens aan bepaalde door de cliënt aan te duiden zorgaanbieders of categorieën van zorgaanbieders (art. 15a lid 2). In deze benadering zijn alle (categorieën van) zorgaanbieders die de persoon niet expliciet heeft benoemd automatisch uitgesloten om zijn gegevens die beschikbaar zijn gesteld in een elektronisch uitwisselingssysteem, te raadplegen.

5. Thema's

5.1. Zeggenschap, regie en toegang

5.1.1. Zeggenschap in plaats van eigendom

In het dagelijks taalgebruik en met name ook in de wereld van ICT, project- en programmamanagement is het gebruikelijk om te spreken over 'eigendom'. Juridisch gezien is 'eigendom van persoonsgegevens' echter onbruikbaar. Persoonsgegevens in de zin van de Wet bescherming persoonsgegevens (Wbp) en straks de AVG zijn alle gegevens "betreffende een geïdentificeerde of identificeerbare natuurlijke persoon". Een persoon is identificeerbaar "indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden". Eigendom is volgens artikel 5:1 lid 1 Burgerlijk Wetboek (BW) "het meest omvattende recht dat een persoon op een zaak kan hebben". Persoonsgegevens zijn deelbaar en kunnen op meerdere plekken tegelijk zijn. Beter is om bij persoonsgegevens uit te gaan van 'zeggenschap of regie over persoonsgegevens', waarbij er een verantwoordelijke is met plichten en een persoon met rechten.

5.1.2. Verantwoordelijke

Juridisch gezien is de centrale vraag bij een persoonlijke gezondheidsomgeving: Wie is verantwoordelijke in de zin van de Wbp en straks (vanaf mei 2018) in de zin van de Algemene Verordening Gegevensbescherming (AVG)? Zie de begrippenlijst voor de definitie.

Wanneer een partij verantwoordelijke is voor een persoonlijke gezondheidsomgeving, dan heeft deze tenminste de volgende plichten:
- rechtmatige grondslag (wet of toestemming)
- beveiligingsplicht (zie ook bij patiëntauthenticatie en normen informatiebeveiliging)
- informatieplicht richting de patiënt over de gegevensverwerking
- het bepalen van een bewaartermijn
- een geheimhoudingsverklaring laten tekenen door medewerkers

5.1.3. Individuele persoon als verantwoordelijke?

Heeft een individuele persoon werkelijk de macht over 'diens' gegevens in de persoonlijke gezondheidsomgeving? Hoe verhoudt zich die macht tot de macht van de aanbieder/leverancier? Wat zijn de plichten van de verantwoordelijke & (sub)bewerker en wat zijn de rechten van persoon/consument. Wordt een persoon voldoende beschermd tegen macht partijen (publiek/privaat)?

Ogenschijnlijk lijkt het dat een persoon zelf de volledige macht heeft 'zijn' persoonlijke gezondheidsomgeving. Vanuit juridisch perspectief draait het om de misschien een beetje wantrouwende vraag of dit ook echt zo is.

Zoals hiervoor is vermeld is de centrale vraag: wie is verantwoordelijke? En stelden we vast dat dit in beginsel niet het persoon dient te zijn, want anders is er geen enkele partij met de plicht jegens hem om diens persoonsgegevens te beschermen. Naast een verantwoordelijke is er vaak een bewerker bij een persoonlijke gezondheidsomgeving. Het is ook mogelijk om “niets” te zijn in de zin van de Wbp indien er feitelijk geen enkele macht over de persoonsgegevens kan worden uitgeoefend, als voorbeeld wordt een huurlijn van een telecomprovider genoemd die zodanig is beveiligd dat de telecomprovider feitelijk geen enkele macht kan uitoefenen over de gegevens die door hem worden doorgegeven.

Een persoon kan niet de doeleinden van de verwerking bepalen bij grote ICT-leveranciers, zoals bijvoorbeeld Microsoft, Apple of Philips. Voor iedere afzonderlijke consument wordt geen maatwerk geboden. Een persoon is bijvoorbeeld ook niet in staat om als verantwoordelijke het beveiligingsbeleid of bewaartermijnen-beleid te bepalen.

