

Privacybescherming en het elektronisch patiëntendossier

Onderzoek naar een oplossing voor de knelpunten in het huidige
EPD ten aanzien van het recht op privacy

Master Scriptie Rechtsgeleerdheid

Accent Staats- en bestuursrecht

Naam: M.A.C. Cools

ANR: 753355

Examencommissie: mr. A.A.L. Beers en dr. G. Leenknecht

Instelling: Universiteit van Tilburg

Afstudeerzitting: 28 februari 2012, 15.00 - 16.00 uur, PZ 10

Inhoudsopgave

Voorwoord	4
Lijst van afkortingen	5
Samenvatting	7
1 Inleiding	8
1.1 Probleemomschrijving	8
1.2 Onderzoeksdoel	10
1.3 Wetenschappelijke relevantie van de onderzoeksvraag	10
1.4 Maatschappelijke relevantie van de onderzoeksvraag	12
1.5 Methoden	12
1.6 Opzet	12
2 De bescherming van het recht op privacy: een analyse van de knelpunten	14
2.1 Inleiding	14
2.1.1 Juridisch perspectief	14
2.1.2 EPD nader uitgelicht: inrichting van het EPD	18
2.2 Knelpunten in het EPD met betrekking tot het recht op privacy	21
2.2.1 Technische knelpunten	21
2.2.2 Juridische knelpunten	23
2.2.3 Politieke knelpunten	25
2.3 Conclusie	27
3 Privacybescherming in Europees perspectief	30
3.1 Inleiding	30
3.2 Richtlijn nr. 95/46/EG	31
3.3 Aanbeveling R (97) 5 betreffende de bescherming van medische gegevens	33
3.4 Jurisprudentie EHRM: handelen van de overheid ten aanzien van persoonsgegevens	37
3.4.1 Reikwijdte artikel 8 EVRM: Is er een privacyschending?	38
3.4.2 Artikel 8, tweede lid, EVRM: waarborgen tegen misbruik van persoonsgegevens	39

3.5 Oplossing knelpunten: Aanbeveling R (97) 5 en jurisprudentie EHRM inzake bescherming persoonsgegevens	41
3.6 Conclusie	45
4 Een vergelijking met het EPD in België	47
4.1 Inleiding	47
4.2 Decreet Gezondheidsinformatiesysteem	47
4.2.1 Het individueel gezondheidsdossier	49
4.2.2 De verantwoordelijkheid voor het dossier	49
4.2.3 De uitwisseling van gegevens in het operationele systeem	49
4.2.4 Kennisgeving, inzage en verzet	51
4.2.5 Toezichtcommissie	52
4.3 Het eHealth-platform	53
4.3.1 Inrichting	53
4.3.2 Verwijzingsrepertorium	55
4.3.3 Systeem voor end-to-end vercijfering	56
4.3.4 Geïntegreerd gebruikers- en toegangsbeheer	57
4.5 Oplossing knelpunten: Decreet GIS en het eHealth-platform	57
4.5 Conclusie	61
5 Regionale opzet van het EPD	63
5.1 Inleiding	63
5.2 Landelijk vs. regionaal	64
5.3 Onderzoek CBP bij regionale EPD's	66
5.3.1 Bevindingen CBP inzake het recht op privacy	67
5.3.2 Handreiking KNMG, VHN, NHG en KNMP	68
5.4 Oplossing knelpunten: toetsing aan een regionaal EPD	70
5.5 Conclusie	73
6 Conclusies en aanbevelingen	75
6.1 Inleiding	75
6.2 Mogelijke oplossingen	76
6.2.1 Schaalgrootte van het EPD	76
6.2.2 De rol van zorgverzekeraars	76
6.2.3 “Geen bezwaar”-systeem	76
6.2.4 Behandelrelatie	77
6.2.5 Schending van de doelbinding	77

6.2.6 UZI-pas	78
6.2.7 Logging	78
6.2.8 Recht op inzage	78
6.2.9 Recht op vernietiging	79
6.2.10 Toezicht op het EPD	79
6.3 Aanbevelingen	80
 Literatuurlijst	 82
 Jurisprudentielijst	 91

Voorwoord

Voor u ligt mijn scriptie die ik heb geschreven ter afsluiting van de master Rechtsgeleerdheid, accent staats- en bestuursrecht aan de Universiteit van Tilburg. Na ruim vier jaar studie komt hiermee een einde aan mijn studententijd en breekt er een nieuwe werkende stap in mijn leven aan.

Mijn interesse in dit onderwerp is een hele tijd geleden gewekt toen ik in het nieuws las dat de overheid een elektronisch patiëntendossier wilde gaan invoeren. In deze moderne tijd van digitalisering is de invoering van een dergelijk dossier vanzelfsprekend. Voordelen als efficiëntie, vergroting van de kwaliteit van de gezondheidszorg en het bevorderen van de samenwerking met andere zorgverleners worden door een elektronisch patiëntendossier eenvoudig gerealiseerd. Doch bedacht ik me al snel dat de privacy weleens in het geding zou komen. Toen bleek dat de minister ondanks de geuite bezwaren van de Eerste en de Tweede Kamer niettemin wilde overgaan tot invoering van een elektronisch patiëntendossier, was mijn scriptieonderwerp snel bedacht. Er dient een oplossing te komen voor de knelpunten in het elektronisch patiëntendossier met betrekking tot het recht op privacy. Enkel wanneer deze oplossingen zijn gevonden, kan en mag mijns inziens een elektronisch patiëntendossier worden ingevoerd.

Allereerst wil ik mijn begeleider, de heer mr. A.A.L. Beers, bedanken voor het in mij gestelde vertrouwen. In tijden dat ik zat te worstelen met mijn scriptie, heeft hij goede ideeën aangedragen en mij weer op weg geholpen. Daarnaast gaat mijn dank uit naar mevrouw mr. C. Ebbers, werkzaam als privacyconsultant, met wie ik eenmaal van gedachten heb gewisseld over de inhoud van mijn scriptie. Door het stellen van kritische vragen heeft zij ervoor gezorgd dat ik een andere blik op mijn scriptie heb geworpen en de inhoud steeds beter heb gemaakt. Ik wil tevens mijn ouders bedanken. Zij hebben mij vanaf het eerste jaar in mijn studie gestimuleerd en gesteund. Zonder hen zou ik nooit zijn gekomen waar ik nu ben. Tot slot gaat mijn dank uit naar mijn vriendinnen voor het luisteren naar mijn belevenissen gedurende het schrijfproces en het geven van tips en ideeën aangaande mijn scriptie.

Miranda Cools

Tilburg, februari 2012

Lijst van afkortingen

BIG	Registratie Beroepsbeoefenaars in de Individuele Gezondheidszorg
BSN	Burgerservicenummer
BW	Burgerlijk Wetboek
CBP	College bescherming persoonsgegevens
CBPL	Commissie voor de Bescherming van de Persoonlijke Levenssfeer
CHP	Centrale Huisartsen Post
CIBG	Centraal Informatiepunt voor Beroepen in de gezondheidszorg
CPI	Centrale Patiëntenindex
CvM	Comité van Ministers
Decreet GIS	Decreet Gezondheidsinformatiesysteem
DigiD	Digitale Identiteit
EHRM	Europees Hof voor de Rechten van de Mens
eNik	Elektronische Nederlandse Identiteitskaart
EPD	Landelijk elektronisch patiëntendossier voor zorgaanbieders
EVRM	Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
IGZ	Inspectie voor de Gezondheidszorg
INSZ	Identificatienummer van de sociale zekerheid
IVBPR	Internationaal Verdrag inzake burgerrechten en politieke rechten
FG	Functionaris voor de gegevensbescherming
KNMP	Koninklijke Nederlandse Maatschappij ter bevordering der Pharmacie
KSZ	Kruispuntbank van de Sociale Zekerheid
LHV	Landelijke Huisartsen Vereniging
LSP	Landelijk Schakelpunt
NHG	Nederlands Huisartsen Genootschap
Nictiz	Nederlands ICT Instituut in de Zorg
NVZA	Nederlandse Vereniging van Ziekenhuisapothekers
OZIS	Open Zorg Informatie Systeem
RSP	Regionaal Schakelpunt
Spitz-MH	SchakelPunt Informatie Transmurale Zorg Midden-Holland
SZC	Servicecentrum Zorg Communicatie
UZI-pas	Unieke Zorgverleners Identificatie-pas
VHN	Vereniging Huisartsenposten Nederland
VWEU	Verdrag betreffende de werking van de Europese Unie

VWS	Volksgezondheid, Welzijn en Sport
VZZ	Vereniging van Zorgaanbieders voor Zorginformatie-uitwisseling
Wbp	Wet bescherming persoonsgegevens
Wet BIG	Wet op de beroepen in de individuele gezondheidszorg
WGBO	Wet op de geneeskundige behandelingsovereenkomst
WVP	Wet Verwerking Persoonsgegevens
WvSr	Wetboek van Strafrecht

Samenvatting

In deze scriptie heb ik een oplossing proberen te vinden voor de knelpunten die het huidige elektronisch patiëntendossier bevat ten aanzien van het recht op privacy. De invoering van een elektronisch patiëntendossier kent een lange en spannende weg. Het wetsvoorstel tot wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatie-uitwisseling in de zorg - waarmee zorg werd gedragen voor een landelijke uitwisseling van patiëntgegevens- stuitte al snel op de nodige kritiek van de Eerste en Tweede Kamer, het College bescherming persoonsgegevens en de zorgsector. De privacy van patiënten zou nog te veel in het geding zijn. Door middel van het private doorstartmodel, waarmee de invoering van een elektronisch patiëntendossier regionaal wordt geregeld door de zorgsector, tracht minister Edith Schippers van Volksgezondheid, Welzijn en Sport op dit moment tegemoet te komen aan alle kritiek. Het overlaten van het patiëntendossier aan private partijen zorgt er echter niet voor dat de knelpunten met betrekking tot het recht op privacy worden opgelost. Het elektronisch patiëntendossier kan en mag alleen worden ingevoerd indien een juridisch kader wordt neergezet met duidelijke rechten en plichten voor zowel de patiënt als de zorgverleners. In deze scriptie heb ik middels de aanbevelingen van de Raad van Europa, de jurisprudentie van het EHRM betreffende de bescherming van medische gegevens, een vergelijking met het elektronisch patiëntendossier in België en een regionale uitwisseling van patiëntgegevens een juridisch kader neergezet voor het elektronisch patiëntendossier waarin het recht op privacy volledig wordt gewaarborgd. Hierbij draag ik zowel organisatorische, technische als juridische oplossingen aan.

1 **Inleiding**

1.1 Probleemomschrijving

In het huidige digitale tijdperk wordt het moeilijker om persoonlijke informatie ook echt privé te houden. Steeds meer persoonsgebonden gegevens worden in digitale bestanden opgeslagen. Het zicht op het beheer en gebruik van deze gegevens is beperkt, terwijl de hoeveelheid data en het aantal instanties dat gegevens verzamelt snel is toegenomen. De bescherming van de privacy lijkt hiermee op losse schroeven te staan. De toenemende automatisering schrikt de overheid echter niet af, maar leidt juist tot een aandringen om wetgeving te realiseren voor de toegang tot digitale informatie om verdieping en verbreding van uitwisseling van gegevens te verbeteren. Zo is op 20 mei 2008 het wetsvoorstel tot wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatie-uitwisseling in de zorg ingediend, dat op 19 februari 2009 is aangenomen door de Tweede Kamer. Dit wetsvoorstel schept de kaders voor het landelijk elektronisch patiëntendossier voor zorgaanbieders (EPD).¹ Het EPD is niet één landelijk dossier, maar een stelsel voor het uitwisselen van gegevens. Hierdoor zijn bepaalde medische gegevens van een patiënt altijd beschikbaar en hoeven de gegevens maar één keer ingevoerd te worden. Ziekenhuizen, huisartsen en andere zorgverleners kunnen zo de actuele gegevens van een patiënt vanuit het hele land opvragen en inzien. Naast de talrijke regionale EPD's die al bestaan, zou door invoering van een landelijk EPD de kans op medische missers worden verkleind, aangezien de arts veel sneller kan achterhalen wat de voorgeschiedenis is van een patiënt. Om vast te stellen van welke patiënt het EPD is, wordt gebruik gemaakt van het burgerservicenummer (BSN) in de zorgsector. De zorgaanbieders zijn verplicht zich aan te sluiten bij het Landelijk Schakelpunt (LSP), dat een overzicht bevat van alle zorgaanbieders die een behandelrelatie met een patiënt hebben. Medische gegevens kunnen dan door de ene zorgaanbieder opgevraagd worden bij de andere zorgaanbieder.² Tevens is de zorgaanbieder gehouden medische gegevens van de patiënt in het EPD vast te leggen en te verstrekken, tenzij de patiënt daartegen bezwaar heeft gemaakt. Als er geen bezwaar wordt gemaakt door de patiënt, zijn de gegevens vrij verkrijgbaar voor de zorgaanbieders. De invoering van het EPD met overheidssteun en een voorziene specifieke wettelijke regeling kwam er echter niet, daar alle fracties in de Eerste Kamer op 5 april 2011 tegen het wetsvoorstel stemden.³

Na het afschieten van het EPD in de Eerste Kamer gaf Minister Edith Schippers van Volksgezondheid, Welzijn en Sport (VWS) het Nederlands ICT Instituut in de Zorg (Nictiz), eigenaar van de restanten

¹ *Kamerstukken II 2007/08*, 31 466, nr. 3, p. 1.

² *Kamerstukken II 2007/08*, 31 466, nr. 3, p. 1-2.

³ *Kamerstukken I 2010/11*, 31 466, nr. Y, p. 1-2.

van het EPD, de opdracht om de mogelijkheden van een doorstart te onderzoeken op basis van een private samenwerking tussen huisartsenorganisaties LHV, VHN, NHG en de apothekerskoepels KNMP en NVZA. Dit voorstel werd ‘Servicecentrum voor Zorgcommunicatie’ (SZC) genoemd.⁴ Hoewel de zorgverleners van mening zijn dat het SZC tegemoet komt aan de wensen van de Eerste Kamer, heeft het College bescherming persoonsgegevens (CBP) in zijn uitgebrachte zienswijze bezwaren gemaakt.⁵ Daarnaast is de doorstart van het EPD naar een SZC in de Tweede Kamer op veel weerstand gestuit. Juist de overheid dient verantwoordelijk te zijn voor de veiligheid en bescherming van de privacy van de burger, nu alleen door middel van overheidsfinanciering of bemoeienis toezicht vorm kan krijgen. Dit leek echter onder een beperkt budget bij een private doorstart van het EPD onmogelijk.⁶ Op 8 november 2011 kwam dan ook een einde aan het SZC.⁷ Hiermee leek het einde van de zoveelste poging om tot invoering van een systeem voor elektronische gegevensuitwisseling in de zorg te komen een feit.

Maar niets is minder waar. Op 10 november 2011 spoorden VVD, CDA en PvdA de regering bij motie aan een doorstart van het EPD te stimuleren: “Het naar de prullenbak verwijzen van infrastructuur die klaar is voor gebruik, is een ongewenste stap achteruit met het oog op de kwaliteit van de zorg, die de zorgsector terugvoert naar het papieren tijdperk.”⁸ Op 8 december 2011 liet de minister per brief aan de Eerste Kamer weten, dat de zorgsector zich toch nog heeft verenigd om het benodigde geld bijeen te krijgen voor de private doorstart van het EPD. Hoewel de minister eerder zei haar handen van het EPD af te trekken en eventuele nieuwe initiatieven aan de zorgsector over te laten, stelt ze nu niet alleen 2,2 miljoen euro ter beschikking, maar blijft ze tevens Nictiz subsidiëren in diverse taken rond het EPD.⁹ Uitgangspunt van het private doorstartmodel is dat zorgverleners in de regio patiëntgegevens gaan uitwisselen. Indien gegevens van patiënten daarom vragen, kunnen zij landelijk door zorgverleners worden uitgewisseld. Met ingang van 2013 zullen zorgverzekeraars deelname aan het LSP verplicht gaan stellen.¹⁰ De minister zegt met de doorstart van het private landelijke EPD tegemoet te komen aan de wensen van de Tweede Kamer om het LSP te behouden. Het CBP ziet met de private doorstart tevens geen bezwaren voor de privacy van patiënten, maar houdt nog wel een slag om de arm en wijst erop dat het oordeel alleen over de voorstellen gaat en niet over de praktijk.¹¹ De Eerste Kamer is echter van oordeel dat het doorstartmodel wel risico’s oplevert met betrekking tot privacyschendingen. De Eerste Kamer heeft op 29 november 2011 dan ook aan de minister laten

⁴ *Handelingen II 2010/11*, 84, p. 51.

⁵ *Zienswijze over doorstartmodel voor landelijke uitwisseling medische gegevens* (zienswijze van 9 augustus 2011), Den Haag: College bescherming persoonsgegevens 2011.

⁶ *Kamerstukken II 2010/11*, 27 529, nr. 73.

⁷ *Handelingen II 2010/11*, 8 november 2011, p. 1.

⁸ *Kamerstukken II 2011/12*, 33 000 XVI, nr. 39.

⁹ Brief van de minister van VWS aan Eerste Kamer, ‘Stand van zaken digitale gegevensuitwisseling in de zorg na aanvaarding van de motie Mulder c.s.’, *MEVA/ICT-3096140* 8 december 2011, p. 1.

¹⁰ Brief VVZ i.o. aan de minister van VWS, 8 december 2011, p. 1.

