Raad voor de Volksgezondheid & Zorg

# Juridische drempels voor toepassing (consumenten) eHealth

Marina de Lint

Achtergrondstudie uitgebracht bij het advies Consumenten-eHealth

Den Haag, 2015

# Inhoudsopgave

# Samenvatting

In het advies over eHealth dat de RVZ momenteel in voorbereiding heeft, staat de opkomst van consumenten-eHealth centraal. Dit is een vorm van eHealth die direct op de consumentenmarkt gericht is en niet op de professionele markt. De producten en diensten vinden hun weg rechtstreeks vanaf de producent naar de consument/patiënt en niet via de 'medische kanalen'. Het gaat onder andere om lifestyle gadgets, apps voor de smartphone, gezondheidsplatforms en ook Persoonlijk Gezondheids Dossiers (PGD's). Een van de hoofdvragen van het advies is welke transformatie in de gezondheidszorg zal plaatsvinden als gevolg van de opkomst van consumenten-eHealth.

Deze vraag is relevant, omdat de ontwikkeling van consumenten-eHealth onstuitbaar is en vroeg of laat om respons vraagt vanuit het professionele zorgdomein. Maar we weten ook dat de implementatie en adaptatie van eHealth door zorgaanbieders moeizaam verloopt. Dit heeft verschillende oorzaken, waaronder belemmeringen die voortvloeien uit wet- en regelgeving (of het ontbreken daarvan).

In deze notitie worden de juridische belemmeringen voor de implementatie en adaptatie van (consumenten)-eHealth in kaart gebracht aan de hand van zeven thema's. Vervolgens worden, daar waar relevant, suggesties gegeven voor oplossingsrichtingen.

**1. Gegevensbescherming**

Voor zorgaanbieders/zorgverleners vormt de wettelijk geregelde privacybescherming (medisch beroepsgeheim en bescherming persoonsgegevens) een voorwaarde waaraan te allen tijde moet worden voldaan. De regels rond het medisch beroepsgeheim en de Wet bescherming persoonsgegevens (Wbp) zijn vooral aan de orde wanneer in contacten tussen zorgverleners persoonsgegevens over patiënten worden uitgewisseld. De hoofdregel is dat een hulpverlener alleen met toestemming van de patiënt informatie over die patiënt aan anderen mag verstrekken. Op die hoofdregel bestaan verschillende uitzonderingen, bijvoorbeeld wanneer verstrekking van gegevens wettelijk verplicht is, wanneer gegevens worden verstrekt aan anderen die rechtstreeks bij de uitvoering van de behandelingsovereenkomst met de patiënt betrokken zijn of in geval van een conflict van plichten. Alleen

wanneer gegevens zonder schending van het beroepsgeheim zijn verkregen komt men toe aan het toetsen van de verwerking van de patiëntgegevens aan de Wbp. Behalve een rechtmatige grondslag (artikel 8) dient ook sprake te zijn van een ontheffing van het verbod op het verwerken van gezondheidsgegevens (artikel 21) of van een uitzondering (artikel 23).

De privacybeschermingsregels gelden ongeacht of er sprake is van conventionele zorg dan wel van eHealth. In geval van eHealth zullen vooral de eisen uit de Wbp navranter aan de orde zijn, door de veel ruimere mogelijkheden tot electronische gegevensuitwisseling.

In beginsel is zowel in nationaal als in Europees verband de bescherming van persoonsgegevens toereikend geregeld. Consumenten en patiënten hebben in dit opzicht houvast in de vorm van de Wet Bescherming Persoonsgegevens en de Wet op de Geneeskundige Behandelingsovereenkomst. Consumenten moeten zich realiseren dat dit niet het geval is wanneer zij zich via het internet buiten Europa begeven en persoonsgegevens verstrekken.

Momenteel wordt de Europese dataprotectierichtlijn herzien en (waarschijnlijk) omgezet in een Verordening. Deze Verordening voorziet ook in een oplossing voor dit probleem: zij bepaalt namelijk dat voor doorgifte van Europese persoonsgegevens aan buitenlandse overheden toestemming is vereist van een toezichthoudende autoriteit (No-NSA clause). Andere belangrijke punten in de voorgestelde Verordening zijn: een verplichting voor de verantwoordelijke en mogelijk de bewerker tot het uitvoeren van risicoanalyses bij de verwerking van de persoonsgegevens; het melden van datalekken binnen 72 uur aan de toezichthoudende autoriteit; en het recht van betrokkenen om te eisen dat alle persoonsgegevens van hem of haar worden gewist (right to erasure).

Aanvankelijk was het de ambitie om voor de verkiezingen in het Europees Parlement, in mei 2014, een definitief akkoord te hebben over de Verordening. Dit is niet gelukt. Op dit moment is niet bekend wanneer de nieuwe Verordening zal kunnen worden vastgesteld.

*Oplossingsrichtingen*
Indien de voortgang in de totstandkoming van de Verordening uitblijft biedt het Nederlandse EU-voorzitterschap in 2016 een

goede gelegenheid om dit onderwerp prominenter op de agenda te krijgen.

Daarbij kan expliciet in de overwegingen worden betrokken of een wettelijk geregeld 'patiëntgeheim' een goede aanvulling is op de waarborgen voor patiënten die de nieuwe Verordening in zich draagt. De RVZ heeft in zijn advies Patiënteninformatie reeds ervoor gepleit om in aanvulling op het medisch beroepsgeheim voor het PGD een 'patiëntgeheim' in het leven te roepen. Dit beschermt de patiënt tegen de oneigenlijke invloed van politie- en opsporingsdiensten, schade- en levensverzekeraars, financiële instellingen, ICT-bedrijven en andere, al dan niet commerciële partijen die macht kunnen uitoefenen om toegang te krijgen tot de inhoud van het PGD.

## 2. Zeggenschap over medische gegevens

Op grond van de WGBO is de hulpverlener verplicht een dossier bij te houden over de patiënt waarmee hij een behandelingsovereenkomst heeft. De patiënt heeft het recht om zijn dossier in te zien en om (evtueel tegen geringe vergoeding) afschrift te vragen van (delen van) het dossier. Er is een voornemen om in de Wet cliëntenrechten zorg (Wcz) een recht van de patiënt op elektronische toegang tot en afschrift van het medisch dossier op te nemen.

De zeggenschap over medische gegevens die zijn opgenomen in het door de hulpverlener aangelegde medische dossier behoort volgens de RVZ bij de betreffende patiënt te liggen. De Raad heeft meerdere malen bepleit dat de patiënt/burger kan beschikken over al zijn gezondheidsgegevens als hij dat kan en wil, uiteindelijk in de vorm van een levenslang persoonlijk gezondheidsdossier (PGD). Dit biedt mogelijkheden om het medische dossier te integreren in het PGD van de patiënt. Daarvoor moet wel geregeld zijn dat de zorgaanbieder verplicht is gegevens uit het medische dossier aan de patiënt te leveren.

Het wetsvoorstel met regels voor elektronische patiëntendossiers (nummer 33 509) voorziet hierin. Het bepaalt dat 'indien de cliënt verzoekt om inzage of afschrift van het dossier van de desbetreffende cliënt, of van de gegevens betreffende deze cliënt die de zorgaanbieder via een elektronisch uitwisselingssysteem beschikbaar stelt, wordt de inzage of het afschrift op verzoek van de cliënt, met redelijke tussenpozen, door

de zorgaanbieder op elektronische wijze verstrekt.'(artikel 15d eerste lid).

### 3. Technische standaarden en infrastructuur

Regelingen die voorzien in de toepassing van uniforme technische standaarden ontbreken, zowel op nationaal als op Europees niveau. Dit houdt in dat eenieder die e-Health-toepassingen aanbiedt, zelf bepaalt welke 'standaarden' gebruikt worden. Dit heeft tot gevolg dat systemen niet op elkaar aansluiten c.q. gegevens niet geautomatiseerd kunnen worden uitgewisseld. Dit leidt tot fragmentatie, inefficiëntie, fouten, onnodig dubbel onderzoek, enz. Dit gegeven vormt een fors obstakel voor eHealth, zowel vanuit het perspectief van de zorgverlener als van de patiënt.

Het ontwikkelen van standaarden (interoperabiliteit) wordt momenteel opgepakt door de Europese Commissie (actieplan eHealth 2014-2020).

### 4. Standaarden van zorg

Zorgverleners dienen te behandelen overeenkomstig hetgeen onder beroepsgenoten gebruikelijk is (de professionele standaard). Deze standaard is onder meer vastgelegd in protocollen en richtlijnen. In beginsel geldt het uitgangspunt: wat offline geldt, geldt ook online. Er zijn nog weinig specifieke standaarden ontwikkeld voor het toepassen van eHealth. Tot op heden is volgens de standaard eHealth alleen toegestaan in het kader van een reeds bestaande behandelrelatie.

### 5. Aansprakelijkheid

De relatie tussen zorgverlener en patiënt wordt in het Nederlands recht beheerst door de Wet op de Geneeskundige Behandelingsovereenkomst. Op grond van deze wet is de zorgverlener verantwoordelijk en aansprakelijk voor al hetgeen in het kader van deze behandelingsovereenkomst plaatsvindt. Deze volledige aansprakelijkheid impliceert dat de zorgverlener (ook) verantwoordelijk en aansprakelijk is voor het handelen van personen die bij de uitvoering van de behandelingsovereenkomst zijn betrokken (zogenoemde hulppersonen) en voor de hulpmiddelen die worden ingezet. Het is om deze reden dat een van de gedragsregels voor artsen is dat eHealth-contacten uitsluitend kunnen plaatsvinden binnen het kader van een reeds bestaande

behandelovereenkomst. Wil de zorgverlener verantwoordelijk en aansprakelijk kunnen zijn voor hulpmiddelen, zoals eHealth-applicaties, dan moet hij de kwaliteit en betrouwbaarheid ervan immers kunnen kennen en kunnen beoordelen.