De filosofie achter de Wbp (straks AVG) is om een persoon te beschermen tegen de macht van de overheden en bedrijven over hun persoonsgegevens. Als een persoon alle plichten van de verantwoordelijke op zich moet laden en niet meer de rechten heeft die hem in de zin van de Wbp toekomen, dan is hij niet beschermd, moet hij zelf het informatiebeveiligingsbeleid opstellen, bewerkersovereenkomsten sluiten etc. Dat past niet bij de bedoelingen van het wettelijk kader ter bescherming van de betrokkene. De illusie is dat een persoon de volledige macht krijgt over zijn gegevens. Dat is niet zo, hij kan wel meer zeggenschap krijgen. Maar hij staat in ongelijke machtsverhouding ten opzichte van bedrijven, zorgaanbieders en overheden.

Uit eerdere uitspraken van de Registratiekamer en het CBP (voorgangers van de AP) bij webdossiers en apps blijkt dat bovendien de AP meent dat een persoon in beginsel niet de rol van verantwoordelijke in de zin van de Wbp past, in de zin dat hij het doel en middelen van de verwerking werkelijk kan bepalen. Al in 2001 stelde de Registratiekamer ten aanzien van het voorgestelde persoonlijke digitale kluisje (Commissie Snellen): “Naast diverse negatieve effecten voor de privacy is het maar de vraag of de burger baas in eigen kluis blijft. Volgens de Registratiekamer bestaan er geen mogelijkheden om de burger te beschermen tegen druk van derden om zijn gegevens beschikbaar te stellen. Het tegendeel is het geval: hoe meer de digitale kluis wordt geïnstitutionaliseerd, des te groter zal de maatschappelijke druk worden om gegevens af te staan”. Zie ook meer recente zaken zoals: Onderzoek CBP naar het combineren van persoonsgegevens door Google, 25 november 2013 z2013-00194 en de Casus Gezondheidsapp Nike van 10/11/2015.

5.1.4. Bewerker (verwerker in de AVG)

De bewerker is ingevolge artikel 1, onder e, Wbp degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. De bewerker verwerkt derhalve gegevens ten behoeve van de verantwoordelijke, dat wil zeggen overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid. Bepalend voor de afbakening van het begrip is de relatie met de verantwoordelijke voor de gegevensverwerking en de mate van zeggenschap waarmee

de verwerking van persoonsgegevens gepaard gaat.

5.1.5. Zeggenschapsscenario's in de praktijk

In de praktijk van persoonlijke gezondheidsomgevingen zijn er ten aanzien van zeggenschap, regie en toegang' vier scenario's:

1. Data blijft bij de bron/zorgaanbieder, recht op elektronische inzage op inzage door de persoon overeenkomstig de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

2. Zelf opslaan en bewerken door de persoon is mogelijk in de persoonlijke gezondheidsomgeving. Indien de leverancier van een persoonlijke gezondheidsomgeving dit mogelijk maakt, zal deze al gauw verantwoordelijke zijn in de zin van de Wbp/AVG.

3. Uitwisseling tussen persoon en zorgaanbieder en zorgaanbieder en persoon. Het kan daarbij voor de benodigde toestemming door de zorgaanbieder van belang zijn of er sprake is van push of pull.

4. Beschikbaar stellen aan secundaire doelen. In dat geval is minimaal pseudonimisering vereist.

5.2. Dossier van de zorgaanbieder

5.2.1. Inleiding

Een persoonlijke gezondheidsomgeving, zoals gedefinieerd in de inleiding, is juridisch gezien geen dossier dat valt onder de dossierplicht van de zorgaanbieder (artikel 7:454 lid 1 BW, ook wel artikel 454 lid 1 WGBO genoemd). Een persoonlijke gezondheidsomgeving kan in aanvulling op het dossier van de zorgaanbieder vrijwillig worden bijgehouden door de persoon.

Beroeps- en 'persoonlijke gezondheidsomgeving-geheim'

Bij een persoonlijke gezondheidsomgeving geniet de persoon niet de bescherming van het medisch beroepsgeheim, tenzij de persoonlijke gezondheidsomgeving wordt beheerd door een zorgaanbieder.