¹¹ Brief CBP aan VVZ, ‘Doorstart landelijke infrastructuur’, 18 januari 2012, p. 1-2.

weten enkel voorstander te zijn van een regionale gegevensuitwisseling.¹² Het nieuwe voorstel van de zorgsector gaat evenwel uit van een landelijke uitwisseling van gegevens, waardoor de Eerste en de Tweede Kamer lijnrecht tegenover elkaar komen te staan.

1.2 Onderzoeksdoel

Door het wetsvoorstel tot wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatie-uitwisseling in de zorg en het daaropvolgende private doorstartmodel is er gewezen op de noodzaak medische gegevens vast te leggen om een einde te maken aan de gebrekkige informatieoverdracht tussen zorgverleners, waardoor medische missers worden verkleind.¹³ Hoewel het landelijke EPD in de Eerste Kamer werd afgewezen, wil de minister nu de infrastructuur doorzetten in de vorm van het private doorstartmodel.¹⁴ De Eerste Kamer is echter van mening dat een landelijk EPD geen waarborg biedt voor de privacy van patiënten. Er dient een juridisch kader te worden geschapen, met duidelijke rechten en plichten voor zowel de patiënt als de zorgaanbieder.¹⁵ Mijn onderzoek heeft dan ook als doel een oplossing te vinden voor de knelpunten die het huidige EPD bevat ten aanzien van het recht op privacy. Deze oplossing zal bestaan uit een aanbeveling. Dit leidt tot de volgende onderzoeksvraag:

Hoe dienen de knelpunten die het huidige EPD bevat ten aanzien van het recht op privacy te worden opgelost zodat het niet meer in strijd is met het recht op privacy?

1.3 Wetenschappelijke relevantie van de onderzoeksvraag

De invoering van het EPD kent een lange weg: toenmalig minister Els Borst van VWS heeft in 1998 al vastgesteld dat er een EPD zou moeten komen. Minister Edith Schippers is na Els Borst, Hans Hoogervorst en Ab Klink de vierde minister die zich met het EPD bezighoudt. Maar veertien jaar later heeft de Eerste Kamer het wetsvoorstel unaniem verworpen: het EPD bewaakt de privacy van patiënten niet goed.¹⁶ Dat de noodzaak voor invoering van een EPD groot is, blijkt wel uit het vele werk dat veertien jaar lang in het EPD is gestopt. Het is dé manier om te zorgen voor een snelle informatieoverdracht tussen zorgverleners zodat de kans op medische missers wordt verkleind.¹⁷ Vandaar ook de vasthoudendheid van minister Edith Schipper van VWS, die na het EPD fiasco zorgverleners opdracht heeft gegeven om de mogelijkheden van een doorstart te onderzoeken op basis

¹² Kamerstukken I 2010/11, 31 466, nr. Y, p. 1-2.

¹³ Kamerstukken II 2007/08, 31 466, nr. 3, p. 1-2.

¹⁴ Brief van de minister van VWS aan Eerste Kamer, 'Stand van zaken digitale gegevensuitwisseling in de zorg na aanvaarding van de motie Mulder c.s.', MEVA/ICT-3096140 8 december 2011, p. 1.

¹⁵ Kamerstukken I 2010/11, 31 466, nr. Y, p. 1-2.

¹⁶ Kamerstukken I 2010/11, 31 466, nr. Y, p. 1-2.

¹⁷ Kamerstukken II 2007/08, 31 466, nr. 3, p. 1-2.

van een private samenwerking. De minister heeft op 8 december 2011 laten weten het private EPD te ondersteunen.¹⁸ De Eerste Kamer acht het landelijk uitwisselen van patiëntgegevens via het LSP echter onwenselijk. Zij is van mening dat de privacy van patiënten nog te veel in het geding komt.¹⁹ De rechten van de patiënten in Nederland wier persoonsgegevens en medische gegevens zijn vastgelegd in een EPD zijn gecodificeerd op internationaal, Europees en nationaal niveau.²⁰ Zo is in artikel 10 van de Grondwet en artikel 8 van het EVRM²¹ het recht op bescherming van het privéleven geregeld. Hieronder vallen ook het gebruik en de opslag van medische persoonsgegevens. Daarnaast is het fundamentele recht op eerbiediging van de persoonlijke levenssfeer vastgelegd in artikel 17 van het IVBPR.²² Tevens is er de Europese richtlijn van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.²³ Uit deze privacyrichtlijn van de Europese Unie is de Wet bescherming persoonsgegevens (Wbp) voortgevloeid. In het kader van het recht op het privéleven wordt actieve overheidsbemoediging verlangd.²⁴ De verplichtingen die de grond- en mensenrechten aan de overheid opleggen worden onderverdeeld in onthoudingsplichten (negatieve verplichtingen) en prestatieplichten (positieve verplichtingen). De typologie van verplichtingen laat zien hoezeer onthoudingsplichten en prestatieplichten met elkaar verweven zijn. Zo bevat het recht op privacy beide verplichtingen: de plicht voor de overheid om zich niet ongerechtvaardigd te mengen in de privésfeer van de burgers alsmede de verplichting om maatregelen te nemen ter bescherming van de privacy (zoals beveiliging en toezicht op de naleving).²⁵ Waar de overheid aanvankelijk - als trekker van het EPD - vooral haar onthoudingsplicht diende na te leven, dient zij nu met name maatregelen te nemen ter bescherming van de privacy in het private doorstartmodel van het EPD. Het EPD bevat immers nog te veel knelpunten ten aanzien van het recht op privacy. Met dit onderzoek wil ik dan ook de knelpunten die het EPD bevat ten aanzien van het recht op privacy gaan analyseren en met aanbevelingen komen die deze knelpunten oplossen. Nog niet eerder zijn hiervoor concrete aanbevelingen gedaan, waardoor ik met mijn onderzoek een vernieuwende aanpak realiseer om de knelpunten in het EPD aan te pakken zodat het EPD het recht op privacy volledig kan respecteren.

¹⁸ Brief van de minister van VWS aan Eerste Kamer, 'Stand van zaken digitale gegevensuitwisseling in de zorg na aanvaarding van de motie Mulder c.s.', *MEVA/ICT-3096140* 8 december 2011, p. 1-3.

¹⁹ *Kamerstukken I* 2010/11, 31 466, nr. Y, p. 1-2.

²⁰ M. Groothuis, 'Het elektronisch patiëntendossier in een veellagige rechtsorde', in: A.C. Hendriks & H.M.Th.D. Ten Napel (red), *Volksgesondheid in een veellagige rechtsorde*, Alphen a/d Rijn: Kluwer 2007, p. 268.

²¹ Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (1951).

²² Internationaal Verdrag inzake burgerrechten en politieke rechten (1966).

²³ Richtlijn 95/46/EG van de Raad van 23 november 1995 inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. (*PbEG* 1995, L 281).

²⁴ G. Overkleef-Verburg, 'Het grondrecht op eerbiediging van de persoonlijke levenssfeer', in: A.K. Koekkoek (red), *De Grondwet, Een systematisch en artikelsgewijs commentaar*, Deventer: Kluwer 2000, p. 158.

²⁵ A.C. Hendriks, *Gelijke toegang tot de arbeid voor gehandicapten; een grondrechtelijke en rechtsvergelijkende analyse* (diss. Amsterdam UvA), Deventer: Kluwer 2000, p. 51.

1.4 Maatschappelijke relevantie van de onderzoeksvraag

Op dit moment zijn er privacygevoelige gegevens van acht miljoen Nederlanders opgenomen in het LSP.²⁶ Hieruit blijkt dat bijna de helft van alle Nederlanders akkoord is gegaan met opname van eigen patiëntgegevens in het LSP. De voornaamste reden voor het EPD is dat het EPD zorgt voor een snelle gegevensuitwisseling tussen zorgverleners zodat de kans op medische missers wordt verkleind. Veel Nederlanders hebben er echter geen weet van dat het EPD ten aanzien van de bescherming van hun privacy niet waterdicht is: patiëntgegevens van acht miljoen Nederlanders liggen ‘op straat’ doordat het EPD ernstige knelpunten bevat ten aanzien van het recht op privacy. Een oplossing voor deze knelpunten is dus noodzakelijk. In mijn onderzoek wil ik nagaan hoe het EPD kan worden aangepast, opdat het recht op privacy van patiënten wier medische gegevens in een EPD vastliggen compleet wordt gewaarborgd. Met de aanbevelingen die voortvloeien uit mijn onderzoek hoop ik tot een oplossing te komen die er toe strekt de privacy van patiëntgegevens van acht miljoen Nederlanders die op dit moment zijn opgenomen in het EPD te beschermen, zodat deze gegevens niet langer meer ‘op straat’ liggen en een snelle informatieoverdracht van patiëntgegevens tussen zorgverleners kan blijven bestaan.

1.5 Methoden

De methoden die ik in dit onderzoek hanteer zijn literatuuronderzoek, jurisprudentieonderzoek en rechtsvergelijking. Door vergelijking met het EPD in België hoop ik tot nieuwe kennis te komen waardoor het recht op privacy in het Nederlandse EPD volledig wordt gewaarborgd. In het literatuuronderzoek ga ik gebruikmaken van de parlementaire stukken, het advies van het CBP, het advies van de Raad van State, de beschikbare documenten van Nictiz, de beschikbare documenten van de verschillende beroepsgroep- en patiëntorganisaties, literatuur en de geldende wetten en verdragen inzake het recht op privacy. Daarnaast zal ik door middel van onderzoek van de aanbevelingen van de Raad van Europa betreffende de bescherming van medische gegevens en de jurisprudentie van het EHRM inzake het recht op privacy versus het opslaan van medische persoonsgegevens een oplossing proberen te vinden voor de knelpunten in het EPD.

1.6 Opzet

In hoofdstuk 2 ga ik inventariseren in welke opzichten het EPD tekortschiet met betrekking tot het recht op privacy, zodat er een duidelijk beeld ontstaat waar de knelpunten liggen. Alvorens een overzicht van de knelpunten te geven ga ik eerst de geldende nationale en internationale normen

²⁶ *Kamerstukken I* 2010/11, 31 466, nr. V, p. 4.

uiteenzetten met betrekking tot het recht op privacy. Daarna ga ik de werking van het EPD beschrijven, gevolgd door een analyse van de technische, juridische en politieke knelpunten van het EPD in paragraaf 2. In paragraaf 3 volgt een conclusie.

In hoofdstuk 3 ga ik, middels de aanbevelingen van de Raad van Europa betreffende de bescherming van medische gegevens en de jurisprudentie van het EHRM inzake de bescherming van persoonsgegevens, bezien hoe het landelijke EPD anders kan worden ingericht opdat het in overeenstemming is met het recht op privacy. In paragraaf 2 zal ik allereerst kort weergeven of er in de Europese privacyrichtlijn (richtlijn nr. 95/46/EG) speelruimte zit met betrekking tot de knelpunten in het EPD. In paragraaf 3 en 4 zal ik respectievelijk de aanbevelingen van de Raad van Europa en de jurisprudentie van het EHRM uiteenzetten. Vervolgens zal ik in paragraaf 5 nagaan of zij een mogelijkheid bieden tot aanpassing van geïnterpreteerde knelpunten. In paragraaf 6 volgt een conclusie.

In hoofdstuk 4 ga ik in op buitenlandse ontwikkelingen betreffende een landelijk EPD, waarbij ik me zal gaan richten op de ontwikkelingen in België. In paragraaf 2 wordt uiteengezet hoe het Decreet Gezondheidsinformatiesysteem (GIS) is ingericht en in paragraaf 3 zal ik de inrichting van het eHealth-platform gaan bespreken. In paragraaf 4 ga ik onderzoeken of in het Decreet GIS en in het eHealth-platform een oplossing te vinden is voor de geïnterpreteerde knelpunten. In paragraaf 5 volgt een conclusie.

In hoofdstuk 5 ga ik onderzoeken of het recht op privacy beter wordt gegarandeerd door de bestaande regionale EPD's aan te pakken dan door één groot nieuw landelijk EPD op te zetten. In paragraaf 2 ga ik de voor- en nadelen van een regionaal EPD bespreken, voortgekomen uit de discussies in de Eerste en Tweede Kamer en de koepel- en brancheorganisaties van zorgverleners en apothekers. In paragraaf 3 ga ik mij richten op de bevindingen van het CBP inzake de privacy bij regionale uitwisseling van patiëntgegevens. Middels een bespreking van de Handreiking van de KNMG, VHN, NHG en KNMP ga ik onderzoeken waarin de huidige opzet van regionale systemen dient te veranderen, opdat die in overeenstemming is met het recht op privacy. In paragraaf 4 worden de bevindingen gerelateerd aan de geïnterpreteerde knelpunten. In paragraaf 5 volgt een conclusie.

In hoofdstuk 6 zal worden afgesloten met aanbevelingen waarin ik een antwoord geef op de onderzoeksvraag.

2 De bescherming van het recht op privacy: een analyse van de knelpunten

2.1 Inleiding

Hoewel de invoering van het private doorstartmodel een feit is, zijn er nog steeds risico's te vinden voor de privacy van personen wier gegevens in het EPD worden verwerkt. Het EPD is niet in overeenstemming met de geldende nationale en internationale privacynormen, waardoor het EPD strijdig is met de bescherming van de persoonlijke levenssfeer van patiënten.²⁷ Door een ieder inzage te geven in het patiëntendossier kan gemakkelijk misbruik van de gegevens worden gemaakt, zonder dat de patiënt er ook maar enig zicht op heeft. Gevoelige informatie gaat een eigen leven leiden, waardoor de privacy van de burger wordt aangetast. Om het EPD in overeenstemming te brengen met de geldende nationale en internationale privacynormen, is het nodig te inventariseren op welke gebieden het EPD tekortschiet met betrekking tot het recht op privacy, zodat er een duidelijk beeld ontstaat waar de knelpunten liggen.

Allereerst zal ik in paragraaf 2.1.1 de nationale en internationale normen die gelden met betrekking tot het recht op privacy uiteenzetten, waarna ik vervolgens voor een goede begripsvorming de inrichting van het EPD zal gaan bespreken in paragraaf 2.1.2. Nadien zal ik in paragraaf 2.2 overgaan tot een analyse van de knelpunten in het EPD met betrekking tot het recht op privacy. In paragraaf 2.3 volgt een conclusie.

2.1.1 Juridisch perspectief

Volgens het CBP is privacy de gangbare term om te verwijzen naar de mogelijkheid van mensen om ongestoord zichzelf te kunnen zijn. Privacy wordt onderscheiden in fysieke privacy, relationele privacy en informationele privacy.²⁸ Onder fysieke privacy wordt bijvoorbeeld de eerbiediging van het menselijk lichaam en de woning verstaan en bij relationele privacy kan worden gedacht aan de vrijheid om met anderen te communiceren. De bescherming van de informationele privacy, waarop ik mij in dit onderzoek zal richten, heeft betrekking op het recht om zelf te beschikken over de eigen persoonsgegevens en dus ook om zelf te kunnen bepalen wanneer, hoe en in welke mate die gegevens aan anderen beschikbaar worden gesteld.²⁹ Persoonsgegevens zijn kort gezegd alle gegevens over een

²⁷ *Kamerstukken I* 2010/11, 31 466, nr. Y, p. 1-2.

²⁸ A.C.M. de Heij & J.A.G. Versmissen, 'Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid', in: *Achtergrondstudies en verkenningen*, Den Haag: College bescherming persoonsgegevens 2002, p. 10.

²⁹ R.M.S. Doppegieter, 'Regelgeving aangaande informationele en ruimtelijke privacy', *Nederlands Tijdschrift voor Geneeskunde* 1993-137, p. 14.

identificeerbaar natuurlijk persoon.³⁰ Een persoon mag erop rekenen dat zijn persoonsgegevens correct zijn en correct worden gebruikt.³¹ De wet- en regelgeving ter bescherming van persoonsgegevens vindt haar oorsprong in het grondrecht van de burger op eerbiediging van zijn persoonlijke levenssfeer. Dit grondrecht is verankerd in onder meer artikel 8 van het EVRM³² en artikel 10 van de Grondwet. Zowel artikel 8 EVRM als artikel 10 Grondwet heeft horizontale werking en normeert daarom niet alleen de verhouding tussen de overheid en de burger, maar werkt ook door in de rechtsbetrekkingen tussen burgers onderling. In het kader van het recht op het privéleven dient de overheid - als trekker van het EPD - eerst en vooral haar onthoudingsplicht na te leven. Daarnaast heeft zij ook een positieve beschermingsplicht als het gaat om verhoudingen tussen zorgverleners en patiënten. Maar de rol van de overheid in het EPD is echter veranderd, nu zij haar handen van het EPD heeft af getrokken en het heeft overgelaten aan de private partijen. Waar de overheid eerst voornamelijk haar onthoudingsplicht diende na te leven, komt de nadruk nu vooral te liggen op de positieve beschermingsplicht in particuliere verhoudingen. De overheid dient te zorgen dat het recht op privacy in de verhoudingen tussen burgers en private partijen onderling wordt gewaarborgd.³³ Daarnaast is het fundamentele recht op eerbiediging van de persoonlijke levenssfeer vastgelegd in artikel 17 van het IVBPR.³⁴

De uitgangspunten voor de bescherming van persoonsgegevens zijn in Europa vastgelegd in het Verdrag van Straatsburg³⁵ en zijn verder uitgewerkt in de Europese richtlijn van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.³⁶ Uit deze privacyrichtlijn van de Europese Unie is de Wet bescherming persoonsgegevens (Wbp) voortgevloeid. Voor het waarborgen van de rechten van een patiënt wiens gegevens zijn vastgelegd in een EPD is naast de Wbp tevens de Wet op de geneeskundige behandelingsovereenkomst (WGBO) van belang.