Hoewel deze uitgebreide (en niet uit te sluiten) aansprakelijkheid de zorgvrager in de Nederlandse situatie een hoog beschermingsniveau biedt vormt het tegelijkertijd een obstakel voor de verdere implementatie van eHealth. De ontwikkeling van consumer driven eHealth brengt met zich mee dat zorgverleners steeds vaker geconfronteerd worden met 'ad hoc' vragen om advies, zonder dat (reeds) sprake is van een behandelingsovereenkomst. Hierbij wordt de zorgverlener geconfronteerd met gegevens die de zorgvrager zelf heeft gegenereerd met behulp van een door hem aangeschaft electronisch hulpmiddel. Omdat het geven van raad of advies onder de reikwijdte van de WGBO valt, zal de zorgverlener, teneinde te kunnen voldoen aan de verplichtingen die deze wet stelt, geneigd zijn 'van voren af te beginnen', onderzoek te herhalen etc. De zorgvrager zal hierdoor geneigd zijn zijn heil elders te zoeken. Commerciële (buitenlandse) aanbieders springen hierop in. Zo heeft bijvoorbeeld Google het voornemen om medische apps en andere eHealth-diensten op de markt te zetten, met in de backoffice door hen gecontracteerde artsen, die bijpassende adviezen kunnen geven. Deze commerciële aanbieders zullen veelal elke vorm van aansprakelijkheid uitsluiten. Bovendien is er geen garantie dat de artsen die zij achter de hand hebben bevoegd en bekwaam zijn.

Als we in Nederland geen passende aansluiting vinden op deze ontwikkeling missen we niet alleen de boot, maar zijn zorgvragers ook aanzienlijk minder goed beschermd dan mogelijk is.

*Oplossingsrichting: overeenkomst van geneeskundig advies*
Een oplossingsrichting voor dit probleem is het ontwerpen van een lichtere variant op de geneeskundige behandelingsovereenkomst voor eHealth-diensten, met een bijbehorend lichter aansprakelijkheidsregime; een 'overeenkomst van geneeskundig advies'. Dit moet het mogelijk maken dat de zorgverlener op basis van door de zorgvrager aangeleverd (onderzoeks)materiaal kan inspelen op diens ad hoc en/of incidentele adviesvragen, zonder verantwoordelijk te zijn voor het (onderzoeks)materiaal en de hulpmiddelen die gebruikt zijn om dat te verkrijgen.

Uiteraard moet voor zorgvragers te allen tijde duidelijk zijn of de overeenkomst die zij met een zorgverlener aangaan een ge-

neeskundige behandelingsovereenkomst is (waarvoor laatstgenoemde volledig aansprakelijk is) dan wel een 'overeenkomst van geneeskundig advies' (waarvoor de zorgverlener beperkt aansprakelijk is). Dit kan bereikt worden door zorgverleners te verplichten bij het ingaan op een advies(aan)vraag de aansprakelijkheidsclausule kenbaar te maken (vgl. verplichting voor opdrachtgevers en – nemers om algemene voorwaarden kenbaar te maken).

Om te voorkomen dat door de introductie van een lichtere variant naast de bestaande geneeskundige behandelingsovereenkomst het beschermingsniveau van zorgvragers afneemt, zijn voorts aanvullende maatregelen nodig: zie onder punt 6 en 7.

## 6. Jurisdictie en rechtsmachtconflicten

In geval van grensoverschrijdende geschillen in relatie tot de toepassing van eHealth is zowel voor patiënten als voor zorgverleners onvoldoende duidelijk welk recht van toepassing is. Wanneer bijvoorbeeld een arts in het buitenland gevestigd is, kan deze als voorwaarde voor de dienstverlening bepalen dat de overeenkomst onderworpen is aan het recht van het land waarin hij, de arts, gevestigd is. Dat kan ten nadele van de zorgvrager zijn, wanneer het beschermingsniveau van zorgvragers in het land waarin de dienstverlener (in casu de arts) gevestigd is lager is dan in Nederland. Binnen de EU is dit probleem opgelost met het *Verdrag inzake het recht dat van toepassing is op verbintenissen uit overeenkomst (Verdrag 80/934/EEG.* Op grond van dit verdrag kan de zorgvrager/patiënt dwingende bepalingen die te zijner bescherming zijn opgenomen in het recht van het land waar hij zijn gewone verblijfplaats heeft inroepen. Dit betekent dat de consument/patiënt een beroep kan doen op de rechten die voor hem voortvloeien uit de WGBO. Het betekent ook dat de arts, zelfs wanneer hij in het buitenland is gevestigd, aansprakelijkheid voor een tekortkoming zijnerzijds niet kan uitsluiten of beperken.

Vanuit de zorgvrager bezien is een probleem dat de reikwijdte van dit verdrag begrensd is tot de lidstaten van de EU. Wanneer zorgvragers eHealth-diensten betrekken van daarbuiten gevestigde aanbieders is onduidelijk welk recht (en dus welk beschermingsniveau) van toepassing is op de overeenkomst.

*Oplossingsrichting: uitbreiding reikwijdte verdrag inzake rechtsmacht (ad 6):*

Dit onderwerp zou geagendeerd kunnen worden voor het Nederlandse EU-voorzitterschap; onderzocht dient te worden of het openstellen van dit verdrag voor bredere (wereldwijde?) ratificering een reële mogelijkheid is.

## 7. Gebruik van electronische hulpmiddelen

Als de zorgverlener in geval van een overeenkomst van geneeskundig advies (zie onder punt 5) niet aansprakelijk is voor gebreken in de gebruikte hulpmiddelen, is het temeer van belang dat de fabrikanten daarvan wel aangesproken kunnen worden voor gebreken. Momenteel geldt dat als een medische app gebruikt wordt voor diagnostiek of therapie het volgens de wet een medisch hulpmiddel is. In dat geval is de Richtlijn Medische Hulpmiddelen (RMH) van toepassing en is een CE-markering verplicht. De meeste medische apps vallen vooralsnog in de minst strenge risicoklasse van de registratie. Dit betekent dat het bedrijf dat de app op de markt brengt, hem zelf mag certificeren door het maken en bijhouden van een technisch dossier, waarin de veiligheid en prestaties van de app worden onderbouwd. Indien de app echter een meetfunctie bevat, dan moet de beoordeling daarvan worden verricht door een onafhankelijke 'aangemelde' instantie.

Het gegeven dat het de fabrikant zelf is die kan bepalen of een app een medisch hulpmiddel is en dus een CE-markering behoeft, is een probleem omdat hij zo gemakkelijk toepassing van de wet (en de Europese richtlijn waarop deze gebaseerd is) kan ontlopen. Hij kan bijvoorbeeld stellen dat de app uitsluitend als spel bedoeld is. Uit een marktverkennend onderzoek dat de IGZ in 2013 heeft uitgevoerd naar de mate waarin fabrikanten bekend zijn met de wetgeving, komt naar voren dat dit een reëel probleem is: twee van de twintig onderzochte softwareproducten waren ten onrechte niet als medisch hulpmiddel aangemeld.

Overigens is een probleem dat een CE-markering niet de kwaliteit van het product of klinische relevantie voor het stellen van een bepaalde diagnose garandeert. zijn.

*Oplossingsrichting: aanscherping regulering omtrent 'medical devices'*
In het kader van het aanstaande Nederlandse EU-voorzitterschap, dat eHealth als topic heeft, zou dit onderwerp geagendeerd kunnen worden om te bezien of aanscherping van de regelgeving mogelijk is. Inzet zou kunnen zijn CE-markering

verplicht te stellen voor apps die betrekking hebben op gezondheid en gezondheidsstatus.

Daarnaast kan in Europees verband, in het kader van het Joint Action Plan voor medische hulpmiddelen, onderzocht worden of het toezicht op medische apps beter afgestemd kan worden, waarbij de resultaten van dat toezicht actief openbaar gemaakt worden.

Om de betrouwbaarheid en medische functionaliteit van medische apps te kunnen waarborgen is het verder wenselijk tot een keurmerk te komen.

# 1 Inleiding

In het advies over eHealth dat de Raad voor de Volksgezondheid en Zorg (RVZ) momenteel in voorbereiding heeft, staat de opkomst van consumenten-eHealth centraal. Dit is een vorm van eHealth die direct op de consumentenmarkt gericht is en niet op de professionele markt. De producten en diensten vinden hun weg rechtstreeks vanaf de producent naar de consument/patiënt en niet via de 'medische kanalen'. Het gaat onder andere om lifestyle gadgets, apps voor de smart-phone, gezondheidsplatforms en ook Persoonlijk Gezondheids Dossiers (PGD's). Eén van de hoofdvragen van het advies is welke transformatie in de gezondheidszorg kan of zal plaatsvinden als gevolg van de opkomst van consumenten-eHealth.

Deze vraag is relevant, omdat de ontwikkeling van consumenten-eHealth onstuitbaar is en vroeg of laat om respons vraagt vanuit het professionele zorgdomein. Maar we weten ook dat de implementatie en adaptatie van eHealth door zorgaanbieders moeizaam verloopt. Dit heeft verschillende oorzaken, waaronder belemmeringen die voortvloeien uit wet- en regelgeving (of het ontbreken daarvan).

In deze notitie worden juridische belemmeringen voor de implementatie en adaptatie van (consumenten-) eHealth in kaart gebracht aan de hand van zeven thema's, te weten:

1. Gegevensbescherming
2. Zeggenschap medisch dossier
3. Technische Standaarden
4. Standaard van zorg
5. Verantwoordelijkheid en aansprakelijkheid
6. Jurisdictie
7. Betrouwbaarheid elektronische hulpmiddelen (CE-markering)

Eerst volgt in deel I per thema een korte beschrijving van het relevante juridische kader, dat zowel uit nationale als Europese regelgeving bestaat. Vervolgens worden in deel II de knelpunten die daarbij aan de orde zijn samengevat. Daar waar relevant worden suggesties gegeven voor oplossingsrichtingen.