Mogelijk is het een idee om te bestuderen of er zoiets als een geheim moet komen voor de gegevens in een persoonlijke gezondheidsomgeving om het persoon te beschermen tegen externe druk van derden jegens het persoon om gegevens ter beschikking te stellen aan politie- en opsporingsdiensten, verzekeraars en andere financiële instellingen, ICT-bedrijven en andere al dan niet commerciële partijen die macht – formele, sociale of financiële druk - kunnen uitoefenen om gegevens vanuit een persoonlijke gezondheidsomgeving te bemachtigen. Ook kan in een rechtszaak het persoon tot gegevensverstrekking uit een persoonlijke gezondheidsomgeving worden gedwongen, waar de zorgaanbieder zich op het verschoningsrecht zou kunnen beroepen.

5.2.2. Scenario's voor het dossier

1. Data blijft bij de bron/zorgaanbieder, recht op elektronische inzage op inzage. In dat geval blijft de zorgaanbieder verantwoordelijke voor het dossier.

2. Zelf opslaan en bewerken door de persoon is mogelijk in de persoonlijke gezondheidsomgeving. Indien de leverancier van een persoonlijke gezondheidsomgeving dit mogelijk maakt, zal deze al gauw verantwoordelijke zijn in de zin van de Wbp/AVG.

3. Uitwisseling tussen persoon en zorgaanbieder en zorgaanbieder en persoon. Het kan daarbij voor de benodigde toestemming door de zorgaanbieder van belang zijn of er sprake is van push of pull.

4. Beschikbaar stellen aan secundaire doelen. In dat geval is minimaal pseudonimisering vereist.

5.3. Toestemming

5.3.1. Inleiding

Bij gegevensverwerking in een persoonlijke gezondheidsomgeving is naast de Wbp ook vaak de WGBO van toepassing. Of dat laatste het geval is hangt af van welke gegevens uit welke bronnen worden verwerkt en wie de verantwoordelijke is voor de verwerking.
Op grond van een van deze wetten of beide kan toestemming als grondslag voor gegevensverwerking aan de orde zijn.

De Autoriteit Persoonsgegevens stelt dat toestemming voor uitwisseling van patiëntgegevens noodzakelijk is als de verantwoordelijkheid daarvoor niet meer bij zorgaanbieders (kan) liggen. (artikel 23 Wbp i.p.v. 21 Wbp). Gespecificeerde toestemming bij uitwisselingssystemen geldt tussen zorgaanbieders 3 jaar na de inwerkingtreding van de Wet aanvullende bepalingen verwerking persoonsgegevens.

5.3.2. Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (cliëntenrechten bij elektronische uitwisseling van gegeven)

Voor wat betreft toestemming bevat deze 4 oktober jl. in de Eerste Kamer aangenomen wet de bepaling dat voor beschikbaarstelling van gegevens via een elektronisch uitwisselingssysteem de zorgaanbieder de voorafgaande toestemming van de betreffende cliënt behoeft (art. 15a lid 1). Hij dient voorts een registratie bij te houden van de door cliënten verleende toestemming waarbij wordt aangetekend vanaf welk moment de toestemming van kracht is geworden. Bij dit alles gaat het om zogenaamde 'gespecificeerde toestemming', dat wil zeggen toestemming voor het beschikbaar stellen van alle of bepaalde gegevens aan bepaalde door de cliënt aan te duiden zorgaanbieders of categorieën van zorgaanbieders (art.

15a lid 2). In deze benadering zijn alle (categorieën van) zorgaanbieders die de persoon niet expliciet heeft benoemd automatisch uitgesloten om zijn gegevens die beschikbaar zijn gesteld in een elektronisch uitwisselingssysteem, te raadplegen.[3]

5.3.3. Toestemming op grond van de Wbp / AVG in de praktijk van persoonlijke gezondheidsomgevingen bij zorgaanbieders

Voor het gebruik van functionaliteit(en) van een persoonlijk gezondheidsomgeving gefaciliteerd door zorgaanbieders in de zorgverlening en behandeling is instemming van een patiënt nodig wanneer gegevens uit het zorgdossier worden ontsloten en uitgewisseld met anderen.
Afhankelijk van de situatie gaat het om WGBO toestemming of uitdrukkelijke toestemming conform de Wbp. Dat laatste speelt in elk geval als anderen dan de zorgaanbieder betrokken worden bij de gegevensuitwisseling en -verwerking als verantwoordelijke.