De Wbp maakt een onderscheid tussen gewone en bijzondere gegevens. Medische gegevens zijn bijzondere gegevens en verdienen derhalve een adequate bescherming. In artikel 16 Wbp is een verbod opgenomen voor het verwerken van bijzondere gegevens. Het verwerken van bijzondere gegevens behelst alle handelingen, zoals het ordenen, bijwerken, raadplegen, gebruiken, verstrekken en koppelen van de gegevens. Artikel 21 Wbp bevat een uitzondering op artikel 16 Wbp: “het verbod van artikel 16 Wbp is niet van toepassing indien de verwerking geschiedt door hulpverleners,

³⁰ De Heij & Versmissen 2002, p. 31.

³¹ M.J. Bonthuis, ‘Privacy en het landelijk elektronisch patiëntendossier’, *Privacy & Informatie* 2008-3, p. 122.

³² Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (1951).

³³ L.F.M. Verhey, ‘Grondrechten in het digitale tijdperk: driemaal is scheepsrecht?’, *TVCR* 2011, p. 162.

³⁴ Internationaal Verdrag inzake burgerrechten en politieke rechten (1966).

³⁵ Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (1981).

³⁶ Richtlijn 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 23 november 1995 inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. (*PbEG* 1995, L 281).

instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene, dan wel het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is.” Essentiële voorwaarde hiervoor is dat er daadwerkelijk sprake is van het verlenen van zorg of behandeling door de medewerkers van die organisatie.³⁷ Het EPD kan echter niet als een instantie worden aangemerkt die medische gegevens verwerkt met het oog op een goede behandeling of verzorging en zou derhalve op basis van een zwaarwegend algemeen belang onder de uitzondering van artikel 23 Wbp moeten vallen. De algemene bepaling in artikel 23 Wbp regelt dat het verbod in artikel 16 Wbp niet van toepassing is voor zover de verwerking geschiedt met uitdrukkelijke toestemming van de betrokkene (sub a), de gegevens door de betrokkene duidelijk openbaar zijn gemaakt (sub b), dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte (sub c), dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting (sub d) of dit noodzakelijk is met het oog op een zwaarwegend algemeen belang (sub e). De uitzondering van artikel 23 Wbp kan echter slechts worden ingeroepen indien er in het EPD passende waarborgen zijn geboden ter bescherming van de persoonlijke levenssfeer en er met een ontheffingsbeschikking van het CBP wordt gewerkt.³⁸ Zo is er op grond van artikel 8 Wbp toestemming nodig voor deelname aan het EPD. Alvorens tot invoering van het EPD wordt overgegaan, dient aan burgers informatie te worden verschaft over het EPD en over de mogelijkheden om bezwaar te maken ten aanzien van de deelname aan het EPD. Daarnaast stelt de Wbp in de artikelen 33 en 34 regels omtrent de informatieverplichting van de zorgverlener. Het dient voor de patiënt kenbaar te zijn hoe de verwerking van zijn gegevens geschiedt en hoe het beleid voor opslag, bewaren en toegang bij de zorgverlener is ingericht. Zo dient er informatie te worden gegeven over het doel van de verwerking, de categorieën van de te verwerken gegevens, de dossiervorming, de eventuele ontvangers, de bewaar- en vernietigingstermijnen en de mogelijkheden voor bezwaar en beroep.³⁹ Daarnaast heeft de patiënt een aantal eigen rechten. In de artikelen 35 en 36 Wbp is bepaald dat de patiënt mag verzoeken om inzage in en verbetering, aanvulling, verwijdering of afscherming van zijn of haar gegevens. De inzage kan worden geweigerd wanneer dit schadelijk is voor anderen dan de patiënt. Indien er gegevens ontbreken is het recht op aanvulling van belang. De patiënt kan zijn gegevens corrigeren wanneer er gegevens onjuist zijn. Dit recht is niet bedoeld om persoonsgegevens bestaande uit meningen en conclusies waarmee een patiënt het oneens is, te corrigeren. Het heeft slechts betrekking op feiten, zoals naam en geboortedatum, waarover in het algemeen geen verschil van mening kan bestaan. Tevens kunnen patiënten zich op basis van bijzondere persoonlijke omstandigheden tegen een verwerking van hun gegevens verzetten dan wel bepaalde uitwisselingen blokkeren (artikel 40 Wbp). Ingevolge artikel 13 Wbp dient de zorgverlener passende

³⁷ *Zienswijze over doorstartmodel voor landelijke uitwisseling medische gegevens* (zienswijze van 9 augustus 2011), Den Haag: College bescherming persoonsgegevens 2011.

³⁸ Bonthuis 2008, p. 122.

³⁹ M.J. Bonthuis, 'Privacy en het landelijk Elektronisch Patiënten Dossier (EPD). Een onderzoek naar het Landelijk EPD op basis van een juridisch raamwerk van de Wet Geneeskundige Behandelingsovereenkomst, de Wet Bescherming Persoonsgegevens en de NEN 7510', *Advies en Implementatie van het privacyrecht* 2007, p. 8.

beveiligingsmaatregelen te nemen tegen vernietiging en verspreiding op niet toegelaten wijze van de medische gegevens. Het CBP houdt op basis van artikel 51 e.v. Wbp toezicht op de naleving van de Wbp.

De WGBO heeft met name als doel de positie van de patiënt te versterken.⁴⁰ Sinds de inwerkingtreding van de WGBO in 1995 zijn in het Burgerlijk Wetboek (BW) een aantal bepalingen inzake de verwerking van medische persoonsgegevens opgenomen.⁴¹ Artikel 7:450 BW bepaalt dat er toestemming van de patiënt vereist is alvorens tot invoering in het EPD wordt overgegaan. Het bepaalde in artikel 7:454 BW dwingt zorgverleners onder andere tot het voeren van een dossier. Tevens is naast artikel 35 Wbp het recht op inzage in de WGBO vastgelegd (artikel 7:456 BW). Daarnaast heeft de patiënt op grond van artikel 7:455 lid 1 BW het recht dat zijn gegevens al dan niet geheel worden vernietigd. Dit recht kan echter worden beperkt indien het verzoek bescheiden betreft waarvan redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de patiënt (artikel 7:455 lid 2 BW). Het fundament van de vertrouwelijke omgang met patiëntgegevens is echter het beroepsgeheim. Het beroepsgeheim bepaalt dat medische gegevens in beginsel voor anderen dan de patiënt geheim moeten blijven en is geregeld in artikel 7:457 BW.⁴² Het beroepsgeheim is daarnaast wettelijk verankerd in artikel 88 van de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG). Schending van het beroepsgeheim is strafbaar gesteld in artikel 272 van het Wetboek van Strafrecht (WvSr). Het beroepsgeheim bestaat uit een zwijgplicht en een verschoningsrecht. De zwijgplicht dwingt de zorgverlener ertoe dat hij zonder (schriftelijke) toestemming geen informatie mag verstrekken aan anderen dan de patiënt. Het verschoningsrecht is de plicht van de zorgverlener te zwijgen tegenover een derde.⁴³ Het beroepsgeheim kan slechts in bepaalde gevallen en om vooraf bepaalde (zwaarwegende) redenen worden doorbroken. Het gaat daarbij dan om situaties waarin de verstrekking plaatsvindt binnen het behandelteam of als er sprake is van een conflict van plichten.⁴⁴ Er is sprake van een conflict van plichten als een zorgverlener over informatie beschikt die hij vanwege zijn beroepsgeheim niet mag prijsgeven, waardoor een ander zwaarwegend belang in gevaar komt. In de WGBO is in artikel 7:457 BW neergelegd onder welke omstandigheden en onder welke voorwaarden een uitzondering op die geheimhoudingsplicht bestaat. Dit is het geval wanneer er sprake is van toestemming van de patiënt of van een wettelijke verplichting voor de hulpverlener om gegevens te verstrekken (lid 1) of wanneer sprake is van verstrekking aan ‘rechtstreeks bij de uitvoering van de behandelingsovereenkomst betrokkenen’ (lid 2).

⁴⁰ Bonthuis 2008, p. 120.

⁴¹ Groothuis 2007, p. 265.

⁴² Bonthuis 2007, p. 8.

⁴³ Bonthuis 2008, p. 120.

⁴⁴ Bonthuis 2008, p. 120.

2.1.2 EPD nader uitgelicht: inrichting van het EPD

Een zorgverlener verzamelt allerlei gegevens over een patiënt die nodig zijn voor de zorg die hij aan de patiënt verleent. Een deel van de gegevens kan ook van belang zijn voor een andere zorgverlener van de patiënt. Dat deel van de gegevens wordt door de zorgverlener vastgelegd in zijn eigen automatiseringssysteem. Daarnaast vermeldt de zorgverlener in een centrale database, de landelijke verwijsindex, van welke patiënt hij gegevens beschikbaar heeft. Hierbij gaat het uitsluitend om een vermelding, de gegevens zelf blijven bij de zorgverlener. De zorgverlener mag enkel veronderstellen dat de informatie geregistreerd mag worden, indien de patiënt geen bezwaar heeft gemaakt tegen het landelijk uitwisselen van gegevens (opt-out systeem).⁴⁵ Andere zorgverleners kunnen vervolgens in de landelijke verwijsindex nagaan of er relevante informatie over de patiënt beschikbaar is en zo ja, bij welke zorgverlener. Zij kunnen dan de gegevens van de patiënt opvragen door contact te maken met het LSP.⁴⁶

In beginsel krijgt alleen de beroepsbeoefenaar die een behandelrelatie met de patiënt heeft, toegang tot de gegevens van de patiënt.⁴⁷ Daarnaast moet de raadpleging noodzakelijk zijn voor de behandeling van de patiënt en dient de patiënt zijn of haar toestemming te hebben gegeven voor de raadpleging (opt-in). In een spoedsituatie waarin de patiënt niet in staat is om toestemming te geven voor het uitwisselen van gegevens, mag de zorgverlener zonder toestemming medische gegevens opvragen.

Een zorgaanbieder wordt toegang tot het LSP verleend op basis van zijn registratie Beroepsbeoefenaars in de Individuele Gezondheidszorg (BIG). De registratie is gebaseerd op het functieprofiel van de zorgverlener. Daarnaast toetst het LSP de toegang op basis van het autorisatieprofiel. Autorisatie is het verlenen van bevoegdheden tot het verrichten van bepaalde handelingen, zoals het kunnen aanmelden, opvragen of wijzigen van patiëntgegevens.⁴⁸ In het autorisatieprofiel heeft de patiënt aangegeven welke zorgverleners hij geen toegang verleent.⁴⁹ Zorgverleners die niet geregistreerd zijn op basis van de BIG, kunnen patiëntgegevens raadplegen op basis van een mandaat onder verantwoordelijkheid van de beroepsbeoefenaar, de zogenaamde ‘verlengde arm constructie’. Medewerkers die de beschikking hebben over een UZI-pas op naam, bij de uitvoering van hun werkzaamheden patiëntgegevens moeten opvragen of aanmelden bij het LSP en op basis van hun rol niet de juiste bevoegdheden hebben, kunnen voor hun taak gemandateerd worden

⁴⁵ B. Jacobs e.a., ‘Beveiligingseisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Electronisch Patiëntendossier’, rapport in opdracht van VWS uitgevoerd door PriceWaterhouseCoopers, Universiteit Nijmegen, en Universiteit van Tilburg 2008.

⁴⁶ *Kamerstukken II* 2007/08, 31 466, nr. 3, p. 2.

⁴⁷ *Toegang elektronisch patiëntendossier beter geregeld. Behandelrelatie voorwaarde voor toegang dossier*, Den Haag: CBP 2011 (<www.cbpweb.nl/Pages/pb_20080428_toegang_epd.aspx>)

⁴⁸ A. Ekker, *Vertrouwensmodel landelijke infrastructuur voor gegevensuitwisseling*, ID nummer 10041, Nictiz 2010, p. 18.

⁴⁹ Bonthuis 2007, p.23.

door een zorgverlener met de juiste bevoegdheden.⁵⁰ Een mandaatgever kan alleen die bevoegdheden verlenen die hij heeft op grond van de eigen rol. Een apotheker kan dus alleen de bevoegdheden verlenen die bij zijn rol als apotheker horen, en niet de bevoegdheden van een andere rol, zoals die van een huisarts.⁵¹

Om verbinding te krijgen met het LSP hebben zorgverleners een speciale pas nodig, de zogenaamde Unieke Zorgverleners Identificatie (UZI)-pas. Deze pas geeft in combinatie met een persoonlijk wachtwoord zorgverleners toegang tot het LSP, waardoor zij inzage hebben in informatie van andere zorgverleners.⁵² De identificatie van de zorgverlener vindt plaats aan de hand van het UZI-nummer op de UZI-pas. Het UZI-nummer wordt uitgelezen nadat de zorgverlener zijn UZI-pas langs een kaartlezer heeft gehaald en zijn wachtwoord heeft ingevoerd. Tevens authenticiseert het LSP de zorgverlener met de UZI-pas aan de hand van het certificaat van de zorgverlener. Het certificaat is voorzien van de elektronische handtekening van het UZI-register en is alleen toegankelijk wanneer het wachtwoord is ingevoerd. Het Centraal Informatiepunt voor Beroepen in de gezondheidszorg (CIBG) beheert de certificaten en houdt de geldigheid ervan in de gaten.⁵³

Aan de hand van het BSN zoekt het LSP welke zorgverleners medische gegevens over de patiënt hebben. Vervolgens worden deze gegevens opgehaald uit de computers van die zorgverleners en op het scherm van de zorgverlener getoond. Het LSP stuurt de medische gegevens van de patiënt alleen door, de medische gegevens worden niet centraal opgeslagen.⁵⁴

Door logging is achteraf te controleren wie inzage heeft gehad en of deze rechtmatig is geweest.⁵⁵ Via het Klantenloket en Toegang Patiënt krijgen patiënten via het internet de mogelijkheid om loggegevens in te zien, waarbij de naam van de zorgaanbieder en de betreffende beroepsbeoefenaar worden getoond. Indien de patiënt twijfelt aan de rechtmatigheid van een raadpleging of de juistheid van de gegevens in het log, kan hij zich wenden tot de betreffende zorgaanbieder of beroepsbeoefenaar, of tot het Klantenloket. De bewaringstermijn van loggegevens is vijftien jaar, opdat de gegevens kunnen dienen als bewijsmateriaal in een eventuele procedure naar aanleiding van onrechtmatig of strafbaar gebruik van de landelijke infrastructuur. Daarnaast biedt het Klantenloket en Toegang Patiënt de patiënt de mogelijkheid de eigen medische gegevens te raadplegen en bezwaar tegen de uitwisseling van medische gegevens via het EPD in te dienen. Tevens kan op verzoek van de

⁵⁰ Zie <www.informatiepuntepd.nl> (E-learningmodule mandaat).

⁵¹ Ekker 2010, p. 18.

⁵² M.C. Ploem e.a., 'Vertrouwen van zorgverleners in elektronische informatie-uitwisseling en het landelijk EPD. Een juridische en sociaal-wetenschappelijke studie naar de positie van zorgverleners', *AMC/NIVEL* 2011, p. 35.

⁵³ Bonthuis 2007, p.23.

⁵⁴ Zie <www.infoepd.nl> (Wettelijke basis voor het landelijke EPD).

⁵⁵ *Kamerstukken I* 2009/10, 31 466, nr. F, p. 34-35.

patiënt de beheerder van het LSP zorg dragen voor vernietiging van de indexgegevens van de patiënt.⁵⁶

Het toezicht op het EPD vindt plaats door de formele toezichthouders de Inspectie voor de gezondheidszorg (IGZ) en het CBP. De IGZ ziet toe op het leveren van verantwoorde zorg door zorgverleners en houdt vanuit die invalshoek toezicht op het gebruik van het landelijk EPD. Het CBP is op grond van artikel 51 lid 1 Wbp aangewezen als toezichthouder op de verwerking van persoonsgegevens en ziet derhalve ook toe op het voorkomen van misbruik van de gegevens.⁵⁷ Teneinde overlapping van de aan de IGZ en het CBP opgedragen taken of de uitoefening van de toegekende bevoegdheden te voorkomen, hebben de IGZ en het CBP een samenwerkingsconvenant gesloten.⁵⁸ Hierin hebben zij afspraken gemaakt over het uitoefenen van toezicht op de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer binnen de gezondheidszorg in geval van samenlopende bevoegdheden.⁵⁹

In het private doorstartmodel zijn primair de zorgaanbieders zelf verantwoordelijk voor de instandhouding van de netwerken van elektronische gegevensuitwisseling in de zorg.⁶⁰ De infrastructuur van het LSP wordt ingebracht in de Open Zorg Informatie Systeem (OZIS) regio's. Dat zijn zestig samenwerkingsverbanden waarin huisartsenposten met huisartsen samenwerken of apothekers onderling hun gegevens uitwisselen. Daarnaast kan een patiënt aangeven dat zijn gegevens landelijk beschikbaar moeten zijn. De zorgaanbieder is dan verplicht de wens van de patiënt te volgen.

Zorgverleners die gebruik willen maken van de dienstverlening moeten lid zijn van de Vereniging van Zorgaanbieders voor Zorginformatieuitwisseling (VZZ). VZZ zorgt voor het realiseren van een rechtmatige gegevensverwerking en ziet er daarnaast op toe dat de patiënt goed geïnformeerd is over de gegevensverwerking en de verschillende manieren waarop hij zijn rechten kan uitoefenen. Er zal tevens een Gebruikersraad worden ingericht ten behoeve van de reële inspraak van de zorgverleners in de vereniging. De Gebruikersraad zal het bestuur van de vereniging periodiek en ad-hoc adviseren over aangelegenheden betreffende de gegevensverwerking. In een reglement wordt vastgelegd hoe de Gebruikersraad functioneert en namens alle gebruikers het verenigingsbestuur adviseert inzake de gegevensverwerking.