# 2 Deel I: Beschrijving juridische kaders

## 2.1 Gegevensbescherming

Bescherming van de privacy bij gebruik van e-Health heeft in de eerste plaats betrekking op bescherming van patiëntengegevens. Het gaat er dan om te waarborgen dat de patiënt zeggenschap heeft en houdt over de toegang tot zijn medische gegevens. Een aspect dat nauw verwant is aan de bescherming van de privacy als zodanig is de identificatie van 'online' partijen. Bij gebruik van e-Health is het immers voor de patiënt moeilijk(er) om vast te stellen met wie hij precies te maken heeft. Daarmee heeft hij evenmin zekerheid of gegevens die hij in het kader van het online contact verstrekt niet in onbevoegde handen terecht komen. Dat kan behalve tot aantasting van de privacy ook tot andere nadelige gevolgen leiden, bijvoorbeeld in financiële zin.

**Bescherming persoonsgegevens**
In Nederland verbiedt de Wet bescherming persoonsgegevens (Wbp) het ongeautoriseerde gebruik of de transmissie van persoonsgegevens. De wet, die op 1 september 2001 in werking is getreden, volgt de Wet persoonsregistraties (Wpr) op, die uitsluitend van toepassing was op de houder van persoonsregistraties. Met de Wbp is het toepassingsbereik in belangrijke mate uitgebreid: behalve het houden is ook het verzamelen van persoonsgegevens onder het toepassingsbereik van de wettelijke regeling gebracht. Dit is een belangrijke uitbreiding, omdat de bedreiging van de persoonlijke levenssfeer in de informatiesamenleving vooral wordt gevormd door het grote aantal mogelijkheden om persoonsgegevens buiten medeweten van de betrokkene te verzamelen en te verwerken.

Behalve het verbod op het ongeautoriseerde gebruik of de transmissie van persoonsgegevens, bevat de Wbp regels die gericht zijn op de transparantie van gegevensverwerking. Het doel daarvan is ongecontroleerde verwerking van persoonsgegevens tegen te gaan. Zo verplicht de wet degene die persoonsgegevens verwerkt, de persoon wiens gegevens geregistreerd en verwerkt worden, hierover te informeren.

Voorts kent deze wet verschillende rechten toe aan degene van wie gegevens geregistreerd worden. Deze persoon heeft bijvoorbeeld het recht zich te verzetten tegen het verzamelen en verwerken van zijn persoonsgegevens, wanneer hij een gerechtvaar-

digd individueel belang kan aantonen. In geval van verwerking in de direct-marketing is dit recht zelfs absoluut.

**Medisch beroepsgeheim**
De Wet op de geneeskundige behandelingsovereenkomst (WGBO) kent een geheimhoudingsplicht voor de hulpverlener. Deze plicht houdt in dat de hulpverlener ervoor moet zorgen dat aan anderen dan de patiënt geen inlichtingen over de patiënt worden verstrekt dan wel inzage in of afschrift van bescheiden wordt gegeven, tenzij de patiënt daarvoor toestemming heeft gegeven. Geheimhouding hoeft niet in acht te worden genomen ten aanzien van degenen die rechtstreeks betrokken zijn bij de uitvoering van de geneeskundige behandelingsovereenkomst.

Het beroepsgeheim van de arts is tevens vastgelegd in het Wetboek van Strafrecht (artikel 272 Sr). Opzettelijke schending van het beroepsgeheim is een misdrijf en wordt bestraft met gevangenisstraf van maximaal één jaar of geldboete van de vierde categorie.

Daarnaast is in de WGBO geregeld onder welke voorwaarden patiëntgegevens voor onderzoek mogen worden benut, waaronder toestemming van de patiënt.

De regels rond het medisch beroepsgeheim en de Wbp zijn vooral aan de orde wanneer in contacten tussen zorgverleners persoonsgegevens over patiënten worden uitgewisseld. De hoofdregel is dat een hulpverlener alleen met toestemming van de patiënt informatie over die patiënt aan anderen mag verstrekken. Op die hoofdregel bestaan verschillende uitzonderingen, bijvoorbeeld wanneer verstrekking van gegevens wettelijk verplicht is, wanneer gegevens worden verstrekt aan anderen die rechtstreeks bij de uitvoering van de behandelingsovereenkomst met de patiënt betrokken zijn of in geval van een conflict van plichten.

Alleen wanneer gegevens zonder schending van het beroepsgeheim zijn verkregen komt men toe aan het toetsen van de verwerking van de patiëntgegevens aan de Wbp. Behalve een rechtmatige grondslag (artikel 8) dient ook sprake te zijn van een ontheffing van het verbod op het verwerken van gezondheidsgegevens (artikel 21) of van een uitzondering (artikel 23).

**Wetsvoorstel Elektronische gegevensuitwisseling in de zorg**

Momenteel ligt het wetsvoorstel Elektronische gegevensuitwisseling in de zorg ter behandeling in de Tweede kamer. In het wetsvoorstel is onder andere opgenomen:

- de plicht van de zorgverlener om toestemming aan de patiënt te vragen voordat de medische gegevens beschikbaar worden gesteld via een elektronisch uitwisselingssysteem en om toestemming te vragen voor het elektronisch raadplegen van gegevens;
- het recht van de cliënt specifieke toestemming te verlenen aan (een) bepaalde (categorie van) zorgaanbieder(s) om zijn gegevens beschikbaar te stellen voor elektronische gegevensuitwisseling;
- het recht van de patiënt om elektronische inzage in en een elektronisch afschrift van het dossier te krijgen;
- een verbod voor zorgverzekeraars om elektronische uitwisselingssystemen voor zorgaanbieders te raadplegen.

**Identificatie**

Ten aanzien van identificatie van online partijen ontbreekt in Nederland regelgeving voor de zorg. Wel is er de wet BIG die onder meer bepaalt dat hulpverleners alleen dan gerechtigd zijn een titel te voeren wanneer zij in het BIG-register zijn ingeschreven. Voor de patiënt zal in een face-to-face-setting meestal geen noodzaak bestaan na te gaan of de andere partij - de hulpverlener - ook daadwerkelijk degene is die hij zegt te zijn en of hij over de veronderstelde kwalificaties beschikt. De setting waarin de hulpverlener werkzaam is zal in beginsel voldoende zekerheid bieden omtrent identiteit en deskundigheid van de hulpverlener. Daarnaast kan de patiënt (via het internet) het BIG-register raadplegen.

In geval van een afstandscontact is niet zichtbaar wie de andere partij online is. Ook ontbreekt het houvast van een fysieke omgeving van waaruit diensten worden aangeboden. Zelfs wanneer de aanbieder een BIG-registratienummer vermeldt in zijn contact met de patiënt, geeft dat onvoldoende zekerheid dat de hulpverlener werkelijk diegene is voor wie hij zich uitgeeft. Identificatie vormt bij de toepassing van e-Health dus een probleem.

**Internationale regelingen**

Het Europees Verdrag ter bescherming van de rechten van de mens en de fundamentele vrijheden van 1950 (EVRM) be-

schermt het recht op privacy van de burger c.q. patiënt. Aanbeveling no. R (97) 5 van 15 februari 1997 over de bescherming van medische gegevens geeft specifieke regels voor de verwerking van dergelijke gegevens. Een aanbeveling is evenwel niet bindend.

De zogenoemde dataprotectierichtlijn (95/46/EC) heeft tot doel de dataprotectie wetgeving van de lidstaten te harmoniseren, teneinde burgers van de Europese Unie maximale bescherming te bieden in het licht van de zich snel ontwikkelende informatietechnologie. Ook een richtlijn is niet rechtstreeks bindend, maar verplicht de lidstaten wel de inhoudelijke bepalingen daarvan om te zetten in nationale regelgeving. Zo is in Nederland de Wbp een direct uitvloeisel van de Europese privacyrichtlijn.

Op dit moment wordt in Brussel onderhandeld over een algemene verordening gegevensbescherming. Deze verordening moet op termijn Richtlijn 95/46/EG gaan vervangen. Deze verordening zal, net als de richtlijn nu, de voorwaarden gaan bevatten voor de verwerking van bijzondere persoonsgegevens zoals gezondheidsgegevens. Deze voorwaarden zullen ook van toepassing zijn op de verwerking van gezondheidsgegevens door middel van mobiele oplossingen.

*Is er behoefte aan specifieke data protectie regelgeving voor de gezondheidszorg?*
Omdat bij e-Health behalve behandelaar en patiënt nog andere partijen betrokken zijn, zoals de access provider, is het bestaan van een meer algemene beschermingsregeling in de vorm van de WBP een onmisbare. Daarnaast is op grond van de WGBO één persoon - de hulpverlener - primair verantwoordelijk gesteld voor de bescherming van de privacy van de patiënt met wie hij/zij een behandelingsovereenkomst heeft. In Nederland lijkt deze combinatie van wettelijke regelingen toereikend om de privacy van de patiënt te borgen, mits er gedegen toezicht op de naleving van de regelingen wordt gehouden.

Omdat de geheimhoudingsplicht van artsen vrijwel universeel is zullen alle Europese lidstaten in beginsel eenzelfde beschermingsniveau kennen (uiteraard voor zover de privacyrichtlijn is omgezet in nationale regelgeving).

De vraag is echter of dit ook geldt wanneer gegevens buiten Europa worden opgeslagen.

De dataprotectierichtlijn bepaalt thans dat de locatie van de *vestiging van 'de verantwoordelijke'* doorslaggevend is voor het van toepassing zijn er van (anders dan vaak wordt gedacht is dus niet de locatie van de *gegevens* bepalend). Hierin is de 'verantwoordelijke': *"de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt"*. De 'vestiging' is de zetel van de persoon en niet de locatie van de IT-faciliteiten die voor de verwerking van persoonsgegevens worden gebruikt.

Hoewel dus de locatie van gegevens in beginsel niet bepalend is voor de toepasselijkheid van de Wbp, is het toch noodzakelijk dat organisaties in Nederland rekening houden met de locatie waarnaar persoonsgegevens doorgegeven en verwerkt worden in het kader van cloud computing.
Als de vestiging van de verantwoordelijke zich **binnen** een EU-lidstaat bevindt, is de richtlijn - en daarmee de Wbp - van toepassing, ook al bevinden de IT-activiteiten en faciliteiten zich buiten de Europese Unie. Wel is het zo dat in dat geval óók andere regelgeving van kracht kan zijn! Wanneer bijvoorbeeld gegevens zijn opgeslagen in een datacenter op Amerikaans grondgebied, is bijvoorbeeld de USA Patriot Act van toepassing; deze wet heeft als doel om de Amerikaanse overheid meer mogelijkheden te geven om informatie te verzamelen over en op te treden in geval van mogelijk terrorisme. Ook als de vestiging van de service provider zich **buiten** Nederland bevindt, maar de verwerking wel gebruik maakt van al dan niet geautomatiseerde middelen die zich binnen Nederland bevinden is de Wbp van toepassing. Omdat ook cookies onder het begrip *geautomatiseerde middelen* vallen, is de Wbp vrijwel zeker ook van toepassing op de cloud diensten van een service provider buiten de Europese Unie.