Dat geldt ook voor overige verantwoordelijken (publiek en privaat) voor persoonlijke gezondheidsomgevingen. In deze gevallen moet worden uitgegaan van uitdrukkelijke toestemming.
Voor de praktijk is het niet zo belangrijk om het onderscheid tussen de noodzaak van toestemming of uitdrukkelijke toestemming steeds vast te stellen: het moment van face to face uitgifte van toegangsmiddelen en inloggegevens van een persoonlijke gezondheidsomgeving van een ziekenhuis aan gebruikers leent zich uitstekend voor het vastleggen van toestemming. Zorgaanbieders zullen die toestemming toch willen vastleggen in verband met een zorgvuldige procedure. Aan uitdrukkelijkheid is in die gevallen dan steeds voldaan. Ook kan men binnen de toepassing van de persoonlijke gezondheidsomgeving een patiënt vragen akkoord te gaan met de voorwaarden van het gebruik.

In het geval van een persoonlijke gezondheidsomgeving van een zorgaanbieder moet de patiënt van toereikende informatie worden voorzien om toestemming voor het gebruik van de toepassing te kunnen geven. Die informatie kan via de persoonlijke gezondheidsomgeving of aan de balie worden verstrekt, alvorens tot vastleggen van toestemming en uitgifte van toegangsgegevens over te gaan.[4]

5.3.4. Geen toestemming nodig voor rechtstreeks bij de behandeling betrokkenen

Voor wat betreft de verstrekking van gegevens aan hulpverleners die (ook transmuraal) bij de actuele behandeling betrokken worden, wordt van oudsher aanvaard dat toestemming in elk geval niet noodzakelijk is als de ene hulpverlener (bijvoorbeeld de huisarts) in het kader van een bepaalde ziekte-episode verwijst naar de ander (bijvoorbeeld de medisch specialist).

[3] Zie J.K.M. Gevers, Toestemming van de patiënt bij elektronische gegevensuitwisseling in de ketenzorg, VZVZ en InEen, Den Haag/Utrecht, juni 2016, p.17.

[4] Zie J.A.L. Krabben, Een juridisch kader voor patiëntportalen, NPCF en Nictiz, 28 juni 2013.

Daarnaast heeft al in de jaren '90 van de vorige eeuw de toenmalige Registratiekamer (thans: Autoriteit persoonsgegevens) een aantal factoren genoemd die in dit verband van belang zijn, namelijk:

- is de betreffende samenwerking/gegevensuitwisseling gebruikelijk?;
- zijn er redelijke alternatieven?;
- houdt de oorspronkelijke behandelaar voldoende zeggenschap?;
- zijn privacybeschermende maatregelen getroffen?;
- is de werkwijze kenbaar voor en in het belang van de persoon?;
- is de omvang van de samenwerking voldoende beperkt?

Het komt erop neer dat in deze visie de toestemming van de persoon voor gegevensuitwisseling niet nodig is als de toegang tot gegevens door de andere hulpverleners in het concrete geval gebruikelijk en noodzakelijk is, als er privacybeschermende maatregelen zijn getroffen, en een en ander kenbaar en voldoende overzienbaar is voor de persoon. In de literatuur vindt deze gedachtegang veel steun.[5]

5.4. Vertrouwensketen: identificatie, authenticatie, autorisatie (incl. eID-stelsel)

Wat bedoelen we met Identificatie, Authenticatie en Autorisatie?

1) Identificatie. Aan de hand van welke gegevens (identifiers, vaak persoonsnummers) wordt een persoon geïdentificeerd? Zowel in de communicatie met een persoon als in een communicatie over een persoon;
2) Authenticatie. Hoe wordt langs elektronische weg geverifieerd dat er inderdaad een bepaalde persoon 'aan de poort staat'? Dit gaat dus over accounts, wachtwoorden, sterkere authenticatie aan de hand van kennis en bezit, federatieve authenticatie zodat een persoon slechts op één plaats echt bekend hoeft te zijn en hoeft te worden geauthentiseerd;
3) Autorisatie. Wat mag een bepaalde persoon, hoe worden diens mandaten en rechten geadministreerd en hoe wordt die informatie gebruikt bij het verlenen van toegang tot elektronische diensten?