⁵⁶ Jacobs e.a. 2008.

⁵⁷ J.A.L. Krabben, *Toezichtkader EPD: in opdracht van Ministerie van VWS*, 2010-1.1, p. 5.

⁵⁸ *Kamerstukken II* 2006/07, 27 529, nr. 29, p. 9.

⁵⁹ Krabben 2010, p. 18.

⁶⁰ *Doorstartmodel landelijke infrastructuur* (model van 17 juni 2011, V1.0) Nictiz 2011, p. 1.

Het doorstartmodel ging er aanvankelijk vanuit dat de gegevensuitwisseling zonder uitdrukkelijke toestemming van de patiënt zou geschieden.⁶¹ Nictiz verwees daarbij naar de uitzondering in artikel 21 lid 1 sub a Wbp en artikel 7:457 lid 2 BW, waarbij patiëntgegevens mogen worden uitgewisseld zonder uitdrukkelijke toestemming van de patiënt. Het CBP stelt echter dat de uitzonderingen niet gelden voor de VVZ, daar de vereniging zich niet bezig houdt met daadwerkelijke zorgverlening en er geen behandelrelatie tussen de patiënt en de VVZ bestaat.⁶² Om tegemoet te komen aan de eis van het CBP, is in het private doorstartmodel opgenomen dat patiënten hun nadrukkelijke toestemming dienen te geven voor landelijke uitwisseling van hun medische gegevens.⁶³

2.2 Knelpunten in het EPD met betrekking tot het recht op privacy

Deze paragraaf bevat een overzicht van de knelpunten in het EPD met betrekking tot het recht op privacy. Hiertoe wordt gekeken naar het advies van het CBP en naar het advies van de Raad van State ten aanzien van het EPD. Het EPD zal getoetst worden aan de Wbp en de WGBO. Daarnaast zal gekeken worden naar de discussie die in de Tweede Kamer en de Eerste Kamer woedde vanaf het moment dat het wetsvoorstel voor het EPD werd ingediend.⁶⁴ In paragraaf 2.2.1 zal ik stilstaan bij de technische knelpunten, paragraaf 2.2.2 bevat een overzicht van de juridische knelpunten en in paragraaf 2.2.3 zal ik tot slot de politieke knelpunten uiteenzetten.

2.2.1 Technische knelpunten

1) Schaalgrootte van het EPD: meer gegevens beschikbaar en een groot aantal zorgverleners aangesloten.

Bij landelijke uitwisseling van patiëntgegevens is een grote hoeveelheid gegevens via het EPD beschikbaar. Het systeem is omvangrijker en de technologie die daarvoor nodig is complexer, waardoor de kans dat het systeem door technische storingen uitvalt toeneemt. Daarnaast maakt de hoeveelheid gegevens die via het EPD beschikbaar is, het voor hackers interessanter om het systeem te kraken. De kans op inbraak in of anderszins onbevoegde toegang tot de patiëntgegevens zal worden vergroot en de impact daarvan zal toenemen. Bovendien zorgt het grote aantal zorgverleners dat aangesloten zal zijn op het EPD, voor een toename van het risico dat iemand door onzorgvuldigheid toegang krijgt tot patiëntgegevens.⁶⁵

⁶¹ *Doorstartmodel landelijke infrastructuur* (model van 17 juni 2011, V1.0) Nictiz 2011, p. 6.

⁶² *Zienswijze over doorstartmodel voor landelijke uitwisseling medische gegevens* (zienswijze van 9 augustus 2011), Den Haag: College bescherming persoonsgegevens 2011.

⁶³ Brief CBP aan VVZ, 'Doorstart landelijke infrastructuur', 18 januari 2012, p. 1-2.

⁶⁴ O.a. *Kamerstukken II* 2007/08, 31 466, nr. 3, p. 1, *Kamerstukken I* 2010/11, 31 466, nr. Y, p. 1-2.

⁶⁵ Ploem e.a. 2011, p. 53- 65.

2) Het bestaan van een behandelrelatie vormt geen sluitende voorwaarde voor het uitwisselen van patiëntgegevens, wegens onduidelijke beschikbaarheid van de (mede)behandelaar.

Alvorens een zorgverlener patiëntgegevens kan raadplegen, dient er een behandelrelatie te bestaan tussen de zorgverlener en de patiënt. Deze behandelrelatie blijkt uit aanmelding van de patiënt bij het LSP door de zorgverlener. Indien de zorgverlener de patiënt niet bij het LSP heeft aangemeld, wordt de behandelrelatie tussen zorgverlener en patiënt uit de financiële administratie geïmpliceerd. De behandelrelatie is echter niet altijd terug te voeren op historische gegevens. Het uitwisselen van patiëntgegevens binnen het behandelteam zal in de praktijk vaak afhankelijk zijn van de beschikbaarheid van de zorgverlener en de medebehandelaars binnen de gekozen zorginstelling. Vaak is er geen tijd om de precieze betrokkenheid van iedere medebehandelaar vast te leggen. In principe mag een hoofdbehandelaar zonder toestemming van de patiënt een medebehandelaar en medewerker toegang tot de gegevens van de patiënt verlenen, maar in de praktijk is moeilijk per geval vast te leggen wie dat precies zijn.⁶⁶

3) De UZI-pas brengt het risico met zich mee dat onbevoegd patiëntgegevens worden geraadpleegd.

Om verbinding te krijgen met het LSP hebben zorgverleners een UZI-pas nodig, die in principe toegang geeft tot alle landelijke dossiers. Doordat elke zorgverlener een eigen pas heeft, komen er ongeveer 200.000 UZI-passen in omloop en valt niet te voorkomen dat passen verloren raken of gestolen worden. Zorgverleners zijn immers niet getraind in een zorgvuldige omgang met logins, wachtwoorden, UZI-passen en authenticatie van patiënten, waardoor er een groot risico ontstaat dat medische gegevens van patiënten onbevoegd worden geraadpleegd.⁶⁷

4) Door logging achteraf wordt onbevoegde toegang tot een patiëntendossier niet altijd voorkomen.

Om bovengenoemd misbruik van de UZI-pas te voorkomen, wordt in het EPD gebruik gemaakt van logging achteraf waardoor mogelijk misbruik al plaatsgevonden heeft. Maar het is juist noodzakelijk een rechtmatige toegang tot patiëntendossiers te bewerkstelligen en mogelijk misbruik te voorkomen, in plaats van achteraf vast te stellen. Tevens is het bij logging achteraf ondoenlijk om alle loggegevens standaard te controleren, waardoor evaluatie van deze gegevens vaak alleen plaats vindt als er een vermoeden is van onbevoegde toegang tot een patiëntendossier.⁶⁸ Misbruik van inzage in patiëntendossiers wordt derhalve niet in alle gevallen ontdekt, maar slechts wanneer er een vermoeden van misbruik bestaat.

⁶⁶ Bonthuis 2008, p. 121.

⁶⁷ Ploem e.a. 2011, p. 37.

⁶⁸ Ploem e.a. 2011, p. 31.

2.2.2 Juridische knelpunten

1) Uitholling van artikel 7:457 BW wegens logging achteraf op bestaan van behandelrelatie.

Formeel hebben enkel zorgverleners met een behandelrelatie recht op inzage in de patiëntgegevens. Desalniettemin bestaat de mogelijkheid voor zorgverleners die rechtstreeks zijn betrokken bij de behandeling dit recht tevens uit te oefenen, aangezien technische controles vooraf op het wel of niet bestaan van de behandelrelatie ontbreken. In plaats van de behandelrelatie onderdeel uit te laten maken van het autorisatieproces, worden in het EPD logging van de transacties van de behandelaar en controle daarop voldoende geacht om misbruik te voorkomen.⁶⁹ Hierdoor kan pas achteraf gecontroleerd worden of een hulpverlener die een dossier heeft geraadpleegd, een behandelrelatie heeft met de desbetreffende patiënt. Dit is gezien de WGBO niet toelaatbaar en betekent tevens een uitholling van het beroepsgeheim.⁷⁰

2) Logging achteraf op bestaan van behandelrelatie biedt onvoldoende beveiliging en is derhalve strijdig met artikel 13 Wbp.

Op grond van artikel 13 Wbp wordt een passend beveiligingsniveau verlangd bij de verwerking van persoonsgegevens. Naarmate de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens.⁷¹ Een passend beveiligingsniveau in de zin van de Wbp impliceert dat slechts medische gegevens kunnen worden verwerkt voor een specifieke behandeling van een specifieke patiënt.⁷² Het is dus van belang dat duidelijk vaststaat wie deze gegevens feitelijk mag en kan verwerken en dat de te verwerken gegevens noodzakelijk zijn voor de behandeling van de patiënt. Deze garantie kan echter niet worden geboden, nu in het EPD logging achteraf van de transacties van de behandelaar en controle daarop voldoende worden geacht om misbruik te voorkomen.⁷³

3) “Geen bezwaar”-systeem is in strijd met artikel 7:457 BW wegens het ontbreken van uitdrukkelijke toestemming van de patiënt.

In het EPD is het zogenoemde "geen bezwaar"-systeem opgenomen inhoudende dat de zorgverlener verplicht is om medische gegevens van de patiënt in het EPD vast te leggen en te verstrekken, tenzij

⁶⁹ *Kamerstukken II 2007/08*, 31 466, nr. 3, p. 26.

⁷⁰ Advies d.d. 22 november 2007, *Kamerstukken II 2007/08*, 31466, nr. 4.

⁷¹ Wet bescherming persoonsgegevens, toelichting, *Kamerstukken II 1997/98*, 25 892, nr. 3, p 99.

⁷² Advies d.d. 22 november 2007, *Kamerstukken II 2007/08*, 31466, nr. 4.

⁷³ Advies d.d. 22 november 2007, *Kamerstukken II 2007/08*, 31466, nr. 4.

de patiënt daartegen bezwaar heeft gemaakt (de zogenaamde opt-outmogelijkheid). Hiermee geeft de patiënt pas achteraf toestemming voor het opnemen van zijn medische gegevens in het EPD. Volgens de toelichting op het wetsvoorstel zou de beoogde werking van het EPD ernstig belemmerd worden indien de zorgverlener, die over de benodigde medische gegevens beschikt, alsnog uitdrukkelijke toestemming van de patiënt dient te verkrijgen om diens gegevens aan andere zorgaanbieders te verstrekken.⁷⁴ Het wetsvoorstel beroept zich met het “geen bezwaar”-systeem op de uitzondering van artikel 7:457, eerste lid, derde volzin, BW dat bij of krachtens de wet kan worden afgeweken van de eisen (de toestemming) die in het eerste lid aan de verstrekking van medische gegevens worden gesteld. In het EPD wordt de uitzondering van artikel 7:457, eerste lid, derde volzin, BW verheven tot regel.⁷⁵

4) Gegevensuitwisseling past niet binnen de reikwijdte van het noodzakelijkheidsvereiste ingevolge artikel 7:457, tweede lid, BW.

De gegevensuitwisseling moet ingevolge artikel 7:457, tweede lid, BW noodzakelijk zijn voor de uitvoering van de behandelovereenkomst. Tevens mag de gegevensverwerking niet bovenmatig zijn (artikel 11, eerste lid, Wbp). Dit impliceert dat slechts die medische gegevens worden verstrekt die relevant zijn voor de behandeling in verband waarmee toegang tot het dossier wordt gevraagd: de gegevensuitwisseling moet beperkt zijn. Het is echter niet te garanderen dat zorgaanbieders ook daadwerkelijk slechts de gegevens opvragen die noodzakelijk zijn voor een goede behandeling van de patiënt. Het is dan ook denkbaar dat een situatie ontstaat waarin de gegevens die via het landelijk EPD worden uitgewisseld voor andere doeleinden worden gebruikt dan oorspronkelijk was bedoeld.⁷⁶

5) Patiënt kan recht op inzage niet uitoefenen wegens het ontbreken van een toegangsmiddel: in strijd met artikel 35 Wbp en artikel 7:456 BW.

Op grond van artikel 7:456 BW en artikel 35 Wbp verstrekt de hulpverlener aan de patiënt zo spoedig mogelijk inzage in en afschrift van de bescheiden. De minister heeft allereerst getracht de patiënt zijn recht op inzage in het EPD te laten uitoefenen middels een elektronische Nederlandse Identiteitskaart (eNik).⁷⁷ De eNik kwam er echter niet en de minister wilde inzage vervolgens mogelijk maken via DigiD met sms-authenticatie. Dit bleek volgens experts te onveilig te zijn, waarna de minister vervolgens het voorstel heeft gedaan dat zorgverleners zelf via hun eigen website of portal inzage

⁷⁴ *Kamerstukken II 2007/08*, 31 466, nr. 3, p. 7.

⁷⁵ Advies d.d. 22 november 2007, *Kamerstukken II 2007/08*, 31466, nr. 4.

⁷⁶ B. Pluut, ‘Het Landelijk EPD als blackbox. Besluitvorming en opinies in kaart’, in: *WRR-Rapport iOverheid*, Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid 2010, p. 40.

⁷⁷ Advies d.d. 22 november 2007, *Kamerstukken II 2007/08*, 31466, nr. 4.

geven in de medische gegevens.⁷⁸ Op dit moment is er echter nog geen toegangsmiddel met een vergelijkbaar beveiligingsniveau voor handen, waardoor de patiënt zijn recht op inzage niet kan uitoefenen. Het recht op inzage in het EPD is derhalve in strijd met artikel 35 Wbp en artikel 7:456 BW.

6) Garantie van volledige vernietiging ontbreekt in een digitaal dossier: in strijd met artikel 36 Wbp en artikel 7:455 BW.

Op grond van artikel 7:455, eerste lid, BW heeft de patiënt het recht om de zorgaanbieder te verzoeken zijn gegevens in het medisch dossier binnen drie maanden al dan niet in hun geheel te vernietigen, tenzij bewaring van aanmerkelijk belang is voor een ander of het BW zich ertegen verzet. In het EPD is het echter onduidelijk wat vernietiging van de patiëntgegevens precies inhoudt. Indien met een verzoek tot vernietiging wordt ingestemd, worden dan de gegevens uit het brondossier verwijderd? Of wordt enkel de landelijke raadpleging van de gegevens onmogelijk gemaakt? En wat gebeurt er in de situatie dat de gegevens die de patiënt vernietigd wil hebben inmiddels door een zorgverlener uit een andere instelling zijn geraadpleegd en aldaar zijn opgeslagen? Worden die met een verzoek tot vernietiging ook verwijderd?⁷⁹ Door de onduidelijkheid ontstaat derhalve het risico dat de gegevens op verzoek van de patiënt zijn verwijderd, terwijl deze gegevens nog op allerlei plaatsen kunnen ‘opduiken’.⁸⁰

2.2.3 Politieke knelpunten

1) Kwaliteit van medische informatie neemt af.

Bij een landelijke uitwisseling van patiëntgegevens wordt het inschatten van de kwaliteit van de gegevens steeds moeilijker. Zorgverleners hebben het idee minder ‘grip’ te hebben op de uitwisseling, omdat de schaalgrootte van uitwisseling toeneemt. De kans dat zorgverleners elkaar persoonlijk kennen is namelijk kleiner dan bij regionale uitwisseling, waardoor zorgverleners hun onderzoeksplicht - inhoudende het onderzoeken of de informatie betrouwbaar is - niet toereikend kunnen uitoefenen. Daarnaast beïnvloedt het inzagerecht tevens de kwaliteit van de informatie. Indien het recht om in het eigen EPD te kijken veel gemakkelijker kan worden uitgeoefend, kan dat gevolgen hebben voor de wijze waarop zorgverleners daarin de relevante medische gegevens optekenen.⁸¹

⁷⁸ *Kamerstukken II* 2010/11, 27 529, nr. 71, p. 20.

⁷⁹ Ploem e.a. 2011, p. 57.

⁸⁰ M.J. Bonthuis, ‘Het EPD en privacy’, *Journal Privacy Gezondheidszorg* 2008-7, p. 3.

⁸¹ Ploem e.a. 2011, p. 52-62 en *Kamerstukken I* 2008/09, 31 466, nr. C, p. 30.

2) Toezicht door CBP en IGZ zorgt voor capaciteitsproblemen.

Het EPD bevat geen specifieke bepalingen voor het toezicht op de naleving van regels door zorgverleners. Dit komt voort uit de gedachte dat hierin al is voorzien via het in de Wbp geregelde toezicht door het CBP en het in gezondheidszorgwetgeving geregelde toezicht door de IGZ. Bij samenlopende bevoegdheden tussen beide instanties zou een samenwerkingsconvenant uitkomst moeten bieden.⁸² Het convenant biedt echter geen oplossing voor de ontstane capaciteitsproblemen. Zo is het onduidelijk wie toezicht - op zowel het niveau van het LSP als de instellingen - dient te houden op de duizenden logs.⁸³

3) De rol van zorgverzekeraars: informatie uit het EPD combineren met andere informatie.

Het doorstartmodel, waarin het LSP wordt gebruikt voor regionale gegevensuitwisseling, wordt naast de zorgaanbieders en het ministerie van VWS tevens gefinancierd door de zorgverzekeraars. De PVV en de SP vrezen dat zorgverzekeraars ongeoorloofd de dossiers van patiënten en cliënten zouden raadplegen wanneer zij meebetalen aan een privaat LSP. Zorgverzekeraars hebben duidelijk gemaakt dat ze alleen contracten afsluiten met zorgverleners die zich aansluiten bij het private doorstartmodel. De kans is dus groot dat de zorgverzekeraars de regie over gaan nemen en in de patiëntgegevens gaan kijken.⁸⁴ Hierdoor ontstaat het risico van 'profiling' (het werken met medische risicoprofielen).⁸⁵

4) "Geen bezwaar"-systeem zorgt voor een ondoorzichtige registratie van gegevens in het EPD.