Verder bepaalt de Wbp dat persoonsgegevens slechts aan landen buiten de Europese Unie mogen worden doorgegeven indien deze landen een *'passend beschermingsniveau waarborgen'*. De Europese Commissie bepaalt formeel of een land een passend beschermingsniveau kent en plaatst deze op een witte lijst. Op deze lijst staan landen als Australië, Canada en de Verenigde Staten. Voor de VS gaat het daarbij om organisaties die voldoen aan de Safe Harbor principes. De Safe Harbor principes zijn bedoeld voor Amerikaanse bedrijven die zaken doen met organisaties binnen de Europese Unie. Amerikaanse bedrijven die

beschikken over een Safe Harbor certificaat worden verondersteld een passend beschermingsniveau te bieden. Wanneer een Nederlandse organisatie een clouddienst afneemt van een service provider in een van deze landen op de witte lijst van de Europese Commissie, is de Wbp van toepassing. In de praktijk zal het echter moeilijk zijn dit recht af te dwingen of handhaving te verlangen. Bovendien is inmiddels duidelijk geworden dat er veel fraude plaatsvindt met de Safe Harbor-certificaten en dat deze dus onvoldoende waarborgen bieden. Uit onderzoek van het Australische bureau Galexia bleek dat veel bedrijven met het Safe Harbor-certificaat niet aan alle voorwaarden daarvoor voldoen. Ook bleek dat veel organisaties die het certificaat beweren te hebben zelfs niet eens bij Safe Harbor zijn geregistreerd. Dit is mogelijk omdat Safe Harbor een systeem van zelfregulering is, met een onvoldoende juridische basis. De Amerikaanse overheid oefent ook geen toezicht uit op de naleving van de Safe Harbor principes.

Het Nederlandse kabinet vraagt zich in reactie op het groenboek van de Europese Commissie over eHealth (april 2014) dan ook af of er aanvullende maatregelen nodig zijn op het gebied van dataprotectie en privacy in het geval dat gegevens van Nederlandse, dan wel Europese burgers door private partijen buiten Europa worden opgeslagen. Het kabinet acht het wenselijk dat de Commissie zaken als privacyaspecten in relatie tot Big data verder in kaart brengt, en indien nodig aanvullende eisen stelt aan andere (niet-Europese) landen.

**Op weg naar een nieuwe EU privacy Verordening**
In januari 2012 presenteerde de Europese Commissie een nieuw wettelijk kader dat de huidige privacyrichtlijn 95/46/EG moet gaan vervangen. Een belangrijke aanleiding hiervoor is dat de huidige richtlijn niet is ingesteld op de huidige en toekomstige technologische ontwikkelingen. De voorgestelde Verordening dient een, voor alle lidstaten direct geldend, technologieneutraal eskader te zijn dat kan anticiperen op deze ontwikkelingen.

Deze Verordening voorziet in een oplossing voor het hiervoor geschetste probleem: zij bepaalt namelijk dat voor doorgifte van Europese persoonsgegevens aan buitenlandse overheden toestemming is vereist van een toezichthoudende autoriteit (NOS clause). Bedrijven mogen persoonsgegevens van Europese burgers niet meer zomaar delen wanneer buitenlandse overheden (van derde landen) dit verzoeken. Voorafgaand aan een dergelijk verzoek dient een toezichthoudende autoriteit hiervoor toestemming te geven. De "No-NSA clause" is voornamelijk ook

een signaal naar landen buiten Europa die persoonsgegevens vorderen. Op het moment is er weinig wetgeving die dit soort verzoeken regelt. Om zicht en controle over deze verzoeken te krijgen is deze “No NSA clause” ontstaan.

Andere belangrijke punten in de voorgestelde privacy Verordening zijn de volgende:

- Profiling en gebruik van pseudonieme gegevens.
  Voor organisaties wordt het mogelijk gemaakt om gemakkelijker gepseudonimiseerde gegevens te verwerken, bijvoorbeeld in een database waarbij NAW gegevens zijn vervangen door ID-nummers. Echter, indien de verantwoordelijke ook de 'sleutel' tot deze gegevens bezit (dus een tabel die de ID-nummers weer terug herleidt naar de NAW gegevens), dan wordt de data niet meer als pseudoniem aangemerkt. Deze nieuwe regeling zal het voor veel organisaties met grote (klant) databases makkelijker maken om deze gegevens te verwerken en profiling toe te passen.
- Criterium voor verplicht aanstellen Functionaris voor de Gegevensbescherming (FG).
  Organisaties die binnen een jaar persoonsgegevens verwerken van meer dan 5000 personen, dienen verplicht een Functionaris voor de Gegevensbescherming aan te stellen.
- Verplichting tot uitvoeren risico analyses.
  De verantwoordelijke (en mogelijk de bewerker) dient indien zij persoonsgegevens verwerkt, een risicoanalyse uit te voeren om na te gaan of en welke risico's zich mogelijk bij de verwerking van de persoonsgegevens kunnen presenteren. De Verordening omschrijft welke verwerkingen hoogstwaarschijnlijk bepaalde risico's met zich meedragen. Het is nog niet gedefinieerd of dit een verplichte PIA (privacy impact assessment) betekent maar ook dit zal aanvullende verplichtingen met zich meebrengen.
- Datalekken: melden binnen 72 uur.
  Indien er sprake is van een datalek dient de verantwoordelijke dit zo snel mogelijk, maar uiterlijk binnen 72 uur, te melden aan de toezichthoudende autoriteit. De bewerker is ook verplicht een dergelijk datalek zo snel mogelijk te melden aan de verantwoordelijke. Onder bepaalde omstandigheden kan er ook een verplichting ontstaan om de betrokkene persoonlijk van de datalek op de hoogte te brengen.
- Recht om gegevens te wissen (*Right to erasure*).
  Betrokkenen hebben het recht om van de verantwoordelijke te eisen dat alle persoonsgegevens van hem of haar worden gewist. Dit wat beter uitvoerbare recht komt in de plaats

van het veelbesproken *right to be forgotten*. Dit *right to erasure* geldt ook voor alle gegevens die de verantwoordelijke met behulp van een derde verwerkt. De verantwoordelijke heeft een plicht om al deze ingeschakelde (derde) partijen over het verzoek van de betrokkenen in te lichten en dient na te gaan of deze partijen ook werkelijk aan dit verzoek hebben voldaan.

- Expliciete toestemming van de betrokkene.
  In het geval dat toestemming als grondslag wordt gebruikt, is de verantwoordelijke in principe genoodzaakt om expliciet toestemming te verkrijgen van de betrokkene voor het verwerken van persoonsgegevens. Ook moet het voor de betrokkene gemakkelijk zijn om deze toestemming weer in te trekken.
- Mogelijkheid voor organisaties tot verkrijgen van Compliance Certificaat.
  Een organisatie mag aan toezichthoudende instanties binnen de Europese Unie vragen om een bevestiging dat zij zich houden aan de regels neergelegd in de Verordening. Dit gaat om een zogenoemde *Data Protection Seal*, oftewel een certificaat dat bewijst dat het organisatie privacy compliant is. De toezichthoudende autoriteit wijst hier speciale derde onafhankelijke partijen (auditors) voor aan die de audit namens de toezichthoudende autoriteit uitvoeren. De toezichthoudende autoriteit beoordeelt de audit die is uitgevoerd door de derde partij en heeft uiteindelijke het laatste woord.
- Boetes: maximaal 5% van de wereldwijde jaaromzet.
  Indien een organisatie de voorgestelde regels niet naleeft of overtreedt, loopt zij het risico op een boete van €100.000.000 of op een boete bestaande uit 5% van de wereldwijde jaaromzet van die organisatie.

De verordening is op elk bedrijf dat persoonsgegevens verwerkt van toepassing. Ook dus op de kleinere bedrijven. Wel is het punt van de boete voornamelijk gericht op de echt grote bedrijven die heel veel persoonsgegevens verzamelen en de regels aan hun laars lappen.

Aanvankelijk was het de ambitie om vòòr de verkiezingen in het Europees Parlement, in mei 2014, een definitief akkoord te hebben over de Verordening. Dit is niet gelukt. Op dit moment is niet bekend wanneer de nieuwe Verordening zal kunnen worden vastgesteld.

## 2.2 Zeggenschap over medisch dossier

Op grond van de WGBO is de hulpverlener verplicht een dossier bij te houden over de patiënt waarmee hij een behandelingsovereenkomst heeft. De patiënt heeft het recht om zijn dossier in te zien en om (eventueel tegen geringe vergoeding) afschrift te vragen van (delen van) het dossier. Het blijkt echter nog geen gangbare praktijk om patiënten inzage in hun medisch dossier te geven. Een patiënt kan dit recht moeilijk effectueren.

Hieraan zou - zo is de verwachting van de minister van Volksgezondheid, Welzijn en Sport (VWS) - (beter) tegemoet gekomen kunnen worden door het voornemen om in de Wet cliëntenrechten zorg (Wcz) een recht van de patiënt op elektronische toegang tot en afschrift van het medisch dossier op te nemen.

Hoewel dit een stap in de goede richting is, gaat dit niet ver genoeg. De RVZ heeft diverse malen ervoor gepleit een andere regeling te treffen omtrent de zeggenschap over het medisch dossier: die zou primair bij de patiënt moeten liggen. De patiënt moet kunnen bepalen wie op welk moment toegang heeft tot 'zijn' medisch dossier of delen daarvan. Het omdraaien van de zeggenschap laat de verplichting van de hulpverlener om dossier te voeren onverlet. Dit biedt tevens mogelijkheden om het medische dossier te integreren in het PGD van de patiënt (indien aanwezig). En, belangrijker nog: aldus ontstaat een integraal 'patiëntvolgend medisch dossier' (zie blog Vesseur op Skipr).