5.4.1. Identificatie

Vraagstukken rond het gebruik (en logging) van het BSN gebruik door de leverancier van de persoonlijke gezondheidsomgeving en straks ook de intermediaire partijen in het stelsel. Dit zijn private partijen, terwijl het BSN is bedoeld voor het burger-domein.

Mag het BSN worden gebruikt door private aanbieders van persoonlijke gezondheidsomgevingen?

Antwoord: gebruik van het BSN is vastgelegd in een gesloten stelsel. Alleen als in de wet staat dat het BSN mag worden verwerkt, is dit toegestaan. Verantwoordelijken bij de overheid en de

[5] Zie J.K.M. Gevers, Toestemming van de patiënt bij elektronische gegevensuitwisseling in de ketenzorg, VZVZ en InEen, Den Haag/Utrecht, juni 2016, p.13.

zorg, inclusief zorgaanbieders, indicatieorganen en zorgverzekeraars mogen – onder voorwaarden – het BSN verwerken. Daarbuiten niet. Dan mogen alleen bewerkers van verantwoordelijken die het BSN mogen gebruiken, ook in het kader van hun bewerkersrol het BSN verwerken.

5.4.2. Authenticatie

Het Rapport 'Patiëntauthenticatie'bij toegang patiëntgegevens' dat in opdracht van de minister van VWS door PrivacyCare en PBLQ is opgesteld kan bij het authenticatievraagstuk bruikbaar zijn, hoewel de vraagstelling van het rapport niet over persoonlijke gezondheidsomgevingen gaat, maar over gegevens onder verantwoordelijkheid van een zorgaanbieder.

Criteria voor het betrouwbaarheidsniveau van patiëntgegevens zijn volgens het rapport:
1) Is er sprake van gezondheidsgegevens?
2) Is er sprake van een BSN?
3) Is er sprake van het medisch beroepsgeheim?

Bij persoonlijke gezondheidsomgevingen zijn wel vaak gezondheidsgegevens, echter lang niet altijd is sprake van het medisch beroepsgeheim.

Conclusie van het rapport is dat bij gezondheidsgegevens minimaal niveau substantieel (eIDAS, STORK3) en vaak hoog (eIDAS, STORK 4) noodzakelijk is. Overigens kunnen eIDAS en STORK niet één op één met elkaar vergeleken worden, voor het gemak is dat tussen haakjes wel even gedaan. Op dit moment zijn authenticatiemiddelen op betrouwbaarheidsniveau hoog nog niet breed beschikbaar, er zal daarom sprake moeten zijn van een overgangsperiode. Voor de elektronische inzage plicht op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg is daarvoor een periode van 3 jaar uitgetrokken.

De minister heeft bij de brief van 4 november wat betreft de overgangsperiode in antwoord op vragen vanuit de Tweede Kamer als volgt gereageerd op het rapport over patiëntauthenticatie:

"Ik ben blij met de heldere conclusies van het onderzoek van PrivacyCare/PBLQ: voor authenticatiemiddelen die gebruikt worden in de zorg is minimaal niveau substantieel eIDAS nodig en als het gaat om gegevens waarop het medisch beroepsgeheim van de zorgverlener rust is het hoogste betrouwbaarheidsniveau (hoog eIDAS) nodig. Op dit moment zijn authenticatiemiddelen op het voor de zorg gewenste hoge betrouwbaarheidsniveau nog niet op brede schaal beschikbaar. Om die reden wordt de inwerkingtreding van de bepaling over het recht op elektronische inzage uit het wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens met drie jaar uitgesteld. In antwoord op uw vraag hoe de regering omgaat met de aanbevelingen uit het rapport het volgende: de conclusies vormen de leidraad bij de invulling van de eisen waaraan authenticatiemiddelen in de zorg moeten voldoen. Deze eisen worden meegenomen in het kabinetsbrede beleid voor de verdere ontwikkeling van de infrastructuur voor (digitaal) inloggen en identificeren, het programma Impuls eID."