In het "geen bezwaar"-systeem mag de zorgverlener veronderstellen dat informatie geregistreerd mag worden, indien de patiënt geen bezwaar heeft gemaakt bij de zorgverlener. In het EPD mogen zorgverleners het ontbreken van bezwaar als toestemming opvatten voor het registreren van patiëntgegevens in het EPD. Hierdoor kan het voor patiënten ondoorzichtig worden of en zo ja welke gegevens wanneer in het EPD worden geregistreerd.⁸⁶

5) Inzagerecht van patiënten: risico aanleg "tweede weg" voor achterhalen van patiëntgegevens.

De mogelijkheid voor de patiënt om zelf inzage te krijgen in zijn of haar medische gegevens heeft tot gevolg dat er een "tweede weg" naar informatie uit het EPD wordt aangelegd. Ook al is het informatiesysteem voldoende veilig, indien patiëntgegevens worden ingezien vanaf slecht beveiligde

⁸² *Kamerstukken II* 2006/07, 27 529, nr. 29, p. 9.

⁸³ Ploem e.a. 2011, p. 57.

⁸⁴ M. Chavannes, 'Schipper orkestreert iedereen over de elektronische snelweg', *NRC Handelsblad* 17 december 2011 <www.weblogs.nrc.nl/opklaringen>.

⁸⁵ Pluut 2010, p. 40.

⁸⁶ *Kamerstukken I* 2009/10, 31 466, nr. C, p. 10 en Jacobs e.a. 2008.

computers, ontstaat er toch een risico dat onbevoegden kennis kunnen nemen van de vertrouwelijke medische gegevens of langs die weg in het systeem kunnen breken.⁸⁷

2.3 Conclusie

De invoering van het EPD kan en mag nog niet worden gerealiseerd. Het EPD bevat - zoals weergegeven in de voorgaande (sub)paragrafen - nog uiteenlopende knelpunten met betrekking tot het recht op privacy. Uit de analyse van de technische, juridische en politieke knelpunten is gebleken dat een zekere overlapping is ontstaan met betrekking tot de genoemde aspecten in het EPD. Voor een goede beeld- en begripsvorming zal ik dan ook per aspect kort aangeven wat de technische, juridische en politieke knelpunten zijn. Dit zal ik hieronder uiteenzetten.

Schaalgrootte van het EPD

Door de grote hoeveelheid gegevens die via het EPD beschikbaar zijn en het grote aantal zorgverleners dat aangesloten is op het systeem, zal de kans op onbevoegde toegang tot het systeem toenemen (technisch knelpunt).⁸⁸ Daarnaast zorgt de schaalgrootte voor een afname van de kwaliteit van de medische informatie, aangezien zorgverleners elkaar veelal niet meer persoonlijk zullen kennen en ze hun onderzoeksplicht derhalve niet meer voldoende kunnen uitoefenen (politiek knelpunt).

De rol van zorgverzekeraars

Indien zorgverzekeraars meebetalen aan het private EPD, is de kans groot dat zij de regie over gaan nemen en in de patiëntgegevens gaan kijken. Hierdoor ontstaat het risico van ‘profiling’ (politiek knelpunt).⁸⁹

“Geen bezwaar”-systeem

Het “geen bezwaar”-systeem zorgt voor een ondoorzichtige registratie van gegevens in het EPD, nu zorgverleners het ontbreken van bezwaar als toestemming mogen opvatten voor het registreren van patiëntgegevens in het EPD (politiek knelpunt).⁹⁰ Daarnaast zorgt het systeem voor strijdigheid met artikel 7:457 BW, nu uitdrukkelijke toestemming van de patiënt ontbreekt (juridisch knelpunt).

Behandelrelatie

Het bestaan van een behandelrelatie vormt geen sluitende voorwaarde voor het uitwisselen van patiëntgegevens, wegens de onduidelijke beschikbaarheid van de (mede)behandelaar. De

⁸⁷ Kamerstukken I 2010/11, 31 466, nr. 20, p. 2-20 en Ploem 2011, p. 54-55.

⁸⁸ Ploem e.a. 2011, p. 53- 65.

⁸⁹ M. Chavannes, ‘Schippers orkestreert iedereen over de elektronische snelweg’, *NRC Handelsblad* 17 december 2011 www.weblogs.nrc.nl/opklaringen en Pluut 2010, p. 40.

⁹⁰ Kamerstukken I 2009/10, 31 466, nr. C, p. 10 en Jacobs e.a. 2008.

behandelrelatie is derhalve niet altijd terug te voeren op historische gegevens, aangezien het uitwisselen van patiëntgegevens binnen het behandelteam in de praktijk vaak afhankelijk is van de beschikbaarheid van de zorgverlener en de medebehandelaars binnen de gekozen zorginstelling (technisch knelpunt).⁹¹

Schending van de doelbinding

In het EPD is niet te garanderen dat zorgaanbieders ook daadwerkelijk slechts de gegevens opvragen die noodzakelijk zijn voor “de goede behandeling of verzorging van de patiënt”.⁹² Er ontstaat derhalve het risico dat de gegevens die via het landelijk EPD worden uitgewisseld voor andere doeleinden worden gebruikt dan oorspronkelijk was bedoeld.⁹³ Hierdoor past de gegevensuitwisseling niet binnen de reikwijdte van het noodzakelijkheidsvereiste ingevolge artikel 7:457, tweede lid, BW (juridisch knelpunt).⁹⁴

UZI-pas

Het grote aantal UZI-passen (iedere zorgverlener heeft een eigen pas), in combinatie met de onzorgvuldige omgang van zorgverleners met de passen, zorgt voor een toename van het risico dat onbevoegd patiëntgegevens worden geraadpleegd (technisch knelpunt).⁹⁵

Logging

Gebleken is dat het bij logging achteraf ondoenlijk is om alle loggegevens te controleren. Hierdoor wordt misbruik van inzage in patiëntendossiers niet in alle gevallen voorkomen, maar slechts indien er een vermoeden van misbruik bestaat (technisch knelpunt).⁹⁶ Daarnaast wordt door middel van logging pas achteraf gecontroleerd op het bestaan van een behandelrelatie, waardoor een zorgverlener die geen behandelrelatie heeft met de patiënt toch kan beschikken over de patiëntgegevens. Dit zorgt voor uitholling van artikel 7:457 BW (juridisch knelpunt).⁹⁷ Nu mogelijk misbruik al plaats kan hebben gevonden, biedt logging achteraf onvoldoende beveiliging en is derhalve strijdig met artikel 13 Wbp (juridisch knelpunt).

Recht op inzage

In het EPD is er nog geen toegangsmiddel voorhanden waarmee patiënten hun recht op inzage kunnen uitoefenen, waardoor strijdigheid ontstaat met artikel 35 Wbp en artikel 7:456 BW (juridisch knelpunt). Daarnaast heeft de mogelijkheid voor de patiënt om zelf inzage te krijgen in zijn of haar

⁹¹ Bonthuis 2008, p. 121.

⁹² *Kamerstukken II* 2007/08, 31 466, nr. 3, p. 27.

⁹³ Pluut 2010, p. 40.

⁹⁴ Pluut 2010, p. 40.

⁹⁵ Ploem e.a. 2011, p. 37.

⁹⁶ Ploem e.a. 2011, p. 31.

⁹⁷ Advies d.d. 22 november 2007, *Kamerstukken II* 2007/08, 31466, nr. 4.

medische gegevens, tot gevolg dat er een "tweede weg" naar informatie uit het EPD wordt aangelegd (politiek knelpunt).⁹⁸ Het inzagerecht heeft tevens gevolgen voor de kwaliteit van de patiëntgegevens, nu zorgverleners de relevante medische gegevens anders zullen gaan optekenen (politiek knelpunt).⁹⁹

Recht op vernietiging

In het EPD is het onduidelijk wat het recht op vernietiging van de patiëntgegevens precies inhoudt, waardoor het risico ontstaat dat de gegevens op verzoek van de patiënt zijn verwijderd, terwijl deze gegevens nog op allerlei plaatsen kunnen 'opduiken'.¹⁰⁰ Het ontbreken van de garantie van volledige vernietiging in het dossier is in strijd met artikel 36 Wbp en artikel 7:455 BW (juridisch knelpunt).

Toezicht op het EPD

Indien enkel het CBP en de IGZ toezicht uitoefenen op het EPD, zullen er capaciteitsproblemen gaan ontstaan (politiek knelpunt).¹⁰¹

Om het EPD in overeenstemming te brengen met het recht op privacy dienen de hierboven weergegeven knelpunten te worden opgelost. Het onderzoek daarnaar zal plaatsvinden in de volgende hoofdstukken. In de hoofdstukken 3, 4 en 5 zal ik respectievelijk door middel van de aanbevelingen van de Raad van Europa, de jurisprudentie van het EHRM betreffende de bescherming van medische gegevens, een vergelijking met het EPD in België en een regionale uitwisseling van patiëntgegevens een oplossing proberen te vinden voor de technische, juridische en politieke knelpunten.

⁹⁸ *Kamerstukken I* 2010/11, 31 466, nr. 20, p. 2-20 en Ploem e.a. 2011, p. 54-55.

⁹⁹ Ploem e.a. 2011, p. 52-62 en *Kamerstukken I* 2008/09, 31 466, nr. C, p. 30.

¹⁰⁰ M.J. Bonthuis, 'Het EPD en privacy', *Journal Privacy Gezondheidszorg* 2008-7, p. 3.

¹⁰¹ *Kamerstukken II* 2006/07, 27 529, nr. 29, p. 9 en Ploem e.a. 2011, p. 57.

3 Privacybescherming in Europees perspectief

3.1 Inleiding

De eerste stappen op het gebied van een internationale persoonsgegevensbescherming werden gezet binnen de Raad van Europa.¹⁰² Zo liggen de wortels van de Europese privacybescherming in het in 1981 aanvaarde Verdrag van Straatsburg van de Raad van Europa.¹⁰³ Het Verdrag is een uitwerking van het recht op eerbiediging van het privéleven, vastgelegd in artikel 8 van het EVRM. Naast het vaststellen van de verdragstekst verschenen er aanbevelingen van de Raad van Europa over de bescherming van medische persoonsgegevens. De aanbevelingen van de Raad van Europa hebben geen bindende juridische kracht, maar bevatten wel nuttige elementen voor het eventueel aanpassen of uitbreiden van nationale wetgeving. Na het Verdrag van Straatsburg heeft het EHRM in zijn jurisprudentie de bescherming van persoonsgegevens voor een belangrijk deel onder artikel 8 EVRM gebracht, waardoor tevens uit jurisprudentie van het EHRM een aantal vereisten voor de bescherming van persoonsgegevens valt af te leiden.¹⁰⁴ Daarnaast heeft de grondrechtelijke bescherming van de informationele privacy een belangrijke communautaire dimensie gekregen met de vaststelling van de Europese richtlijn van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.¹⁰⁵ In dit hoofdstuk ga ik dan ook vanuit een internationale invalshoek bekijken of de knelpunten met betrekking tot de privacybescherming in het EPD kunnen worden opgelost.

Allereerst zal ik in paragraaf 3.2 de betekenis van richtlijn nr. 95/46/EG uiteenzetten, waarbij ik in zal gaan op de speelruimte in de richtlijn met betrekking tot de knelpunten in het EPD. In paragraaf 3.3 ga ik over tot een bespreking van de aanbevelingen van de Raad van Europa inzake de bescherming van medische gegevens. In paragraaf 3.4 zal ik de jurisprudentie van het EHRM betreffende de bescherming van persoonsgegevens uiteenzetten. In paragraaf 3.5 zal ik nagaan of de aanbevelingen van de Raad van Europa en de jurisprudentie van het EHRM betreffende de bescherming van persoonsgegevens de mogelijkheid bieden tot oplossing van de geïnterpreteerde knelpunten. In paragraaf 3.6 volgt een conclusie.

¹⁰² H.R. Kranenborg, *Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie. Over de openbaarheid van persoonsgegevens*, (diss. Leiden), Deventer: Kluwer 2007, p. 68.

¹⁰³ Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (1981).

¹⁰⁴ Kranenborg 2007, p. 115.

¹⁰⁵ Richtlijn 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 23 november 1995 inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. (*PbEG* 1995, L 281) en Overkleef-Verburg 2000, p. 170.

3.2 Richtlijn nr. 95/46/EG

In een democratische rechtsstaat is de bescherming van de burger tegen inbreuken op de persoonlijke levenssfeer noodzakelijk. De internationale handel wordt echter afgeremd indien elk land daartoe zijn eigen regels opstelt. Het Europees Parlement verzocht daarom al in 1979 de Europese Commissie een richtlijn op te stellen met het oog op harmonisatie van wetgeving ten aanzien van gegevensbescherming in de lidstaten. Omdat de Europese Commissie eerst wilde nagaan of het Verdrag van Straatsburg tot de gewenste harmonisatie zou leiden, kwam richtlijn nr. 95/46/EG (verder te noemen richtlijn) pas tot stand toen duidelijk werd dat de harmonisatie uit bleef. Op 24 oktober 1995 kwam de richtlijn formeel tot stand.¹⁰⁶ De richtlijn is vastgesteld op grond van artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU) en heeft als doel het bereiken van een evenwicht tussen het vrije verkeer van persoonsgegevens in de EU en een hoog niveau van bescherming van de persoonlijke levenssfeer.¹⁰⁷ De reikwijdte van de richtlijn is beperkt tot geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens. Niet-geautomatiseerde verwerkingen vallen enkel onder de reikwijdte van de richtlijn voor zover zij in een bestand zijn opgenomen of zullen worden opgenomen.¹⁰⁸

De richtlijn bestaat uit een aantal materiële bepalingen omtrent de rechtmatigheidsvoorwaarden voor gegevensbescherming, waarbij een verzaamd regime voor gezondheidsgegevens is opgenomen.¹⁰⁹ Zo mogen de gezondheidsgegevens enkel worden verwerkt ten behoeve van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Hieraan gekoppeld zijn verplichtingen tot dataminimalisatie, zorg voor de kwaliteit van gegevens, terughoudendheid met verdere verwerking en een beveiligingsverplichting.¹¹⁰ Daarnaast moeten de verantwoordelijken zoveel mogelijk transparantie vervullen ten aanzien van de verwerkingen onder hun verantwoordelijkheid. Zo dient er een meldplicht voor verwerkingen te zijn bij het CBP of een Functionaris voor de gegevensbescherming (FG) en dienen zij aan de betrokkene bekend te maken voor welke doeleinden zij gegevens verwerken. Verantwoordelijken hebben tevens een informatieplicht.¹¹¹ Door middel van vaststelling van een gedragscode¹¹² en een FG¹¹³ dienen verantwoordelijken het toezicht op de naleving deels intern te organiseren. Het handhavingsregime gaat uit van toezicht op de naleving door

¹⁰⁶ C. Cuijpers, 'Privacy in context', in: J.M.A. Berkvens & J.E.J. Prins, *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2007, p. 13.

¹⁰⁷ *Kamerstukken I* 2010/11, 32 761, nr. 1, Bijlage Leidraad afstemmen van wetgeving op de Wet bescherming persoonsgegevens, p. 33.

¹⁰⁸ Artikel 3, lid 1 Richtlijn nr. 95/46/EG.

¹⁰⁹ Overkleef-Verburg 2000, p. 170. In de richtlijn is tevens een verzaamd regime opgenomen voor andere gevoelige gegevens. Dit zijn gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsmede gegevens die het seksuele leven betreffen.

¹¹⁰ Artikel 6 Richtlijn nr. 95/46/EG.

¹¹¹ Artikel 10 en 11 Richtlijn nr. 95/46/EG.

¹¹² Artikel 27 Richtlijn nr. 95/46/EG.

¹¹³ Artikel 18 Richtlijn nr. 95/46/EG.

een onafhankelijke toezichthouder die doeltreffend moet kunnen optreden (het CBP in Nederland).¹¹⁴ Voor de betrokkene voorziet de richtlijn in rechten op informatie, inzage en correctie alsmede in een individueel recht van verzet.¹¹⁵ De richtlijn bevat tevens een verbod op grensoverschrijdend gegevensverkeer naar derde landen (niet EU-landen), tenzij een passend niveau van gegevensbescherming kan worden geboden.¹¹⁶

De richtlijn is gericht tot de lidstaten en niet tot particulieren. De richtlijn is namelijk verbindend in al haar onderdelen voor de lidstaten waarvoor zij bestemd is. De lidstaat krijgt derhalve de opdracht om de richtlijn binnen een bepaalde termijn om te zetten in nationale wetgeving (implementatie). De regeling waarin de richtlijn is geïmplementeerd is in Nederland de Wbp. De richtlijn is niet uitgewerkt met de Wbp. Het EPD staat op dit moment echter op gespannen voet met de richtlijn, nu het nog te veel knelpunten bevat met betrekking tot het recht op privacy. Aan de Wbp komt derhalve een bijzondere betekenis toe. Indien een wettelijk voorschrift wordt vastgesteld dat aspecten van de bescherming van persoonsgegevens regelt die onder het bereik van de richtlijn vallen, dient eerst te worden nagegaan of de Wbp het betreffende onderwerp niet reeds regelt. Wanneer wordt afgeweken van de Wbp kan namelijk al snel het risico ontstaan dat in strijd met de richtlijn wordt gehandeld.¹¹⁷ In dat geval moet de rechter het strijdige nationale recht buiten toepassing laten en de richtlijn voorrang verlenen.¹¹⁸ Er dient derhalve nadrukkelijk op te worden gelet dat bij de voorbereiding van wetgeving die betrekking heeft op de bescherming van persoonsgegevens de voorgestelde regeling volledig in overeenstemming is met de richtlijn.¹¹⁹

Indien een richtlijn niet juist, niet op tijd of helemaal niet is geïmplementeerd in de nationale regelgeving kan in een verticale verhouding aan de richtlijn rechtstreekse werking toekomen.¹²⁰ De richtlijn moet hiervoor wel voldoende duidelijk en onvoorwaardelijk zijn. Dit betekent dat de bepalingen precies moeten zijn geformuleerd en geen afwijkingsmogelijkheden voor de lidstaten mogen bevatten.¹²¹ In particuliere verhoudingen is rechtstreekse werking echter niet mogelijk.¹²² De nationale rechter is echter ook verplicht om het nationale recht zoveel mogelijk uit te leggen in het licht van het Europees recht. Dit wordt richtlijnconforme interpretatie genoemd. Het beginsel van conforme interpretatie kan worden beschouwd als een belangrijke aanvulling op het leerstuk van

¹¹⁴ Artikel 28 Richtlijn nr. 95/46/EG.