Een PGD is een dossier waarmee de patiënt zelf begint en dat hij zelf bijhoudt. In juridische zin is de Wbp niet van toepassing bij een PGD als het wordt bijgehouden voor uitsluitend persoonlijke doeleinden of als het zo is ingericht dat de beheerder van het PGD (bijv. de zorgverlener) feitelijk geen macht kan uitoefenen over de persoonsgegevens in het PGD.

Juridisch gezien is het PGD vanwege de dossierplicht van de zorgverlener (artikel 7:454 lid 1 BW) binnen het geldende recht geen alternatief voor de medische gegevens die de hulpverlener/zorgaanbieder dient bij te houden. De zorgverlener is namelijk verplicht zelf een dossier van de patiënt bij te houden. De WGBO maakt het voor de patiënt mogelijk om van het aanvullingsrecht gebruik te maken. Dit biedt de mogelijkheid dat beide

dossiers elkaar aanvullen en onderling patiëntgegevens uitwisselen.

Het PGD wordt (aannemende dat het niet in handen is van zorgaanbieders) niet beschermd door het medisch beroepsgeheim. Medische gegevens in het PGD kunnen onder sociale of financiële druk ook inzichtelijk worden voor personen of instanties buiten de gezondheidszorg. Ook kan in een rechtszaak de patiënt tot gegevens verstrekking uit het PGD worden gedwongen waar de arts zich op het verschoningsrecht zou kunnen beroepen. Mogelijk is het een idee om te onderzoeken of er zoiets als een patiëntengeheim moet komen voor het PGD?

## 2.3 Technische standaarden

Het gebruik van uniforme technische standaarden heeft verschillende voordelen: het bewerkstelligt een vereenvoudiging van de administratie en kan daarmee leiden tot kostenbesparing; het bevordert de kwaliteit van zorg, doordat minder fouten worden gemaakt bij de overdracht van gegevens en doordat gegevens gemakkelijker (en sneller) zijn uit te wisselen, waardoor de continuïteit van zorg (ketenzorg) beter is te waarborgen. In de praktijk worden echter verschillende technische standaarden gebruikt, onder andere voor de communicatie tussen systemen en netwerken, voor de opslag, bewerking en transmissie van elektronische patiëntengegevens en voor de bescherming van de veiligheid, integriteit en authenticiteit van elektronische data.

**Nationale regelingen**
In Nederland ontbreekt een (wettelijke) regeling die voorziet in de toepassing van uniforme technische standaarden. Iedere fabrikant van eHealth-applicaties bepaalt zelf welke 'standaarden' hij gebruikt. Wel bestaan er organisaties, bestaande uit veldpartijen in verschillende samenstelling, die de ontwikkeling en toepassing van standaarden bevorderen. Deze organisaties zijn per 1 januari 2002 opgegaan in de stichting Nationaal ICT Instituut in de Zorg (NICTIZ).

**Internationale regelingen**
Ook op Europees niveau zijn er geen regelingen die technische standaardisatie voorschrijven dan wel bevorderen. Wel is er door de Europese Standaardisatie Commissie (CEN) onder mandaat van de Europese Commissie een aantal belangrijke technische specificaties ontwikkeld, maar deze worden niet door alle lidstaten gehanteerd.

Vanuit Europees perspectief bezien dient standaardisatie in de eerste plaats een economisch doel. Het gebrek aan uniforme standaarden wordt gezien als een belangrijke reden waarom ICT niet optimaal wordt gebruikt in de zorg. Daarmee wordt voorkomen dat een Europese markt voor producten ontstaat en worden barrières opgeworpen voor de grensoverschrijdende communicatie van zorggerelateerde informatie.

eHealth groeit vooral in die sectoren waarin wel open, gepubliceerde standaarden en technische specificaties worden gehanteerd. Zo heeft bijvoorbeeld de HL7 groep standaarden gedefinieerd voor de transmissie van data ten behoeve van de patiëntenadministratie, facturering, ordercommunicatie en resultatenrapportage. Dit protocol maakt het bijvoorbeeld mogelijk om bedside terminals, patiëntenregistratiesystemen, ordercommunicatiesystemen en IC-monitoren te incorporeren in één enkel systeem. Hierdoor zijn patiëntenadministratiesystemen inmiddels nagenoeg gangbaar geworden en is er een Europese markt voor dergelijke systemen.

Er bestaat in Europa vrij algemeen overeenstemming over het feit dat het gebrek aan (uniforme) technische standaarden vooruitgang belemmert en dat actie om tot standaardisering te komen urgent is.

In de richtlijn Patiëntenrechten bij grensoverschrijdende zorg (van 9 maart 2011) wijst de EU onder meer op het belang van interoperabiliteit tussen ICT-systemen in de lidstaten. In dat verband kan hier worden gewezen op het epSOS-project, dat zich richt op de bouw van een infrastructuur die grensoverschrijdende interoperabiliteit mogelijk moet maken tussen EPD-systemen in Europa.

Op verzoek van de EU-lidstaten heeft de Europese Commissie in 2009 het eHealth actieplan voor de periode 2012-2020 opgesteld. Door de snelle technische ontwikkelingen, zoals de komst van medische apps voor de smartphone, was een update van het actieplan nodig. Daarom ligt er nu het eHealth actieplan 2014-2020. Begin 2014 heeft het Europees Parlement hiermee ingestemd. Onder leiding van de commissaris digitale agenda (Neelie Kroes) gaat de Commissie werken aan internationale eHealth-normen. Ook zullen voor het eHealth-verkeer tussen de EU-lidstaten standaarden, protocollen en procedures ontwikkeld worden.

## 2.4 Standaard van zorg

Elektronische communicatiemiddelen worden behalve ten behoeve van de zorgondersteuning ook steeds meer ingezet voor de zorg zelf (eHealth). Hoewel ontwikkelingen op dit vlak nog in de kinderschoenen staan is het van groot belang na te gaan hoe gewaarborgd wordt (of kan worden) dat eHealth voldoet aan de 'standaard van zorg'.

**Nationale regelingen**
De regels die de behandelingsovereenkomst tussen arts en patiënt beheersen zijn in Nederland neergelegd in de Wet op de geneeskundige behandelingsovereenkomst (WGBO). De WGBO is van toepassing op de 'geneeskundige behandelingsovereenkomst'. Dat is de overeenkomst waarbij de hulpverlener zich tegenover de patiënt verbindt tot het verrichten van handelingen op het gebied van de geneeskunst (artikel 7: 446 lid 1 BW).

Handelingen op het gebied van de geneeskunst zijn alle verrichtingen - inclusief het onderzoeken en het geven van raad - die rechtstreeks betrekking hebben op een persoon en ertoe strekken om hem van een ziekte te genezen, voor het ontstaan van een ziekte te behoeden of zijn gezondheidstoestand te beoordelen, dan wel deze verloskundige bijstand te verlenen. Onder handelingen op het gebied van de geneeskunst worden tevens begrepen het in het kader daarvan verplegen en verzorgen van de patiënt en het overigens rechtstreeks ten behoeve van de patiënt voorzien in de materiële omstandigheden waaronder die handelingen kunnen worden verricht. Ook bij eHealth is er dus sprake van een overeenkomst tussen een hulpverlener en een patiënt, die beheerst wordt door de WGBO.

De belangrijkste verplichtingen voor de hulpverlener die uit de WGBO voortvloeien zijn de informatieplicht, het vereiste van informed consent en de zorgvuldigheidsplicht:

- *Informatieplicht*
  De WGBO verplicht de hulpverlener in beginsel om de patiënt op duidelijke wijze en desgevraagd schriftelijk in te lichten over het voorgenomen onderzoek en de voorgestelde behandeling en over de ontwikkelingen omtrent het onderzoek, de behandeling en de gezondheidstoestand van de patiënt.
- *Vereiste van informed consent*

Voor verrichtingen ter uitvoering van een behandelingsovereenkomst is de toestemming van de patiënt vereist. Op verzoek van de patiënt legt de hulpverlener in ieder geval schriftelijk vast voor welke verrichtingen van ingrijpende aard deze toestemming heeft gegeven.

- *Zorgvuldigheidsplicht (standaard van zorg)*
  De hulpverlener moet bij zijn werkzaamheden 'de zorg van een goed hulpverlener' in acht nemen. Hij moet daarbij handelen in overeenstemming met de op hem rustende verantwoordelijkheid, die voortvloeit uit de voor hulpverleners geldende professionele standaard. Deze verplichting gaat verder dan louter de plicht voor de hulpverlener om zo goed mogelijk zijn best te doen; dat is niet voldoende. Hij moet handelen conform 'de standaard'; doet hij dat niet dan is hij in gebreke en deswege aansprakelijk.

Het toezicht op de medische beroepsuitoefening berust bij de Inspectie. Daarnaast toetst ook de rechter het medisch tuchtcollege, de civiele rechter en/of de strafrechter of hulpverleners handelen conform de standaard van zorg. Deze standaard is voor de rechter ankerpunt van toetsing. De wet bepaalt evenwel niet de inhoud van de standaard van zorg; dat gebeurt door de beroepsbeoefenaren zelf. De standaard van zorg is kenbaar uit bijvoorbeeld gedragsregels van professionele organisaties, wetenschappelijke literatuur etc. Het gaat er daarbij om wat in de (internationale) kring der beroepsgenoten gebruikelijk is.

Het is duidelijk dat een standaard niet van de ene op de andere dag ontstaat noch dat deze op voorhand is vast te stellen dat wil zeggen nog voordat een nieuwe behandelmethode of subspecialiteit van de geneeskunde wordt toegepast. Een standaard moet zich ontwikkelen. Omdat de ontwikkeling van eHealth in Nederland (nog) in de kinderschoenen staat heeft de rechter weinig houvast om te kunnen toetsen. Wel is duidelijk dat de rechter desgevraagd als uitgangspunt hanteert dat de burger c.q. patiënt recht heeft op dezelfde kwaliteit van zorg van dezelfde hoge standaard als die welke door conventionele methoden wordt geleverd.