Tevens gaat de minister in deze brief in op het groeimodel voor patiëntauthenticatie:

"Zoals aangegeven in de brief van het kabinet over de Impuls eID is het doel dat vanaf oktober 2018 in principe alle dienstverleners in het BSN-domein in staat zijn op grote schaal de door BZK toegelaten authenticatiemiddelen in hun dienstverlening te gebruiken. De zorgsector en de Belastingdienst gelden als eerste prioriteiten ('de voorlopers'). In overleg met de zorgsector, verenigd in het Informatieberaad, wordt een strategie ontwikkeld om het gebruik van beschikbare authenticatiemiddelen op het betrouwbaarheidsniveau substantieel in de zorg aan te jagen en te faciliteren en op termijn toe te groeien naar patiëntauthenticatie op het hoogste betrouwbaarheidsniveau zodra deze middelen breed beschikbaar komen."

5.4.3. Autorisatie

Met een persoonlijke gezondheidsomgeving toegang geven aan personen en zorgaanbieders (toegangsprofielen) tot de juiste informatie, voor de juiste personen op de juiste tijd en plaats via afschermmogelijkheden moet nader worden uitgewerkt.

5.5. Aansprakelijkheid

5.5.1. Aansprakelijkheidsvragen algemeen

Er zijn aansprakelijkheidsvragen indien een persoonlijke gezondheidsomgeving deel gaat uitmaken van de medische behandelrelatie tussen zorgaanbieder en een persoon.

Vraagstukken in het kader van de aansprakelijkheid.
1) Gegevens in een persoonlijke gezondheidsomgeving kunnen steeds veranderen, terwijl het voor de aansprakelijkheid noodzakelijk is dat de oude gegevens beschikbaar, en veranderingen zichtbaar blijven, en dat wordt vastgelegd door wie op welk moment veranderingen zijn aangebracht.
Dit probleem zou deels via goede logging-software en analyse kunnen worden opgelost.
Ook is het raadzaam in de persoonlijke gezondheidsomgeving een 'time-stamp' op te nemen wanneer data is toegevoegd aan de betreffende persoonlijke gezondheidsomgeving.
Daarnaast dient er ook te worden opgenomen uit welke bron de gegevens afkomstig zijn. Door de gegevens traceerbaar te maken en een 'time-stamp 'toe te voegen kan een zorgaanbieder zelf de inschatting maken om gegevens uit de persoonlijke gezondheidsomgeving wel of niet op te nemen in zijn medische behandeldossier. Bovendien dient aangegeven te worden wat de bron is van de gegevens via metadata, zodat de betrouwbaarheid bepaald kan worden door de zorgaanbieder en/ of persoonlijke gezondheidsomgeving.

2) Een tweede mogelijk aansprakelijkheidsvraagstuk is in hoeverre de zorgaanbieder aansprakelijk kan worden gesteld indien hij de informatie in een persoonlijke gezondheidsomgeving niet of onvolledig betrekt bij zijn behandeling. Is hij daartoe te verplichten? Antwoord: nee, de zorgaanbieder is hiertoe niet te verplichten.

3) Wanneer personen een persoonlijk gezondheidsomgeving hebben dat is verbonden met een elektronisch dossier van hun zorgaanbieder kunnen zij van hun zorgaanbieder gaan verwachten dat hij/zij hun elektronische dossier raadplegen? Antwoord: Nee, het initiatief voor het delen ligt bij de persoon. De zorgaanbieder valt niet te verplichten om de persoonlijke gezondheidsomgeving te raadplegen.

Het zou goed zijn als beroepsorganisaties van zorgaanbieders en de Patiëntenfederatie voor bovenstaande vragen een handreiking kunnen bieden, wellicht in het afsprakenstelsel en via professionele standaarden die op grond van de bepaling over 'Goed hulpverlenerschap' in de Wgbo ook een wettelijke grondslag hebben gericht op de kwaliteit van de zorgverlening. Overigens zijn er naast de Wgbo ook andere wetten die betrekking hebben op de kwaliteit van zorg zoals de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) en de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG). Daarnaast hebben de beroepsgroepen diverse kwaliteitsrichtlijnen opgesteld, waaronder het KNMG Kwaliteitskader medische zorg 'Staan voor kwaliteit'(april 2012).

Bij twijfel over aangeleverde informatie is het raadzaam dat de zorgaanbieder deze twijfel vastlegt bij het opnemen van de informatie in het dossier.

5.5.2. Aansprakelijkheidsvragen toegangsdienstverleners

De AVG kent echter een bepaling waarin staat[6]:
"Deze verordening laat de toepassing van Richtlijn 2000/31/EG, en met name van de regels in de artikelen 12 tot en met 15 van die richtlijn betreffende de aansprakelijkheid van als tussenpersoon optredende dienstverleners onverlet."