¹¹⁵ Artikel 12-15 Richtlijn nr. 95/46/EG.

¹¹⁶ Artikel 25 en 26 Richtlijn nr. 95/46/EG.

¹¹⁷ *Kamerstukken I* 2010/11, 32 761, nr. 1, Bijlage Leidraad afstemmen van wetgeving op de Wet bescherming persoonsgegevens, p. 38.

¹¹⁸ HvJ EG 15 juni 1964, nr. 6/64, *Costa/ENEL*, *Jur.* 1964, p. I-1199.

¹¹⁹ *Kamerstukken I* 2010/11, 32 761, nr. 1, Bijlage Leidraad afstemmen van wetgeving op de Wet bescherming persoonsgegevens, p. 32.

¹²⁰ Zie <www.wetenschap.infonu.nl/recht-en-wet/71544-werking-van-het-europees-recht-in-de-nationale-rechtsorde.html> (werking van het Europees recht in de nationale rechtsorde).

¹²¹ *Factsheet Rechtstreekse werking van bepalingen uit Europese richtlijnen: Regels en risico's* (factsheet van december 2009), Den Haag: Europa decentraal 2009, p. 5.

¹²² HvJ EG 15 december 1995, nr. C- 415/93, *Faccini Dori*, *Jur.* 1995, p. I-3325.

rechtstreekse werking. Zo bestaat de uitlegverplichting onafhankelijk van de vraag of de richtlijn voldoende duidelijk en onvoorwaardelijk is en de plicht strekt zich eveneens uit tot particuliere verhoudingen.¹²³ De nationale rechter mag deze vorm van interpretatie daarentegen niet altijd gebruiken. Indien de rechter het recht zo ver moet oprekken om het gewenste effect op nationaal niveau te verkrijgen waardoor dit tegen het geldende recht ingaat (contra legem werking), zal de rechter niet interpreteren.¹²⁴ De nationale rechter kan derhalve stuiten op het rechtszekerheidsbeginsel. De rechtszekerheidsgrens wordt bereikt wanneer de nationale wetgeving onvoldoende speelruimte biedt voor een conforme interpretatie, wanneer de rechter buiten zijn rechterlijke taakopdracht treedt en/of aan particulieren verplichtingen worden opgelegd waarmee zij geen rekening behoeven te houden.¹²⁵

Gebleken is dat de richtlijn erg gedetailleerd is, waardoor de richtlijn niet veel speelruimte bevat met betrekking tot de knelpunten in het EPD. De nationale component zal stapsgewijs verder worden ingeperkt, nu met de richtlijn harmonisatie is beoogd. De ruimte voor de eigen rechtsvorming is beperkt tot de door de richtlijn aan de lidstaten gelaten bandbreedte.¹²⁶ Het EPD dient derhalve volledig in overeenstemming te zijn met de richtlijn. Indien dit niet het geval is, zal aan de richtlijn voorrang worden verleend. Teneinde het EPD volledig in overeenstemming te brengen met de richtlijn, dient het EPD te voorzien in een recht op informatie, inzage, correctie en verzet voor de betrokkene. Daarnaast mogen de persoonsgegevens in het EPD alleen worden verwerkt ten behoeve van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De verantwoordelijke heeft de plicht te zorgen voor de vertrouwelijkheid van gegevensverwerking, beveiliging en aanmelding ervan bij de toezichthouder of een FG. Ten slotte dient er toezicht op een rechtmatige gegevensverwerking in het EPD plaats te vinden door het CBP.¹²⁷

3.3 Aanbeveling R (97) 5 betreffende de bescherming van medische gegevens

De achtergrond voor de totstandkoming van de aanbeveling vormde het toenemend gebruik van computers in de gezondheidszorg, waardoor een bedreiging ontstond voor de privacy van patiënten. Hiertoe is eind jaren zeventig een onderzoek verricht door een “comité van experts”, bestaande uit juridische, medische en computer-deskundigen, naar de regels inzake medische databanken. Vanuit dit comité werd een “working party” opgericht die voor de voorbereiding van een ontwerpaanbeveling

¹²³ J.M. Prinssen, *Doorwerking van Europees recht: de verhouding tussen directe werking, conforme interpretatie en overheidsaansprakelijkheid* (Europese monografieën nr. 73), Deventer: Kluwer 2004, p. 52 en HvJ EG 13 november 1990, nr. C-106/89, *Marleasing*, *Jur.* 1990, p. I-4135.

¹²⁴ Zie <www.wetenschap.infonu.nl/recht-en-wet/71544-werking-van-het-europees-recht-in-de-nationale-rechtsorde.html> (werking van het Europees recht in de nationale rechtsorde).

¹²⁵ Prinssen 2004, p. 52.

¹²⁶ Aldus Overkleeft-Verburg 2000, p. 171.

¹²⁷ *Kamerstukken I* 2010/11, 32 761, nr. 1, Bijlage Leidraad afstemmen van wetgeving op de Wet bescherming persoonsgegevens, p. 34 en 35.

moest zorg dragen. Op 23 januari 1981 werd Aanbeveling R (81) 1 inzake geautomatiseerde medische databanken door het Comité van Ministers (CvM) aanvaard. Deze aanbeveling bleek eind jaren tachtig door de ontwikkelingen in de informatietechnologie echter achterhaald, waarna het “comité of experts” tot herziening van de aanbeveling besloot. Dit leidde uiteindelijk tot de in 1997 door het CvM aanvaarde Aanbeveling R (97) 5 inzake de bescherming van medische gegevens.¹²⁸ De aanbeveling richt zich op de verzameling en geautomatiseerde verwerking van medische gegevens, maar kan tevens op niet-geautomatiseerde gegevensverwerking van toepassing worden verklaard. In de aanbeveling wordt met de term persoonsgegevens alle informatie bedoeld die betrekking heeft op een geïdentificeerde of identificeerbare persoon. Een persoon is niet identificeerbaar indien voor identificatie een onevenredige hoeveelheid tijd en mankracht nodig is. In het geval een persoon niet identificeerbaar is zijn de gegevens “anoniem”. De term medische gegevens heeft betrekking op alle persoonsgegevens die een nauwe band met de gezondheid vertonen, alsmede genetische gegevens.¹²⁹ Hieronder zal ik de voor dit onderzoek belangrijkste principes van Aanbeveling R (97) 5 uiteenzetten.

Principe 3.2 R (97) 5 (Verzamelen en verwerken van medische gegevens slechts toegestaan voor beroepsbeoefenaren)

Als beginsel geldt dat medische gegevens enkel mogen worden verzameld en verwerkt onder verantwoordelijkheid van medische beroepsbeoefenaren. Daarnaast is het verzamelen en verwerken van medische gegevens tevens toegestaan aan personen of instellingen die handelen namens medische beroepsbeoefenaren. Degenen die medische gegevens mogen verwerken en verzamelen dienen een geheimhoudingsplicht te hebben.

Principe 4.3 onder c R (97) 5 (Toestemming van betrokkene nodig bij verzamelen en verwerken van medische gegevens)

Medische gegevens mogen slechts worden verzameld en verwerkt indien de betrokkene of diens wettelijke vertegenwoordiger, gezagsdrager, of een daartoe bij de wet aangewezen persoon of instantie hiervoor toestemming heeft verleend.

Principe 5.1 en 5.3 R (97) 5 (Verstrekken van informatie aan betrokkene)

In dit principe is vastgelegd dat de betrokkene dient te worden geïnformeerd over het bestaan van een bestand met zijn medische gegevens en de categorie waartoe de verzamelde of te verzamelen gegevens behoren. Daarnaast dient aan de betrokkene informatie te worden gegeven over de doeleinden ten behoeve waarvan de medische gegevens worden of zullen worden verwerkt. Tevens dient de betrokkene informatie te krijgen over de personen of instellingen bij wie de gegevens worden of zullen

¹²⁸ M.C. Ploem, *Tussen privacy en wetenschapsvrijheid. Regulering van gegevensverwerking voor medisch-wetenschappelijk onderzoek*, (diss. Amsterdam UvA) Den Haag: Sdu 2004, p. 123.

¹²⁹ Aanbeveling no. R (97) 5 van het Comité van Ministers van de Lid-Staten betreffende de bescherming van medische gegevens, Stcrt. 1998, 38.

worden opgevraagd en over de personen of instellingen aan wie de gegevens kunnen worden verstrekt, alsmede de redenen daarvoor. De betrokkene dient ook te worden geïnformeerd over de mogelijkheden die hij heeft om zijn toestemming te weigeren of in te trekken, alsmede de consequenties daarvan en de voorwaarden voor de uitoefening van het recht van inzage en correctie. De betrokkene dient bij voorkeur individueel te worden geïnformeerd over de bovengenoemde punten.¹³⁰

Principe 5.6 onder b R (97) 5 (Afwijken van het verstrekken van informatie aan betrokkene)

Dit principe bevat een uitzondering op de principes 5.1 en 5.3 en houdt in dat in spoedgevallen medische gegevens mogen worden verzameld voordat de betrokkene is geïnformeerd.

Principe 7.1 R (97) 5 (Verstrekken van medische gegevens)

Principe 7.1 bepaalt dat medische gegevens niet mogen worden verstrekt, behoudens uitzonderingen. De - voor dit onderzoek relevante - uitzonderingen zijn te vinden in principe 7.2 en 7.3 onder c en d, die ik hierna zal gaan bespreken.

Principe 7.2 R (97) 5 (Verstrekken van medische gegevens en de geheimhoudingsplicht)

Medische gegevens mogen slechts worden verstrekt aan zorgverleners, indien de betreffende zorgverlener gebonden is aan de voorschriften inzake geheimhouding die van toepassing zijn op medische beroepsbeoefenaren of aan vergelijkbare voorschriften inzake geheimhouding.

Principe 7.3 onder c en d R (97) 5 (Voorwaarden voor verstrekken medische gegevens)

Principe 7.3 onder c bepaalt dat medische gegevens slechts mogen worden verstrekt, indien zij relevant zijn en de betrokkene hiervoor ten behoeve van een of meer doeleinden toestemming heeft verleend. Daarnaast mag de verstrekking van medische gegevens niet strijdig zijn met het interne recht.

Principe 7.3 onder d bepaalt dat medische gegevens mogen worden verstrekt:

- mits de betrokkene hiertegen niet uitdrukkelijk bezwaar heeft gemaakt en de verstrekking van gegevens niet verplicht is;
- indien de gegevens op vrijwillige basis zijn verzameld om preventieve, diagnostische of therapeutische redenen;
- indien het doel van de verstrekking niet strijdig is met het doel van de behandeling waarvoor de gegevens zijn verzameld, met name ten behoeve van de aan de patiënt verstrekte zorg of van het beheer van een gezondheidsdienst die handelt in het belang van de patiënt.

¹³⁰ Aanbeveling no. R (97) 5 van het Comité van Ministers van de Lid-Staten betreffende de bescherming van medische gegevens, Stcrt. 1998, 38.

Principe 8.1 R (97) 5 (Recht van inzage door betrokkene)

De betrokkene dient inzage in zijn of haar medische gegevens te kunnen krijgen die hem of haar betreffen. Dit recht kan echter, ondanks het grote belang dat aan het recht op kennisneming van medische gegevens wordt toegekend, worden beperkt ingevolge principe 8.2 R (97) 5.

Principe 8.2 onder c R (97) 5 (Uitzondering inzagerecht van betrokkene)

Inzage in medische gegevens kan uitsluitend worden geweigerd, beperkt of opgeschort, indien de informatie aan de betrokkene tevens informatie over derden bevat.

Principe 8.3 R (97) 5 (Recht op correctie door betrokkene)

Dit principe bepaalt dat betrokkene kan verzoeken om correctie van hem betreffende onjuiste gegevens. Indien hem dit wordt geweigerd, moet er voor de betrokkene de mogelijkheid bestaan om hiertegen in beroep te kunnen gaan.

Principe 9.2 R (97) 5 (Passende veiligheidsmaatregelen)

Dit principe bepaalt dat gepaste veiligheidsmaatregelen dienen te worden genomen, met het oog op:

- het verhinderen van toegang tot de databases van zorgverleners voor degenen die daartoe niet geautoriseerd zijn (onder a);
- het voorkomen dat gegevensdragers door onbevoegden kunnen worden gelezen, gekopieerd, gewijzigd of verplaatst (onder b);
- het voorkomen dat gegevens door onbevoegden in het informatiesysteem worden ingevoerd of dat onbevoegden kennisnemen van in het geheugen opgeslagen persoonsgegevens dan wel deze wijzigen of wissen (onder c);
- het voorkomen dat systemen voor de geautomatiseerde verwerking van gegevens door onbevoegden kunnen worden gebruikt met behulp van apparatuur voor de overbrenging van gegevens (onder d);
- het waarborgen dat, met het oog op de selectieve toegang tot de gegevens en de veiligheid van de medische gegevens, de verwerking in de regel zodanig geschiedt dat scheiding mogelijk is van gegevens ter identificatie, administratieve gegevens, medische gegevens, sociale gegevens en genetische gegevens (onder e);
- het waarborgen dat kan worden gecontroleerd en vastgesteld aan welke personen of instellingen persoonsgegevens kunnen worden verstrekt via apparatuur voor de overbrenging van gegevens (onder f);
- het waarborgen dat a posteriori kan worden gecontroleerd en vastgesteld wie toegang heeft gehad tot het systeem en welke persoonsgegevens op welk moment en door wie in het informatiesysteem zijn ingevoerd (onder g);

- het voorkomen dat tijdens het verstrekken van persoonsgegevens of tijdens het transport van gegevensdragers gegevens door onbevoegden kunnen worden gelezen, gekopieerd, gewijzigd of gewist (onder h);
- het veiligstellen van de gegevens door het maken van kopieën (onder g).

Principe 9.4 R (97) 5 (Aanwijzen onafhankelijk persoon voor veiligheid systeem)

Dit principe bepaalt dat beheerders van bestanden met medische gegevens, zo nodig een onafhankelijk persoon dienen aan te wijzen die verantwoordelijk is voor de veiligheid van de informatiesystemen en de bescherming van de gegevens, en die in staat is dienaangaande adequaat advies te geven.

Principe 10.3 R (97) 5 (Uitzonderingen op het verwijderen van medische gegevens)

Medische gegevens dienen op verzoek van de betrokkene te worden verwijderd, tenzij zij anoniem zijn gemaakt, er een verplichting bestaat tot archivering of verwijdering strijdig is met hogere legitieme belangen. Onder hogere legitieme belangen kunnen worden verstaan de volksgezondheid, de medische wetenschap, de functionaris die verantwoordelijk is voor de medische behandeling of de bestandsbeheerder teneinde deze in staat te stellen zijn rechten uit te oefenen of te verdedigen, dan wel historische of statistische doeleinden (principe 10.2 R (97) 5).

3.4 Jurisprudentie EHRM: handelen van de overheid ten aanzien van persoonsgegevens

Zoals reeds vermeld heeft het EHRM in zijn jurisprudentie na het Verdrag van Straatsburg de bescherming van persoonsgegevens voor een belangrijk deel onder artikel 8 EVRM gebracht. Naast een negatieve verplichting (de overheid moet zich onthouden van inmenging) zijn er ook positieve verplichtingen uit het recht op privacybescherming afgeleid (de overheid moet actief optreden om het recht te waarborgen).¹³¹ Artikel 8 EVRM is voornamelijk bedoeld om burgers te beschermen tegen het handelen van de overheid, maar heeft tevens gelding in private relaties (zoals tussen een private zorginstelling en een patiënt¹³²). In Nederland komt aan artikel 8 EVRM horizontale werking toe.

Artikel 8 EVRM luidt als volgt:

“1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

¹³¹ Kranenborg 2007, p. 115.

¹³² HR 9 januari 1989, NJ 1987, 928 (Edamse bijstandmoeder).