De KNMG heeft in 2004 een aantal uitgangspunten geformuleerd in de Richtlijn online arts-patiëntcontact voor zorgverleners die online contact onderhouden met patiënten. In 2007 is deze Richtlijn herzien. De richtlijn beperkt zich tot online contacten waarbij de arts een vraagt beantwoordt, een gericht advies geeft, farmacotherapie start of een herhaalrecept uitschrijft.

De algemene uitgangspunten uit de richtlijn houden in dat online contact bij voorkeur ingebed moet zijn in een reeds bestaande behandelrelatie tussen arts en patiënt. Zonder een bestaande behandelrelatie is online contact ook wel toegestaan mits de risico's die daarmee gepaard gaan minimaal zijn. De arts kan immers alleen maar afgaan op de informatie die hem door de patiënt is verstrekt.

Het voorschrijven van geneesmiddelen via internet is daarentegen verboden als de voorschrijver de patiënt nog nooit persoonlijk heeft ontmoet of de voorschrijver de patiënt niet kent of van wie de voorschrijvende medicatiehistorie niet beschikbaar heeft (art. 67 Geneesmiddelenwet). Dit is bevestigd in jurisprudentie in de zaak Multatuli (handelend voor dokteronline.nl) en de staat.

Overigens geldt meer in het algemeen het adagium: offline = online; dwz wat een arts offline niet zou doen, doet hij ook online niet.

## 2.5 Aansprakelijkheid

Bij gebruik van elektronische communicatiemiddelen ter uitvoering van een individuele behandelingsovereenkomst zijn meer partijen betrokken dan de hulpverlener en de patiënt. Daarmee is de vraag naar wie aansprakelijk is wanneer in die uitvoering iets misgaat complexer dan bij gebruik van conventionele methoden.

**Nationale regelingen**

*Aansprakelijkheid wegens wanprestatie*

Wanneer de hulpverlener niet de zorg van een goed hulpverlener betracht, dat wil zeggen niet handelt conform de voor hem geldende professionele standaard, pleegt hij wanprestatie en is hij deswege aansprakelijk op grond van de WGBO.
Naast de aansprakelijkheid van de hulpverlener roept de WGBO een centrale aansprakelijkheid in het leven. Als ter uitvoering van een behandelingsovereenkomst verrichtingen plaatsvinden in een ziekenhuis dat bij die overeenkomst geen partij is, is het ziekenhuis voor een tekortkoming daarin mede aansprakelijk, als ware het zelf bij de overeenkomst partij. De aansprakelijkheid van een hulpverlener of van het ziekenhuis kan niet worden beperkt of uitgesloten.

*Aansprakelijkheid voor gebrekkige apparatuur*
Wanneer in de uitvoering van de eHealth-overeenkomst iets misgaat ten gevolge van het verkeerd overbrengen van informatie kunnen verschillende personen aansprakelijk gesteld worden. Als de fout zit in het niet adequaat functioneren van de apparatuur dan is de hulpverlener c.q. het ziekenhuis in de eerste plaats zelf aansprakelijk als het schuld heeft aan dat niet functioneren, bijvoorbeeld vanwege fouten in de aanschaf, onvoldoende onderhoud of controle van de apparatuur. Heeft de hulpverlener/het ziekenhuis geen schuld dan zal de tekortkoming als gevolg van het gebruik van een ongeschikte zaak in de regel (toch) aan het ziekenhuis worden toegerekend op grond van artikel 6;77 van het Burgerlijk Wetboek als er een overeenkomst is en op grond van artikel 6;173 BW als die overeenkomst er niet is (= aansprakelijkheid voor gebrekkige zaken). Een uitzondering geldt als toerekening onredelijk zou zijn.

Aanvankelijk kon in gevallen van medische aansprakelijkheid een beroep op deze ontsnappingsclausule voor de hand liggen. Daarop wijst bijvoorbeeld de uitspraak van de Minister bij de parlementaire behandeling van boek 6 BW. Daar staat dat de mogelijkheid open dient te worden gelaten dat een vordering tegen een arts of ziekenhuis ter zake van het falen van gebruikte apparatuur of geneesmiddelen wordt afgewezen, bijvoorbeeld omdat aansprakelijkheid van de producent van de zaak meer voor de hand ligt. Deze opvatting is in de toelichting op de WGBO overgenomen.

Het is echter zeer de vraag of de rechter zo'n verweer van het ziekenhuis gemakkelijk zal aanvaarden want er zijn sterke argumenten om met name het ziekenhuis juist wel aansprakelijk te houden. Denk bijvoorbeeld aan het feit dat de keuze voor bepaalde apparatuur of materiaal aan het ziekenhuis is of aan het feit dat het ziekenhuis altijd verzekerd is.

Als de hulpverlener dan wel het ziekenhuis niet aansprakelijk zijn, kan de producent dat wel zijn. Artikel 6;185 BW bepaalt dat de producent aansprakelijk is voor de schade veroorzaakt door een gebrek in zijn product, ongeacht of hem iets valt te verwijten. Een product is gebrekkig als het niet de veiligheid bezit die men daarvan mag verwachten.

**Internationale regelingen**
*Professionele aansprakelijkheid*

Hoewel de wetgeving in de lidstaten van de EU ten aanzien van medische beroepsbeoefenaren die wanprestatie plegen verschilt, ligt daaraan wel steeds hetzelfde basisprincipe ten grondslag. Het gaat er steeds om of de betreffende beroepsbeoefenaar heeft gehandeld overeenkomstig de voor hem geldende standaard van zorg.

Wanneer bijvoorbeeld een patiënt letsel oploopt doordat een radioloog een vergroting van het ruggenmergkanaal niet heeft waargenomen op een digitaal radiogram dat door een huisarts per e-mail naar hem is gezonden, is de radioloog nalatig/pleegt hij wanprestatie indien - overeenkomstig de standaard van zorg - een redelijk bekwaam en zorgvuldig handelend radioloog zo'n vergroting op datzelfde moment wel had gezien. Maar als de gemiste diagnose van een abnormaliteit is die normaal gesproken niet duidelijk kenbaar zou zijn voor een consultant die een digitaal radiogram bekijkt, dan is hij niet aansprakelijk. De aansprakelijkheid van een hulpverlener is dus afhankelijk van het bewijs van nalatigheid.

*Aansprakelijkheid voor gebrekkige apparatuur*

Wanneer in het hierboven geschetste voorbeeld een patiënt letsel oploopt en de hulpverlener niet nalatig is geweest kan de fout een gevolg zijn van een technisch defect in het systeem waarmee het beeld verzonden was. Het defect kan veroorzaakt zijn door nalatigheid van degenen die verantwoordelijk zijn voor het onderhoud, de inspectie of reparatie of door een gebrek in het product zelf. In het laatste geval is de fabrikant of leverancier van de apparatuur aansprakelijk.

De aansprakelijkheid voor een gebrekkig product is een risico-aansprakelijkheid, dat wil zeggen dat aansprakelijkheid is gegeven wanneer gebrekkigheid vaststaat. Deze aansprakelijkheid vloeit voort uit de Europese Richtlijn voor aansprakelijkheid van gebrekkige producten (85/374/EC). De productaansprakelijkheid omvat alle bestanddelen van een product. Wanneer de producent niet geïdentificeerd kan worden is de leverancier in zijn plaats aansprakelijk. De bescherming die van deze richtlijn uitgaat is evenwel beperkt omdat de definitie van een product in deze richtlijn (artikel 2) beperkt is tot roerende goederen; met andere woorden: aansprakelijkheid voor zorgtelematica-applicaties is beperkt tot gebrekkige tastbare en technische componenten.

**Is een apart aansprakelijkheidsregime voor eHealth gewenst?**
Veel zorgaanbieders zijn bezorgd dat het gebruik van informatie- en communicatietechnologie om zorg op afstand te leveren een substantieel nieuwe risicoblootstelling teweeg zal brengen en daardoor meer claims wegens medische wanprestatie. Zij zijn er niet zeker van dat het gebruik van zorgtelematica onder de dekking van hun aansprakelijkheidsverzekering valt.

Er zijn tot op heden nog geen gegevens beschikbaar over wanprestatiezaken bij gebruik van zorgtelematica die voor een rechter zijn verschenen, noch in Europa noch in USA. Dit moet echter niet gezien worden als een indicatie van de veiligheid van e-zorg, maar als inherent aan het feit dat het gebruik van dergelijke technologie nog niet gangbaar is. Sommige partijen hebben gesuggereerd dat er een verplicht risico aansprakelijkheidsregime tot stand gebracht moet worden voor patiënten die schade hebben geleden door het gebruik van e-zorg. De vraag is of dit voorstel kans van slagen heeft, aangezien het eHealth zou afzonderen van het aansprakelijkheidsregime dat voor de algemene medische praktijk geldt (en waarbij bewijs van nalatigheid/wanprestatie geleverd moet worden).

Het Nederlands kabinet geeft in zijn reactie op het eerder genoemde groenboek van de Eu aan het te vroeg te vinden om een uitspraak te kunnen doen over de aansprakelijkheid op Europees niveau. Vooralsnog voorziet het kabinet dat het aansprakelijkheidsrecht dat op nationaal niveau van kracht is, voldoende waarborgen geeft.

## 2.6 Jurisdictie

Een elektronisch medisch consult bestaat momenteel voornamelijk uit het vragen om en geven van advies. Naar Nederlands recht valt het geven van raad onder de werkingssfeer van de Wet op de geneeskundige behandelingsovereenkomst (WGBO). Het is echter niet vanzelfsprekend dat op de overeenkomst inzake het consult het Nederlands recht van toepassing is. Wanneer de arts in het buitenland gevestigd is, kunnen partijen - de arts en de consument/patiënt - verklaren dat de overeenkomst onderworpen is aan het recht van het land waar de arts, de dienstverlener, is gevestigd. Dat neemt niet weg dat de consument/patiënt op grond van het *Verdrag inzake het recht dat van toepassing is op verbintenissen uit overeenkomst (Verdrag 80/934/EEG)* dwingende

bepalingen die te zijner bescherming zijn opgenomen in het recht van het land waar hij zijn gewone verblijfplaats heeft kan inroepen. Dit betekent dat de consument/patiënt een beroep kan doen op de rechten die voor hem voortvloeien uit de WGBO. Het betekent ook dat de arts, zelfs wanneer hij in het buitenland is gevestigd, aansprakelijkheid voor een tekortkoming zijnerzijds niet kan uitsluiten of beperken. In beginsel lijkt de patiënt juridisch goed beschermd. De praktijk zal moeten uitwijzen of ook hierbij handhaving van de wet adequaat mogelijk is.