Het betreft hier een aantal bijzondere aansprakelijkheidsbepalingen in de richtlijn inzake 'Elektronische handel' die gelden voor de aansprakelijkheid van dienstverleners die als tussenpersoon optreden , zoals bijvoorbeeld 'hosting providers'. Deze bijzondere aansprakelijkheidsbepalingen zijn door de Nederlandse wetgever overgenomen in het Burgerlijk Wetboek. Op grond hiervan moet worden geconcludeerd dat wanneer een dienst van de 'hosting provider' bestaat in de opslag van de door een afnemer van de dienst verstrekte informatie, de 'hosting provider' niet aansprakelijk is voor de op verzoek van de afnemer van de dienst opgeslagen informatie, op voorwaarde dat:

- de 'hosting provider' niet daadwerkelijk kennis heeft van een eventuele onwettige activiteit of informatie en, wanneer het een schadevergoedingsvordering betreft, geen kennis heeft van feiten of omstandigheden waaruit het onwettige karakter van de activiteiten of informatie duidelijk blijkt; of,
- de 'hosting provider', zodra hij van het bovenbedoelde daadwerkelijk kennis heeft of besef krijgt, prompt handelt om de informatie te verwijderen of de toegang daartoe onmogelijk te maken.

[6] Zie bijlage met notitie van Ad van Loon waar deze passage op is gebaseerd.

5.6. Vertegenwoordiging

Bij vertegenwoordiging is er een verschil tussen het ophalen en delen van de gegevens uit naam van iemand anders enerzijds en de situatie waarbij gegevens al in de persoonlijke gezondheidsomgeving zitten en de betreffende persoon ter plekke anderen toegang geeft tot de persoonlijke gezondheidsomgeving.

Wat betreft het ophalen en delen van de gegevens uit naam van iemand anders is het raadzaam aan te sluiten bij de landelijke ontwikkelingen om tot een digitaal vertegenwoordigingsregister te komen. Voor het tweede ligt de verantwoordelijkheid bij de betreffende persoon, al kunnen in de aansluitvoorwaarden voorwaarden worden opgenomen voor de betreffende persoon.

De overheid gebruikt in de praktijk DigiD Machtigen door natuurlijke personen om andere personen te machtigen. Zodat die gemachtigden de natuurlijke persoon in kwestie kan vertegenwoordigen bij de aangesloten overheidsdiensten.
Dit wordt bijvoorbeeld gebruikt bij de Aangifte InkomstenBelasting. Mensen kunnen hiermee andere personen machtigen om namens hun de Aangifte IB te verzorgen.
Bij een persoonlijke gezondheidsomgeving is er zeker ook behoefte aan vertegenwoordigingsrelaties tussen natuurlijke personen. De meest voorkomende behoefte is dat herkend kan worden welke volwassene gaat over een bepaalde persoon, bijvoorbeeld in mantelzorgsituaties. Er bestaan nog geen breed beschikbare mogelijkheden in de zorg om digitale vertegenwoordiging betrouwbaar te regelen.
In de ‘Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg’ komt de verplichte wilsverklaring aan bod.

Een voorbeeld van een persoonlijke gezondheidsomgeving met een vertegenwoordigingsvraagstuk, namelijk mantelzorgers die een persoonlijke gezondheidsomgeving moeten kunnen aanmaken is Carenzorgt: https://www.carenzorgt.nl/welcome.

Overigens hoeft een persoon zichzelf geen toestemming te geven, mits er sprake is van een voldoende hoog authenticatieniveau, zodat met voldoende zekerheid bepaald kan worden dat de persoon ook degene is die hij zegt te zijn.

5.7. Medische apps

1) De Privacy Code of Conduct on mobile health apps

2) De Draft mHealth assessment guidelines.

Beide documenten (concept versies en stand van zaken) zijn te vinden op: https://ec.europa.eu/digital-single-market/en/news/current-initiatives-unlock-potential-mobile-health-europe.

Verder is er de Richtlijn medische hulpmiddelen, de bijbehorende CE-markering en het besluit medische hulpmiddelen mogelijk van belang. De vraag is of een app met een persoonlijke gezondheidsomgeving te kwalificeren is als een medisch hulpmiddel.