Uit de jurisprudentie van het EHRM valt een aantal belangrijke vereisten voor de bescherming van persoonsgegevens af te leiden, alsmede een overzicht van handelingen ten aanzien van persoonsgegevens die als een inbreuk op de persoonlijke levenssfeer worden beschouwd. Het EHRM hanteert bij artikel 8 EVRM een vast toetsingsschema. Allereerst (nadat aan de ontvankelijkheidseisen is voldaan) kijkt het EHRM of de situatie binnen de reikwijdte van artikel 8 EVRM valt. Daarna beoordeelt het EHRM of sprake is van een inmenging in een van de rechten van artikel 8 EVRM. Tot slot toetst het EHRM of die inmenging gerechtvaardigd is op grond van artikel 8, tweede lid, EVRM. Indien dit niet het geval is, is sprake van een schending van artikel 8 EVRM.¹³³

3.4.1 Reikwijdte artikel 8 EVRM: Is er een privacyschending?

Naar het oordeel van het EVRM levert het enkel bewaren van persoonsgegevens door de overheid geen inmenging in artikel 8 EVRM op. De bescherming van artikel 8 EVRM komt pas in beeld indien de overheid bepaalde vervolghandelingen verricht met de persoonsgegevens.¹³⁴ Zoals in het arrest Rotaru tegen Roemenië, waarbij de overheid gegevens systematisch verzamelt en opslaat.¹³⁵ In het arrest P.G. en J.H. tegen het Verenigd Koninkrijk, waarin stemopnames van twee gedetineerden tijdens een ondervraging door de politie werden gebruikt om een vergelijking te maken met stemmen op eerder opgenomen telefoongesprekken, oordeelde het EHRM dat sprake was van een inmenging in artikel 8 EVRM.¹³⁶ In de zaak Peck tegen het Verenigd Koninkrijk werd iemand tijdens een zelfmoordpoging op straat gefilmd door een beveiligingscamera. Het EHRM hanteerde hierbij een aantal aanknopingspunten om de toepassing van artikel 8 EVRM vast te stellen: het privacygevoelige karakter van de gegevens zelf, de manier waarop de gegevens waren verkregen en het beoogde gebruik van de gegevens, namelijk een beperkt gebruik of een algemene openbaarmaking.¹³⁷ Het eerste aanknopingspunt (het privacygevoelige karakter van de gegevens zelf) duidt op de toepassing van artikel 8 EVRM indien de overheid privacygevoelige gegevens - zoals medische gegevens - in bezit heeft. Bij het tweede aanknopingspunt, de manier waarop de gegevens zijn verkregen, maakt het EHRM gebruik van het criterium 'reasonable expectation of privacy' (de redelijke privacyverwachting) indien het gaat om het vastleggen van persoonsgegevens in het publieke domein.¹³⁸ Dit criterium houdt een impliciete instemming van de betrokkene met het handelen van de overheid in.¹³⁹ Het derde aanknopingspunt ziet op de vervolghandelingen van de overheid. Indien de overheid gegevens van iemand opslaat, kan het EHRM artikel 8 EVRM van toepassing achten.¹⁴⁰ Bij dit aanknopingspunt

¹³³ Kranenborg 2007, p. 81.

¹³⁴ Kranenborg 2007, p. 80-81.

¹³⁵ EHRM 4 mei 2000, nr. 28341/95, RJD 2000-V, r.o. 41 (*Rotaru tegen Roemenië*).

¹³⁶ EHRM 25 september 2001, nr. 44787/98, RJD 2001-IX, r.o. 57 (*P.G. en J.H. tegen het Verenigd Koninkrijk*).

¹³⁷ ECRM 19 mei 1994, nr. 15225/89, r.o. 48 (*Friedl tegen Oostenrijk*), Zie ook EHRM 24 juni 2004, nr. 59320/00, RJD 2004-VI, r.o. 52 (*Von Hannover tegen Duitsland*).

¹³⁸ Kranenborg 2007, p. 120.

¹³⁹ Kranenborg 2007, p. 122.

¹⁴⁰ EHRM 4 mei 2000, nr. 28341/95, RJD 2000-V, r.o. 41 (*Rotaru tegen Roemenië*).

speelt de verwachting van het individu ten aanzien van het gebruik tevens een rol. Het EHRM oordeelt eveneens dat artikel 8 EVRM van toepassing is indien iemand een 'reasonable expectation of privacy' had, wat in het EPD het geval is.¹⁴¹ De patiënt mag immers verwachten dat alleen de beroepsbeoefenaar met wie hij of zij een behandelrelatie heeft, zijn of haar medische gegevens verwerkt. Indien de privacybescherming niet al op grond van de eerdere aanknopingspunten van toepassing is, kan zij als het gebruik van de gegevens de normale verwachting van een individu te boven gaat alsnog van toepassing zijn. Zo oordeelde het EHRM dat in de zaak Peck tegen het Verenigd Koninkrijk, gezien 'the recording of the data and the systematic or permanent nature of the record' en het onvoorziene en excessieve gebruik van de opname (de beelden kwamen namelijk door toedoen van de overheid in de media), artikel 8 EVRM van toepassing was.¹⁴²

Zoals reeds aangegeven, is bij het tweede en derde aanknopingspunt het criterium van de redelijke privacyverwachting van belang, inhoudende dat indien betrokkene vooraf redelijkerwijs kon verwachten wat de overheid zou kunnen doen, hij of zij impliciet met het overheidshandelen heeft ingestemd door bepaald gedrag te vertonen.¹⁴³ Het EHRM heeft het criterium van de redelijke privacyverwachting voor de afbakening van het recht op privacy onder artikel 8 EVRM voornamelijk toegepast in het voordeel van de betrokkene: alleen in zeer specifieke gevallen, los van het gedrag van de overheid, valt het buiten de reikwijdte van artikel 8 EVRM.¹⁴⁴ Dit geldt tevens voor de verwerking van persoonsgegevens.¹⁴⁵

3.4.2 Artikel 8, tweede lid, EVRM: waarborgen tegen misbruik van persoonsgegevens

Nadat is vastgesteld dat artikel 8 EVRM van toepassing is op de situatie, kan getoetst worden aan artikel 8, tweede lid, EVRM. Volgens deze bepaling is een inmenging gerechtvaardigd, indien deze bij wet is voorzien, een legitiem doel dient en noodzakelijk is in een democratische samenleving. Volgens het eerste vereiste hoeft een 'wet' geen wet in formele zin te zijn. Dit kan tevens een wet in materiële zin zijn of vaste rechtspraak. Verder dient de rechtsregel kenbaar en voldoende voorzienbaar te zijn.¹⁴⁶ Bij het tweede vereiste dient gekeken te worden of een van de in artikel 8 EVRM genoemde belangen met de schending gediend wordt. Hierbij kan sprake zijn van een belangenafweging tussen het recht op privacy van de betrokkene en de rechten en vrijheden van anderen. Het derde vereiste wordt uitgelegd middels de beginselen van proportionaliteit en subsidiariteit. Proportionaliteit houdt in dat de

¹⁴¹ EHRM 25 juni 1997, nr. 20605/92, *RJD* 1997-III, r.o. 45 (*Halford tegen het Verenigd Koninkrijk*).

¹⁴² EHRM 28 januari 2001, nr. 44647/98, *RJD* 2003-I, r.o. 59 (*Peck tegen het Verenigd Koninkrijk*).

¹⁴³ Kranenborg 2007, p. 122.

¹⁴⁴ Zie bijvoorbeeld EHRM 28 januari 2001, nr. 44647/98, *RJD* 2003-I, r.o. 59 (*Peck tegen het Verenigd Koninkrijk*). Permanent cameratoezicht verschilt nauwelijks van een politieagent die toezicht houdt op de hoek van de straat en valt derhalve buiten het privacybegrip.

¹⁴⁵ Kranenborg 2007, p. 122.

¹⁴⁶ L. Dierickx, *Het recht op afbeelding*, Antwerpen: Intersentia 2005, p. 10.

inmenging evenredig moet zijn aan het nagestreefde doel en subsidiariteit betekent dat de daarvoor aangevoerde gronden relevant en toereikend moeten zijn.

Wanneer sprake is van een gerechtvaardigde inbreuk op het privéleven betreffende het verwerken van persoonsgegevens, kan uit de jurisprudentie van het EHRM worden afgeleid.¹⁴⁷ Allereerst stelt het EHRM beperkingen ten aanzien van de verwerking van gegevens. Zo blijkt uit het arrest *Z. tegen Finland* dat een belangrijk vereiste voor het gebruik van persoonsgegevens een doelbinding is. Gegevens mogen alleen gebruikt worden voor het wettelijk vastgelegde doel waarvoor ze zijn verkregen.¹⁴⁸ Daarnaast blijkt uit de zaak *Murray tegen het Verenigd Koninkrijk* dat de gegevens relevant dienen te zijn voor het beoogde doel.¹⁴⁹ Tevens hecht het EHRM in zijn arresten *Rotaru tegen Roemenië* en *Segerstedt-Wiberg e.a. tegen Zweden* belang aan het stellen van grenzen aan de termijn voor het bewaren van gegevens.¹⁵⁰

Daarnaast overweegt het EHRM in het arrest *Leander tegen Zweden* dat een belangrijke waarborg tegen misbruik van persoonsgegevens de mogelijkheid van toegang tot die gegevens is.¹⁵¹ De mogelijkheid van toegang tot de persoonsgegevens strekt zich echter niet zo ver uit dat iemand die vanuit zijn professionele hoedanigheid bij naam in bepaalde zakelijke documenten genoemd wordt, toegang tot die documenten moet hebben.¹⁵² Het EHRM oordeelt in het arrest *I tegen Finland* dat het recht op privacy niet alleen een afweerrecht is, maar tevens een actief optreden van de overheid vergt.¹⁵³ De overheid dient onder meer te kunnen aantonen wie toegang heeft gehad tot de persoonsgegevens. Indien de overheid dit niet kan aantonen, overweegt het EHRM in het arrest *I tegen Finland* dat de beveiliging onvoldoende was. Het EHRM oordeelde hierin dat aan patiënt *I* een schadevergoeding diende te worden toegekend door het overheidsziekenhuis, aangezien zij schade heeft geleden wegens onvoldoende beveiliging van een elektronisch patiëntendossier.¹⁵⁴ Tevens dient de betrokkene de mogelijkheid te hebben om correcties aan te brengen en dient de betrokkene te worden geïnformeerd over het feit dat zijn persoonsgegevens in handen van de overheid zijn.¹⁵⁵ Naast bovengenoemde waarborgen zijn ook andere elementen van belang. Uit het arrest *Z. tegen Finland* blijkt dat het EHRM rekening houdt met de gevoelige aard van de persoonsgegevens. Het EHRM oordeelde hierin dat de HIV-besmetting van de klaagster als medisch gegeven extra vertrouwelijk

¹⁴⁷ L.F.M. Verhey, 'De EG-richtlijn bescherming persoonsgegevens: uitgangspunten en hoofdlijnen', *NJCM-Bulletin* 1997, p. 242 en I. Harden, 'Citizenship and Information', *EPL* 2001, p. 173-174.

¹⁴⁸ Zie EHRM 25 januari 1997, nr. 22009/93, *RJD* 1997-I, r.o. 103 (*Z. tegen Finland*).

¹⁴⁹ EHRM 28 oktober 1994, nr. 14310/88, A-300-A, r.o. 93 (*Murray tegen het Verenigd Koninkrijk*).

¹⁵⁰ EHRM 4 mei 2000, nr. 28341/95, *RJD* 2000-V, r.o. 57 (*Rotaru tegen Roemenië*); EHRM 6 juni 2006, nr. 62332/00, r.o. 90 (*Segerstedt-Wiberg e.a. tegen Zweden*).

¹⁵¹ EHRM 26 maart 1987, nr. 9248/81, r.o. 48 (*Leander tegen Zweden*).

¹⁵² EHRM 4 januari 2007, nr. 39658/05, p. 4 (*Smith tegen het Verenigd Koninkrijk*).

¹⁵³ C.C.M. de Raaij, 'Noot bij EHRM 17 juli 2008 (I. tegen Finland). Onvoldoende beveiliging van elektronisch patiëntendossier', *Privacy & Informatie* 2009-2, p. 89-90.

¹⁵⁴ EHRM 17 juli 2008, nr. 20511/03 (*I tegen Finland*).

¹⁵⁵ EHRM 26 maart 1987, nr. 9248/81, A-116, r.o. 48 (*Leander tegen Zweden*) en EHRM 4 mei 2000, nr. 28341/95, *RJD* 2000-V, r.o. 46 (*Rotaru tegen Roemenië*); EHRM 6 september 1978, nr. 5029/71, A-28, r.o. 58 (*Klass tegen Duitsland*).

behandeld diende te worden.¹⁵⁶ Tevens kan het nagestreefde doel in de belangenafweging zwaarder wegen.¹⁵⁷ Dit was bijvoorbeeld het geval in het arrest Murray, waarin het EHRM de bestrijding van terrorisme als legitiem doel in de belangafweging zwaar liet meewegen.¹⁵⁸ Daarnaast kan de redelijke privacyverwachting (waar ik in paragraaf 3.3.1 nader op ben ingegaan) een rol spelen. Zo oordeelde het EHRM in zaak Wypych tegen Polen dat Wypych als politicus willens en wetens blootstond aan publieke controle en daardoor bepaalde openbaarheid over zijn persoon kon verwachten. Het openbaar maken van zijn persoonsgegevens hield derhalve een gerechtvaardigde inbreuk op het recht op privacy in.¹⁵⁹

3.5 Oplossing knelpunten: Aanbeveling R (97) 5 en jurisprudentie EHRM inzake bescherming persoonsgegevens

In deze paragraaf ga ik onderzoeken of het recht op privacy in het EPD beter kan worden gegarandeerd met behulp van de aanbevelingen van de Raad van Europa betreffende de bescherming van medische gegevens en de jurisprudentie van het EHRM inzake de bescherming van persoonsgegevens. Per aspect zal ik een oplossing proberen te vinden voor de geïnventariseerde technische, juridische en politieke knelpunten.

Schaalgrootte van het EPD

Een technisch knelpunt van de schaalgrootte van het EPD, is dat onbevoegden toegang zullen krijgen tot het EPD. Teneinde dit te voorkomen, dienen ingevolge principe 9.2 onder h R (97) 5 gepaste veiligheidsmaatregelen te worden genomen. Wat onder gepaste veiligheidsmaatregelen moet worden verstaan, vermeldt het principe echter niet. Wel kan men denken aan het aanwijzen van een onafhankelijk persoon voor het uitoefenen van toezicht op de rechtmatige gegevensverwerking in het EPD (zie principe 9.4 R (97) 5). Bijvoorbeeld een FG, aangesteld op grond van artikel 62 Wbp. De FG kan dan worden aangewezen binnen Nictiz, als interne toezichthouder op het gebruik van het landelijk EPD via het LSP. De FG houdt onafhankelijk toezicht op de toepassing en de naleving van de Wbp. Daarnaast kunnen meldingen van gegevensverwerkingen bij deze functionaris worden gedaan.¹⁶⁰ De FG kan dan tevens zorg dragen voor de kwaliteit van de patiëntgegevens, opdat afname van de kwaliteit van informatie wordt tegengegaan (politiek knelpunt).

¹⁵⁶ EHRM 25 januari 1997, nr. 22009/93, RJD 1997-I, r.o. 96 (*Z. tegen Finland*).

¹⁵⁷ Kranenborg 2007, p. 87.

¹⁵⁸ EHRM 28 oktober 1994, nr. 14310/88, A-300-A, r.o. 91 (*Murray tegen het Verenigd Koninkrijk*).

¹⁵⁹ EHRM 25 oktober 2005, nr. 2428/05, p. 11 (*Wypych tegen Polen*).

¹⁶⁰ *Informatieblad De functionaris voor de gegevensbescherming* (informatieblad van 16 september 2010), Den Haag: College Bescherming Persoonsgegevens 2010.

De rol van zorgverzekeraars

Teneinde te voorkomen dat zorgverzekeraars in de patiëntgegevens gaan kijken en risicoprofielen gaan maken, dient er op te worden toegezien dat slechts medische beroepsbeoefenaren met een geheimhoudingsplicht de patiëntgegevens verzamelen en verwerken (zie principe 3.2 R (97) 5). De patiënt dient - ingevolge principe 4.3 onder c R (97) 5 - hiervoor (uitdrukkelijke) toestemming te hebben verleend. Er dient tevens toezicht plaats te vinden, opdat het doel van de verstrekking van patiëntgegevens niet strijdig is met het doel van de behandeling waarvoor de gegevens zijn verzameld (zie principe 7.3 onder d R (97) 5 en de zaak Murray tegen het Verenigd Koninkrijk¹⁶¹). Een onafhankelijk persoon, zoals een FG, kan ingevolge principe 9.4 R (97) 4 voor dit toezicht zorg dragen.

“Geen bezwaar”-systeem

Ingevolge principe 4.3 onder c R (97) 5 is toestemming van de betrokkene nodig bij het verzamelen en verwerken van medische gegevens. Of het ontbreken van bezwaar als toestemming mag worden opgevat voor het registreren van patiëntgegevens in het EPD, vermeldt het principe niet. Uit de jurisprudentie van het EHRM inzake de bescherming van persoonsgegevens kan echter wel worden afgeleid dat de verwachting van het individu ten aanzien van het gebruik een rol speelt: de patiënt dient een 'reasonable expectation of privacy' te hebben.¹⁶² Indien de patiënt vooraf en individueel wordt geïnformeerd over het registreren en verwerken van zijn of haar gegevens (zie principe 5.1 en 5.3 R (97) 5), kan een redelijke privacyverwachting worden verondersteld en heeft de patiënt derhalve impliciet met het overheidshandelen ingestemd door geen bezwaar te maken.¹⁶³ Hiermee wordt het politieke knelpunt van een ondoorzichtige registratie van gegevens in het EPD opgelost.

Indien het “geen bezwaar-systeem” stand houdt, blijft het echter wel in strijd met artikel 7:457 BW. Teneinde dit juridische knelpunt op te lossen, dient de patiënt derhalve uitdrukkelijke toestemming te geven voor het registreren van zijn of haar gegevens in het EPD.