## 2.7 Betrouwbaarheid elektronische hulpmiddelen

Als een medische app wordt gebruikt voor diagnostiek of therapie is het volgens de wet een medisch hulpmiddel. In dat geval is de Richtlijn Medische Hulpmiddelen (RMH) van toepassing en is een CE-markering verplicht. De meeste medische apps vallen vooralsnog in de minst strenge risicoklasse van de registratie. Dit betekent dat het bedrijf dat de app op de markt brengt, hem zelf mag certificeren door het maken en bijhouden van een technisch dossier, waarin de veiligheid en prestaties van de app worden onderbouwd. Indien de app echter een meetfunctie bevat, dan moet de beoordeling daarvan worden verricht door een onafhankelijke 'aangemelde' instantie.

De IGZ, die belast is met het toezicht op de naleving van de RMH, heeft aangekondigd vanaf 2013 te gaan toezien op certificering van medische apps. Hoewel dit een stap in de goede richting is, is hiermee onvoldoende geborgd dat twijfels over de betrouwbaarheid van health apps kunnen worden weggenomen, en wel om twee redenen:

- Het is de fabrikant zelf die kan bepalen of een app een medisch hulpmiddel is en dus een CE-markering behoeft. Voor de vraag of software onder de RMH valt is immers doorslaggevend "het gebruik waartoe het hulpmiddel is bestemd volgens de aanwijzingen die de fabrikant op het etiket, de gebruiksaanwijzing en/of het reclamemateriaal verschaft". Door bijvoorbeeld aan te geven dat een app uitsluitend voor recreatieve doeleinden of als spel bedoeld is, ontlopen fabrikanten vrij eenvoudig toepassing van deze richtlijn.
- Veel medische apps worden buiten de EU vervaardigd en gekocht (zoals apps van Apple, die uitsluitend in de Apple Appstore te koop zijn). De RMH is in dit geval niet van toepassing, evenals de Europese richtlijn terzake.

**Internationale regelingen**
Een mobiele oplossing zoals een leefstijl- of een welzijnsapp valt al naar gelang de kwalificatie onder verschillende Europese instrumenten. Indien hij wordt gekwalificeerd als medisch hulpmiddel dan valt hij onder Richtlijn 93/42/EEG betreffende medische hulpmiddelen of Richtlijn 98/79/EG betreffende medische hulpmiddelen voor in-vitro diagnostiek. Beide richtlijnen worden momenteel herzien. Er is nu nog niet te voorzien of leefstijl- en welzijnsapps binnen het toekomstige toepassingsbereik zullen worden opgenomen en wat de specifieke vereisten zullen zijn voor medische apps die voldoen aan de definitie van een medisch hulpmiddel. Indien de mobiele oplossing niet wordt gekwalificeerd als een medisch hulpmiddel dan is Richtlijn 2001/95/EG inzake algemene productveiligheid van toepassing.

De genoemde richtlijnen zijn omgezet in nationale wetgeving. Er is op dit moment nog onvoldoende zicht op de brede ontwikkeling van mobiele oplossingen inclusief leefstijl- en welzijnsapps om de vraag te kunnen beantwoorden of er nadere regelgeving noodzakelijk is. Het kabinet is ter zake van mening dat Europa zich terughoudend moet opstellen ten aanzien van nieuwe regulering, maar gezien het gegeven dat er sprake is van één (Europese) markt moet naar mening van het kabinet de aanbieder van de app wel aantonen dat de app doet wat deze belooft te doen.

# 3 Juridische drempels voor (consumenten) eHealth en oplossingsrichtingen

## 3.1 Gegevensbescherming

Voor zorgaanbieders/zorgverleners vormt de wettelijk geregelde privacybescherming (medisch beroepsgeheim en bescherming persoonsgegevens) een voorwaarde waaraan te allen tijde moet worden voldaan. De regels rond het medisch beroepsgeheim en de Wbp zijn vooral aan de orde wanneer in contacten tussen zorgverleners persoonsgegevens over patiënten worden uitgewisseld. De hoofdregel is dat een hulpverlener alleen met toestemming van de patiënt informatie over die patiënt aan anderen mag verstrekken. Op die hoofdregel bestaan verschillende uitzonderingen, bijvoorbeeld wanneer verstrekking van gegevens wettelijk verplicht is, wanneer gegevens worden verstrekt aan anderen die rechtstreeks bij de uitvoering van de behandelingsovereenkomst met de patiënt betrokken zijn of in geval van een conflict van plichten. Alleen wanneer gegevens zonder schending van het beroepsgeheim zijn verkregen komt men toe aan het toetsen van de verwerking van de patiëntgegevens aan de Wbp. Behalve een rechtmatige grondslag (artikel 8) dient ook sprake te zijn van een ontheffing van het verbod op het verwerken van gezondheidsgegevens (artikel 21) of van een uitzondering (artikel 23).

De privacybeschermingsregels gelden ongeacht of er sprake is van conventionele zorg dan wel van eHealth. In geval van eHealth zullen vooral de eisen uit de Wbp navranter aan de orde zijn, door de veel ruimere mogelijkheden tot elektronische gegevensuitwisseling.

In beginsel is zowel in nationaal als in Europees verband de bescherming van persoonsgegevens toereikend geregeld. Consumenten en patiënten hebben in dit opzicht houvast in de vorm van de Wet Bescherming Persoonsgegevens en de Wet op de Geneeskundige Behandelingsovereenkomst. Consumenten moeten zich realiseren dat dit niet het geval is wanneer zij zich via het Internet buiten Europa begeven en persoonsgegevens verstrekken.

Momenteel wordt de Europese dataprotectierichtlijn herzien en (waarschijnlijk) omgezet in een Verordening. Deze Verordening voorziet ook in een oplossing voor dit probleem: zij bepaalt

namelijk dat voor doorgifte van Europese persoonsgegevens aan buitenlandse overheden toestemming is vereist van een toezichthoudende autoriteit (No-NSA clause). Andere belangrijke punten in de voorgestelde Verordening zijn: Een Verplichting voor de verantwoordelijke en mogelijk de bewerker tot het uitvoeren van risicoanalyses bij de verwerking van de persoonsgegevens; het melden van datalekken binnen 72 uur aan de toezichthoudende autoriteit; en het recht van betrokkenen om te eisen dat alle persoonsgegevens van hem of haar worden gewist (right to erasure).

Aanvankelijk was het de ambitie om vòòr de verkiezingen in het Europees Parlement, in mei 2014, een definitief akkoord te hebben over de Verordening. Dit is niet gelukt. Op dit moment is niet bekend wanneer de nieuwe Verordening zal kunnen worden vastgesteld.

*Oplossingsrichtingen:*
Indien de voortgang in de totstandkoming van de Verordening uitblijft biedt het Nederlandse EU-voorzitterschap in 2016 een goede gelegenheid om dit onderwerp prominenter op de agenda te krijgen.

Daarbij kan expliciet in de overwegingen worden betrokken of een wettelijk geregeld 'patiëntgeheim' een goede aanvulling is op de waarborgen voor patiënten die de nieuwe Verordening in zich draagt. De RVZ heeft in zijn advies 'Patiënteninformatie' reeds ervoor gepleit om in aanvulling op het medisch beroepsgeheim voor het PGD een 'patiëntgeheim' in het leven te roepen. Dit beschermt de patiënt tegen de oneigenlijke invloed van politie- en opsporingsdiensten, schade- en levensverzekeraars, financiële instellingen, ICT-bedrijven en andere, al dan niet commerciële partijen die macht kunnen uitoefenen om toegang te krijgen tot de inhoud van het PGD.

## 3.2 Zeggenschap over medische gegevens

Op grond van de WGBO is de hulpverlener verplicht een dossier bij te houden over de patiënt waarmee hij een behandelingsovereenkomst heeft. De patiënt heeft het recht om zijn dossier in te zien en om (eventueel tegen geringe vergoeding) afschrift te vragen van (delen van) het dossier. Er is een voornemen om in de Wet cliëntenrechten zorg (Wcz) een recht van de patiënt

op elektronische toegang tot en afschrift van het medisch dossier op te nemen.

De zeggenschap over medische gegevens die zijn opgenomen in het door de hulpverlener aangelegde medische dossier behoort volgens de RVZ bij de betreffende patiënt te liggen. De Raad heeft meerdere malen bepleit dat de patiënt/burger kan beschikken over al zijn gezondheidsgegevens als hij dat kan en wil, uiteindelijk in de vorm van een levenslang persoonlijk gezondheidsdossier (PGD). Dit biedt mogelijkheden om het medische dossier te integreren in het PGD van de patiënt. Daarvoor moet wel geregeld zijn dat de zorgaanbieder verplicht is gegevens uit het medische dossier aan de patiënt te leveren.

Het wetsvoorstel met regels voor elektronische patiëntendossiers (nummer 33 509) voorziet hierin. Het bepaalt dat 'indien de cliënt verzoekt om inzage of afschrift van het dossier van de desbetreffende cliënt, of van de gegevens betreffende deze cliënt die de zorgaanbieder via een elektronisch uitwisselingssysteem beschikbaar stelt, wordt de inzage of het afschrift op verzoek van de cliënt, met redelijke tussenpozen, door de zorgaanbieder op elektronische wijze verstrekt.' (artikel 15d eerste lid).