Bovendien is ook het (herziene) Convenant medische technologie van de IGZ mogelijk relevant.

5.8. Inrichting & governance, Toezicht & handhaving

Begin 2017 wordt over dit onderwerp onderzoek uitgezet, waarvan de uitkomsten zullen worden besproken in de juridische werkgroep van eind maart.

5.9. Juridische vraagstukken om nader te regelen in het afsprakenstelsel

Diverse juridische vraagstukken zijn voor persoonlijke gezondheidsomgevingen niet of nauwelijks wettelijk geregeld en zullen privaatrechtelijk in het afsprakenstelsel moeten worden uitgewerkt, zoals:

- Financiering (hierover loopt een project bij VWS);
- Interoperabiliteit en standaarden
- Gebruiks- en aansluitvoorwaarden

5.10. Specifieke juridische vraagstukken

5.10.1. Erfelijkheidsgegevens in een persoonlijke gezondheidsomgeving

Erfelijkheidsgegevens vormen een bijzondere situatie. Een essentieel verschil tussen erfelijkheidsgegevens en andere gezondheidsgegevens is dat zij niet uitsluitend betrekking hebben op de gezondheidstoestand van de persoon van wie zij in eerste instantie afkomstig zijn, maar ook op diens familieleden. Erfelijkheidsgegevens hebben per definitie ook betrekking op anderen. Het verwerken van persoonsgegevens over erfelijke eigenschappen is in beginsel alleen toegestaan voor zover de verwerking plaatsvindt voor/met de persoon bij wie de betreffende erfelijkheidsgegevens zijn verkregen. Op dit strikte voorschrift gelden als enige uitzonderingen:

- Een zwaarwegend geneeskundig belang;
- Noodzakelijk ten behoeve van wetenschappelijk onderzoek en statistiek.

Van die uitzonderingsgronden is bij de leveranciers van persoonlijke gezondheidsomgevingen doorgaans geen sprake. Dat betekent dat de erfelijkheidsgegevens zelfs met toestemming van de persoon - behoudens de genoemde uitzonderingen - niet gebruikt mogen worden voor of in relatie tot anderen, zoals familieleden. In die zin is de wetgever paternalistisch, onder andere om te voorkomen dat discriminatie op grond van erfelijkheidsgegevens plaats kan vinden voor bijvoorbeeld verzekeringen. Specifieke wetgeving, zoals de Wet medische keuringen, geeft hieraan nadere invulling. Hetzelfde geldt voor het vaststellen van strafbare feiten aan de hand

van DNA-sporen.
Zelfs als de erfelijkheidsgegevens alleen met betrekking tot de persoon bij wie de erfelijkheidsgegevens zijn verkregen worden verwerkt, dan nog heeft de leverancier van de persoonlijke gezondheidsomgeving de uitdrukkelijke toestemming van de betrokkene nodig.
Een interessante vraag voor de nabije toekomst is in hoeverre dankzij het snel voortschrijdende genetica-onderzoek binnenkort niet vrijwel alle medische gegevens erfelijkheidsgegevens worden.
Als dat het geval is zou het hiervoor beschreven strikte regime van toepassing zijn, hetgeen lastig te handhaven wordt.

Bestudeerde documentatie

#	Documentnaam
	Theo Hooghiemstra en Jacqueline Krabben, presentatie voor eerste juridische expertgroep
	Krabben (Privacycare) en Hooghiemstra (PBLQ), patiëntauthenticatie, voor minister VWS
	RVZ, Patiënteninformatie
	Theo Hooghiemstra, Juridische uitdagen: Persoon aan de macht? In: Bettine Pluut: Wetenschappers over het PGD, 15 november 2012, NPCF
	T.F.M. Hooghiemstra en S.Nouwt, SDU Commentaar, Wet bescherming persoonsgegevens, editie 2016.
	KNMG Richtlijn omgaan met medische gegevens
	KNMG Kwaliteitskader medische zorg 'Staan voor kwaliteit'(april 2012).
	Juridische aspecten eHerkenning
	Juridische aspecten Qiy
	Ad van Loon, : https://www.qiyfoundation.org/personal-data-controllers-and-processors-beware/

Bijlage: document van Ad van Loon

Apart bijgevoegd in Pdf.