## 3.3 Technische standaarden en infrastructuur

Regelingen die voorzien in de toepassing van uniforme technische standaarden ontbreken, zowel op nationaal als op Europees niveau. Dit houdt in dat eenieder die eHealth-toepassingen aanbiedt, zelf bepaalt welke 'standaarden' gebruikt worden. Dit heeft tot gevolg dat systemen niet op elkaar aansluiten c.q. gegevens niet geautomatiseerd kunnen worden uitgewisseld. Dit leidt tot fragmentatie, inefficiëntie, fouten, onnodig dubbel onderzoek, enzovoort. Dit gegeven vormt een fors obstakel voor eHealth, zowel vanuit het perspectief van de zorgverlener als van de patiënt.

Het ontwikkelen van standaarden (interoperabiliteit) wordt momenteel opgepakt door de Europese Commissie (actieplan eHealth 2014-2020).

## 3.4 Standaarden van zorg

Zorgverleners dienen te behandelen overeenkomstig hetgeen onder beroepsgenoten gebruikelijk is (de professionele stan-

daard). Deze standaard is onder meer vastgelegd in protocollen en richtlijnen. In beginsel geldt het uitgangspunt: wat off line geldt, geldt ook online. Er zijn nog weinig specifieke standaarden ontwikkeld voor het toepassen van eHealth. Tot op heden is volgens de standaard eHealth alleen toegestaan in het kader van een reeds bestaande behandelrelatie.

## 3.5 Aansprakelijkheid

De relatie tussen zorgverlener en patiënt wordt in het Nederlands recht beheerst door de Wet op de Geneeskundige Behandelingsovereenkomst. Op grond van deze wet is de zorgverlener verantwoordelijk en aansprakelijk voor al hetgeen in het kader van deze behandelingsovereenkomst plaatsvindt. Deze volledige aansprakelijkheid impliceert dat de zorgverlener (ook) verantwoordelijk en aansprakelijk is voor het handelen van personen die bij de uitvoering van de behandelingsovereenkomst zijn betrokken (zogenaamd hulppersonen) en voor de hulpmiddelen die worden ingezet. Het is om deze reden dat een van de gedragsregels voor artsen is dat eHealth-contacten uitsluitend kunnen plaatsvinden binnen het kader van een reeds bestaande behandelovereenkomst. Wil de zorgverlener verantwoordelijk en aansprakelijk kunnen zijn voor hulpmiddelen, zoals eHealth applicaties, dan moet hij de kwaliteit en betrouwbaarheid ervan immers kunnen kennen en kunnen beoordelen.

Hoewel deze uitgebreide (en niet uit te sluiten) aansprakelijkheid de zorgvrager in de Nederlandse situatie een hoog beschermingsniveau biedt vormt het tegelijkertijd een obstakel voor de verdere implementatie van eHealth. De ontwikkeling van consumer driven eHealth brengt met zich mee dat zorgverleners steeds vaker geconfronteerd worden met 'ad hoc' vragen om advies, zonder dat (reeds) sprake is van een behandelingsovereenkomst. Hierbij wordt de zorgverlener geconfronteerd met gegevens die de zorgvrager zelf heeft gegenereerd met behulp van een door hem aangeschaft elektronisch hulpmiddel. Omdat het geven van raad of advies onder de reikwijdte van de WGBO valt, zal de zorgverlener, teneinde te kunnen voldoen aan de verplichtingen die deze wet stelt, geneigd zijn 'van voren af te beginnen', onderzoek te herhalen etcetera. De zorgvrager zal hierdoor geneigd zijn heil elders te zoeken. Commerciële (buitenlandse) aanbieders springen hierop in. Zo heeft bijvoorbeeld Google het voornemen om medische apps en andere eHealth-diensten op de markt te zetten, met in de backoffice door hen

gecontracteerde artsen, die bijpassende adviezen kunnen geven. Deze commerciële aanbieders zullen veelal elke vorm van aansprakelijkheid uitsluiten. Bovendien is er geen garantie dat de artsen die zij achter de hand hebben bevoegd en bekwaam zijn.

Als we in Nederland geen passende aansluiting vinden op deze ontwikkeling missen we niet alleen de boot, maar zijn zorgvragers ook aanzienlijk minder goed beschermd dan mogelijk is.

*Oplossingsrichting: Overeenkomst van geneeskundig advies*
Een oplossingsrichting voor dit probleem is het ontwerpen van een lichtere variant op de geneeskundige behandelingsovereenkomst voor eHealth-diensten, met een bijbehorend lichter aansprakelijkheidsregime; een 'overeenkomst van geneeskundig advies'. Dit moet het mogelijk maken dat de zorgverlener op basis van door de zorgvrager aangeleverd (onderzoeks)materiaal kan inspelen op diens ad hoc en/of incidentele adviesvragen, zonder verantwoordelijk te zijn voor het (onderzoeks)materiaal en de hulpmiddelen die gebruikt zijn om dat te verkrijgen.

Uiteraard moet voor zorgvragers te allen tijde duidelijk zijn of de overeenkomst die zij met een zorgverlener aangaan een geneeskundige behandelingsovereenkomst is (waarvoor laatstgenoemde volledig aansprakelijk is) dan wel een 'overeenkomst van geneeskundig advies' (waarvoor de zorgverlener beperkt aansprakelijk is). Dit kan bereikt worden door zorgverleners te verplichten bij het ingaan op een advies(aan)vraag de aansprakelijkheidsclausule kenbaar te maken (vergeleken verplichting voor opdrachtgevers en - nemers om Algemene voorwaarden kenbaar te maken).

Om te voorkomen dat door de introductie van een lichtere variant naast de bestaande geneeskundige behandelingsovereenkomst het beschermingsniveau van zorgvragers afneemt, zijn voorts aanvullende maatregelen nodig: zie onder punt 6 en 7.

## 3.6 Jurisdictie en rechtsmachtconflicten

In geval van grensoverschrijdende geschillen in relatie tot de toepassing van eHealth is zowel voor patiënten als voor zorgverleners onvoldoende duidelijk welk recht van toepassing is. Wanneer bijvoorbeeld een arts in het buitenland gevestigd is, kan deze als voorwaarde voor de dienstverlening bepalen dat de overeenkomst onderworpen is aan het recht van het land waarin

hij, de arts, gevestigd is. Dat kan ten nadele van de zorgvrager zijn, wanneer het beschermingsniveau van zorgvragers in het land waarin de dienstverlener (in casu de arts) gevestigd is lager is dan in Nederland. Binnen de EU is dit probleem opgelost met het *Verdrag inzake het recht dat van toepassing is op verbintenissen uit overeenkomst (Verdrag 80/934/EEG.* Op grond van dit verdrag kan de zorgvrager/patiënt dwingende bepalingen die te zijner bescherming zijn opgenomen in het recht van het land waar hij zijn gewone verblijfplaats heeft inroepen. Dit betekent dat de consument/patiënt een beroep kan doen op de rechten die voor hem voortvloeien uit de WGBO. Het betekent ook dat de arts, zelfs wanneer hij in het buitenland is gevestigd, aansprakelijkheid voor een tekortkoming zijnerzijds niet kan uitsluiten of beperken.

Vanuit de zorgvrager bezien is een probleem dat de reikwijdte van dit verdrag begrensd is tot de lidstaten van de EU. Wanneer zorgvragers eHealth-diensten betrekken van daarbuiten gevestigde aanbieders is onduidelijk welk recht (en dus welk beschermingsniveau) van toepassing is op de overeenkomst.

*Oplossingsrichting: Uitbreiding reikwijdte verdrag inzake rechtsmacht (ad 6):* Dit onderwerp zou geagendeerd kunnen worden voor het Nederlandse EU-voorzitterschap; insteek hiervan zou moeten zijn het openstellen van dit verdrag voor bredere (wereldwijde?) ratificering.

## 3.7 Betrouwbaarheid elektronische hulpmiddelen

Als de zorgverlener in geval van een overeenkomst van geneeskundig advies (zie onder punt 5) niet aansprakelijk is voor gebreken in de gebruikte hulpmiddelen, is het temeer van belang dat de fabrikanten daarvan wel aangesproken kunnen worden voor gebreken. Momenteel geldt dat als een medische app gebruikt wordt voor diagnostiek of therapie het volgens de wet een medisch hulpmiddel is. In dat geval is de Richtlijn Medische Hulpmiddelen (RMH) van toepassing en is een CE-markering verplicht. De meeste medische apps vallen vooralsnog in de minst strenge risicoklasse van de registratie. Dit betekent dat het bedrijf dat de app op de markt brengt, hem zelf mag certificeren door het maken en bijhouden van een technisch dossier, waarin de veiligheid en prestaties van de app worden onderbouwd. Indien de app echter een meetfunctie bevat, dan moet de beoor-

deling daarvan worden verricht door een onafhankelijke 'aangemelde' instantie.

Het gegeven dat het de fabrikant zelf is die kan bepalen of een app een medisch hulpmiddel is en dus een CE-markering behoeft, is een probleem omdat hij zo gemakkelijk toepassing van de wet (en de Europese richtlijn waarop deze gebaseerd is) kan ontlopen. Hij kan bijvoorbeeld stellen dat de app uitsluitend als spel bedoeld is. Uit een marktverkennend onderzoek dat de IGZ in 2013 heeft uitgevoerd naar de mate waarin fabrikanten bekend zijn met de wetgeving, komt naar voren dat dit een reëel probleem is: twee van de twintig onderzochte softwareproducten waren ten onrechte niet als medisch hulpmiddel aangemeld.

Overigens is een probleem dat een CE-markering niet de kwaliteit van het product of klinische relevantie voor het stellen van een bepaalde diagnose garandeert.

*Oplossingsrichting:*
In het kader van het aanstaande Nederlandse EU-voorzitterschap, dat eHealth als topic heeft, zou dit onderwerp geagendeerd kunnen worden om te bezien of aanscherping van de regelgeving mogelijk is. Inzet zou kunnen zijn CE-markering verplicht te stellen voor apps die betrekking hebben op gezondheid en gezondheidsstatus.

Daarnaast kan in Europees verband, in het kader van het Joint Action Plan voor medische hulpmiddelen, onderzocht worden of het toezicht op medische apps beter afgestemd kan worden, waarbij de resultaten van dat toezicht actief openbaar gemaakt worden.

Om de betrouwbaarheid en medische functionaliteit van medische apps te kunnen waarborgen is het verder wenselijk tot een keurmerk te komen.