Behandelrelatie

Teneinde het technische knelpunt van de onduidelijke beschikbaarheid van de (mede)behandelaar op te lossen en derhalve het bestaan van een behandelrelatie als sluitende voorwaarde te vormen voor het uitwisselen van patiëntgegevens, is het nodig dat de patiënt vooraf wordt geïnformeerd over welke collega's ooit als medebehandelaar of medewerker zullen optreden (zie principe 5.1 en 5.3 R (97) 5). Daarnaast dient de patiënt ingevolge principe 7.3 onder c R (97) 5 toestemming ten behoeve van een

¹⁶¹ EHRM 28 oktober 1994, nr. 14310/88, A-300-A, r.o. 93 (*Murray tegen het Verenigd Koninkrijk*).

¹⁶² O.a. EHRM 4 mei 2000, nr. 28341/95, RJD 2000-V, r.o. 41 (*Rotaru tegen Roemenië*) en EHRM 25 juni 1997, nr. 20605/92, RJD 1997-III, r.o. 45 (*Halford tegen het Verenigd Koninkrijk*).

¹⁶³ EHRM 26 maart 1987, nr. 9248/81, A-116, r.o. 48 (*Leander tegen Zweden*) en EHRM 4 mei 2000, nr. 28341/95, RJD 2000-V, r.o. 46 (*Rotaru tegen Roemenië*); EHRM 6 september 1978, nr. 5029/71, A-28, r.o. 58 (*Klass tegen Duitsland*).

of meer doeleinden te verlenen, alvorens zijn of haar gegevens mogen worden verwerkt. De patiënt dient zo nodig de behandelrelatie tevens expliciet te bevestigen.

Schending van de doelbinding

De eis dat alleen patiëntgegevens verwerkt mogen worden voor het beoogde doel, blijkt onder meer uit principe 7.3 onder d R (97) 5 en de zaken *Z. tegen Finland*¹⁶⁴ en *Murray tegen het Verenigd Koninkrijk*.¹⁶⁵ Een onafhankelijke toezichthouder dient - ingevolge principe 9.4 R (97) 5 - er op toe te zien dat patiëntgegevens worden verwerkt voor het beoogde doel, namelijk “de goede behandeling of verzorging van de patiënt”.¹⁶⁶ Alvorens er tot gegevensuitwisseling wordt overgegaan, dient de patiënt ingevolge principe 5.1 en 5.3 R (97) 5 geïnformeerd te worden over de doeleinden ten behoeve waarvan de medische gegevens worden of zullen worden verwerkt. Indien aan het bovenstaande wordt voldaan, wordt het juridische knelpunt (strijdigheid met artikel 7:457, tweede lid, BW) opgelost.

UZI-pas

Het nemen van gepaste veiligheidsmaatregelen ingevolge principe 9.2 onder a R (97) 5, dient te voorkomen dat met de UZI-pas onbevoegd patiëntgegevens worden geraadpleegd, waardoor het technische knelpunt zal worden opgelost. Mogelijk denkbare maatregelen zijn de pashouders bewust maken van de risico's en hen daartoe adviezen te geven (zoals fysieke afscherming van het gebruikte systeem, het beveiligen van toegang tot de pc met een schermbeveiliging met wachtwoord bij het verlaten van de werkplek, het nalaten van uitlening van de UZI-pas en het wijzigen van de pincode wanneer het vermoeden bestaat dat anderen deze kennen). Daarnaast kunnen onder mogelijke maatregelen het plaatsen van een apart numeriek toetsenbord dat kan worden afgeschermd bij het invoeren van de pincode en meer controle op virussen worden verstaan.¹⁶⁷

Logging

Het EHRM overweegt in het arrest *I tegen Finland* dat de overheid moet kunnen aantonen wie toegang heeft gehad tot de persoonsgegevens.¹⁶⁸ Dit doet zij in het EPD door middel van logging achteraf. Logging achteraf zorgt er echter wel voor dat misbruik van inzage in het patiëntdossier niet in alle gevallen wordt voorkomen, maar slechts indien er een vermoeden van misbruik bestaat. Teneinde dit technische knelpunt op te lossen dienen de gegevens niet enkel te worden gecontroleerd in het geval een vermoeden van misbruik bestaat. Controle op alle raadplegingen dient bijvoorbeeld wekelijks en steekproefsgewijs plaats te vinden. Daarnaast moeten gepaste veiligheidsmaatregelen (zie principe 9.2 onder a R (97) a) worden genomen, opdat alleen zorgverleners die een behandelrelatie met de patiënt

¹⁶⁴ EHRM 25 januari 1997, nr. 22009/93, *RJD 1997-I*, r.o. 103 (*Z. tegen Finland*).

¹⁶⁵ EHRM 28 oktober 1994, nr. 14310/88, A-300-A, r.o. 93 (*Murray tegen het Verenigd Koninkrijk*).

¹⁶⁶ *Kamerstukken II* 2007/08, 31 466, nr. 3, p. 27.

¹⁶⁷ Zie <www.uziregister.nl> (veilig gebruik UZI-pas).

¹⁶⁸ De Raaij 2009, p. 89-90 en EHRM 17 juli 2008, nr. 20511/ 03 (*I tegen Finland*).

hebben over de patiëntgegevens kunnen beschikken. Hierbij kan men denken aan een FG (zie principe 9.4 R (97) 5) die toezicht houdt op een rechtmatige raadpleging van de patiëntgegevens. Hiermee worden de juridische knelpunten die logging achteraf met zich mee brengt - uitholling van artikel 7:457 BW en strijdigheid met artikel 13 Wbp - opgelost.

Recht op inzage

Het EPD is in strijd met artikel 35 Wbp en artikel 7:456 BW, aangezien er geen toegangsmiddel voorhanden is waarmee patiënten hun recht op inzage kunnen uitoefenen. Principe 8.1 en principe 8.2 R (97) 5 bepalen tevens dat de patiënt zijn of haar recht op inzage dient te kunnen uitoefenen, tenzij de informatie over de patiënt tevens informatie over derden bevat. Er dient derhalve een toegangsmiddel voorhanden te zijn om het juridische knelpunt op te lossen. De jurisprudentie van het EHRM alsmede de aanbevelingen van de Raad van Europa bepalen echter niet hoe dit toegangsmiddel dient te worden ingericht. De minister heeft voorgesteld het verlenen van inzage in de medische gegevens vorm te geven via de website of portal van de zorgverlener.¹⁶⁹

Teneinde het politieke knelpunt van het aanleggen van een “tweede weg” naar informatie uit het EPD op te lossen, dient een onafhankelijk orgaan, zoals een FG, toe te zien op de veiligheid van de informatiesystemen (zie principe 9.4 R (97) 5). Indien naar het voorstel van de minister inzage in de medische gegevens vorm wordt gegeven via de website of portal van de zorgverlener, moet toegang voor de patiënt worden verleend via de zorgverlener die daartoe geautoriseerd is (zie principe 9.2 onder a) zodat alleen bevoegden inzage hebben in de patiëntgegevens. Daarnaast dienen de zorgverleners onderling toezicht te houden op elkaar, teneinde het politieke knelpunt van de afname van de kwaliteit van patiëntgegevens op te lossen.

Recht op vernietiging

In het EPD ontbreekt de garantie van volledige vernietiging, waardoor strijdigheid ontstaat met artikel 36 Wbp en artikel 7:455 BW. Teneinde dit juridische knelpunt op te lossen is het nodig passende veiligheidsmaatregelen te nemen ingevolge principe 9.2 onder h R (97) 5. Zo dient duidelijk in het EPD te worden vastgelegd dat bij een verzoek tot vernietiging de gegevens uit het brondossier moeten worden verwijderd alsmede de gegevens die door een zorgverlener uit een andere instelling zijn geraadpleegd en aldaar zijn opgeslagen. Een onafhankelijk orgaan, zoals een FG (principe 9.4 R (97) 5), dient toezicht te houden op de volledige vernietiging van gegevens in het EPD. In het EPD moet tevens worden vastgelegd dat de gegevens niet worden vernietigd, indien zij anoniem zijn gemaakt, er een verplichting bestaat tot archivering of verwijdering strijdig is met hogere legitieme belangen (zie principe 10.2 en 10.3 R (97) 5).

¹⁶⁹ *Kamerstukken II* 2010/11, 27 529, nr. 71, p. 20.

Toezicht op het EPD

Teneinde het politieke knelpunt op te lossen inhoudende de ontstane capaciteitsproblemen indien enkel het CBP en de IGZ toezicht uitoefenen op het EPD, dient een toezichthouder, met eigen taken en bevoegdheden (waarbij aansluiting en afstemming wordt gezocht met het reeds door het CBP en IGZ uitgevoerde toezicht) te worden opgericht (zie principe 9.4 R (97) 5). Zoals eerder vermeld, kan je hierbij denken aan een FG (aangesteld op grond van artikel 62 Wbp). Middels het aanstellen van FG kunnen ‘eerste lijns’ maatregelen worden getroffen en wordt de mogelijkheid om horizontaal toezicht uit te oefenen geoptimaliseerd. Het CBP kan zich dan terughoudend opstellen en betrokkenen die vragen of klachten hebben doorverwijzen naar de FG.¹⁷⁰

3.6 Conclusie

In dit hoofdstuk is duidelijk geworden dat de privacyrichtlijn nr. 95/46/EG weinig speelruimte bevat met betrekking tot de geïnventariseerde knelpunten in het EPD. Het EPD dient derhalve volledig in overeenstemming te zijn met de richtlijn. De aanbevelingen van de Raad van Europa betreffende de bescherming van medische gegevens en de jurisprudentie van het EHRM inzake de bescherming van persoonsgegevens bieden vooral algemene oplossingen teneinde het EPD meer in overeenstemming te brengen met het recht op privacy. Zo is het met name van belang passende veiligheidsmaatregelen te nemen, ter voorkoming dat onbevoegden het EPD kunnen raadplegen (principe 9.2 R (97) 5). Voor het toezicht op en uitvoering van deze veiligheidsmaatregelen dient ingevolge principe 9.4 een onafhankelijk persoon te worden aangewezen, zoals een FG (die wordt aangesteld op grond van artikel 62 Wbp). Daarnaast is komen vast te staan dat zowel voor het registreren als verstrekken van de medische gegevens de patiënt altijd zijn of haar uitdrukkelijke toestemming dient te geven.¹⁷¹ Tevens is het van belang dat de patiënt geïnformeerd wordt over het feit dat zijn persoonsgegevens in handen van de overheid zijn.¹⁷² Daarnaast dient ingevolge principe 5.1 en 5.3 aan de betrokkene (individueel) informatie te worden gegeven over de doeleinden ten behoeve waarvan de medische gegevens worden of zullen worden verwerkt. Dit doel mag niet strijdig zijn met het doel van de behandeling waarvoor de gegevens zijn verzameld.¹⁷³ Uit de zaak Murray tegen het Verenigd Koninkrijk blijkt tevens dat de te verwerken gegevens relevant dienen te zijn voor het beoogde doel.¹⁷⁴ Principe 7.3 onder d bepaalt onder meer dat medische gegevens mogen worden verstrekt, indien het doel van de verstrekking niet strijdig is met het doel van de behandeling waarvoor de gegevens zijn verzameld, met name ten behoeve van de aan de patiënt verstrekte zorg of van het beheer van een gezondheidsdienst die handelt

¹⁷⁰ Krabben 2010, p. 8-9.

¹⁷¹ Principe 4.3 onder c R (97) 5 en principe 7.3 onder c R (97) 5.

¹⁷² EHRM 26 maart 1987, nr. 9248/81, A-116, r.o. 48 (*Leander tegen Zweden*) en EHRM 4 mei 2000, nr. 28341/95, RJD 2000-V, r.o. 46 (*Rotaru tegen Roemenië*); EHRM 6 september 1978, nr. 5029/71, A-28, r.o. 58 (*Klass tegen Duitsland*).

¹⁷³ EHRM 25 januari 1997, nr. 22009/93, RJD 1997-I, r.o. 103 (*Z. tegen Finland*).

¹⁷⁴ EHRM 28 oktober 1994, nr. 14310/88, A-300-A, r.o. 93 (*Murray tegen het Verenigd Koninkrijk*).

in het belang van de patiënt. Gegevens mogen alleen worden verstrekt en verwerkt met als doeleinde “de goede behandeling of verzorging van de patiënt”.¹⁷⁵

Daarnaast dient de patiënt ingevolge principe 8.1 inzage in zijn of haar gegevens te kunnen krijgen. Het EHRM overweegt dat een belangrijke waarborg tegen misbruik van persoonsgegevens de mogelijkheid van toegang tot die gegevens is.¹⁷⁶ Er dient derhalve een toegangsmiddel voorhanden te zijn. De aanbevelingen van de Raad van Europa en de jurisprudentie van het EHRM laten zich er echter niet over uit op welke wijze de patiënt zijn recht op inzage kan bewerkstelligen. Het is echter wel van belang dat toegang aan de patiënt wordt verleend via een zorgverlener die daartoe geautoriseerd is (zie principe 9.2 onder a) zodat alleen bevoegden inzage hebben in de patiëntgegevens. De overheid dient tevens aan te tonen wie toegang heeft gehad tot de persoonsgegevens.¹⁷⁷ Dit toont zij aan door middel van logging achteraf. Teneinde misbruik te voorkomen dient niet enkel een controle plaats te vinden indien een vermoeden van misbruik bestaat, maar dienen alle raadplegingen wekelijks en steekproefsgewijs te worden gecontroleerd.

¹⁷⁵ *Kamerstukken II* 2007/08, 31 466, nr. 3, p. 27.

¹⁷⁶ EHRM 26 maart 1987, nr. 9248/81, r.o. 48 (*Leander tegen Zweden*).

¹⁷⁷ EHRM 17 juli 2008, nr. 20511/03 (*I tegen Finland*).

4 Een vergelijking met het EPD in België

4.1 Inleiding

Niet alleen in Nederland is het EPD onderwerp van discussie, maar ook in België stuit de invoering van een EPD op veel weerstand aangezien het recht op privacy nog te veel in het geding is.¹⁷⁸ Door deze discussie blijft het Belgische EPD in ontwikkeling en wordt het door aanpassing steeds meer in overeenstemming gebracht met het recht op privacy. Nu bij de ontwikkeling van zowel het Belgische EPD als dat van Nederland wordt gestreefd naar een systeem waarin het recht op privacy volledig wordt gewaarborgd, is het Belgische EPD geschikt om het te vergelijken met het EPD in Nederland. Dit hoofdstuk heeft dan ook als doel te onderzoeken hoe het EPD in België, in het bijzonder in de Vlaamse Gemeenschap, is ingericht, opdat zo tot nieuwe kennis kan worden gekomen waardoor de geïnterviewde knelpunten in het Nederlandse EPD mogelijk kunnen worden opgelost.

In België wordt getracht de elektronische gegevensuitwisseling in de zorg te vergemakkelijken door middel van twee initiatieven: het Decreet Gezondheidsinformatiesysteem (GIS) en de oprichting van het eHealth-platform. In paragraaf 4.2 zal ik de inrichting van het Decreet GIS gaan bespreken en in paragraaf 4.3 zal de inrichting van het eHealth-platform worden uiteengezet. In paragraaf 4.4 ga ik onderzoeken of er in het Decreet GIS en in het eHealth-platform een oplossing te vinden is voor de geïnterviewde knelpunten. In paragraaf 4.5 volgt een conclusie.

4.2 Decreet Gezondheidsinformatiesysteem

Op 16 juni 2006 werd met het Decreet GIS de juridische basis gelegd voor de uitwisseling van persoonsgegevens binnen de gezondheidszorg. Het Decreet GIS creëert een algemeen wettelijk kader voor het verzamelen, doorgeven en verwerken van patiëntgegevens.¹⁷⁹ Artikel 3 van het Decreet introduceert twee verschillende informatiesystemen. Enerzijds het operationeel systeem en anderzijds het epidemiologisch systeem. Het epidemiologisch systeem behelst de gegevensuitwisseling met de administratie om het Vlaams gezondheidsbeleid te coördineren en zal verder onbesproken worden gelaten.¹⁸⁰ Via het operationeel informatiesysteem wordt het bijhouden van een individueel gezondheidsdossier opgelegd en wordt de uitwisseling van die gegevens tussen zorgverleners onderling geregeld.¹⁸¹ Het individuele gezondheidsdossier vormt de basis voor de elektronische

¹⁷⁸ K. van Gossum, 'Het Elektronisch gedeeld patiëntendossier in België: stand van zaken', *Privacy & Informatie* 2008-1, p. 15.

¹⁷⁹ Decreet van 16 juni 2006 tot oprichting van het Gezondheidsinformatiesysteem, BS 7 september 2006 (Decreet GIS).

¹⁸⁰ Artikel 4, tweede lid, Decreet GIS.

¹⁸¹ Artikel 6, §1 Decreet GIS.

registratie.¹⁸² De elektronische registratie vat de relevante gegevens uit het individueel gezondheidsdossier samen op een uniforme en gestandaardiseerde wijze, om de operationele gegevensuitwisseling tussen zorgverleners onderling te vergemakkelijken.¹⁸³

Het toepassingsgebied van het operationele informatiesysteem wordt bepaald in artikel 5, §1 Decreet GIS:

- de zorgverstrekkers¹⁸⁴, voor de activiteiten van zorgverlening waarvoor ze door de Vlaamse Regering erkend zijn of op enerlei wijze door de Vlaamse Regering gefinancierd worden en voor de activiteiten in het kader van een preventieprogramma¹⁸⁵;
- de organisaties met terreinwerking¹⁸⁶, voor de activiteiten van zorgverlening waarvoor ze door de Vlaamse Regering erkend zijn of op enerlei wijze door de Vlaamse Regering gefinancierd worden en voor de activiteiten in het kader van een preventieprogramma;
- de informatieknooppunten¹⁸⁷;
- de diensten, belast met de organisatie van een preventieprogramma of met het toezicht op de aanwending van de middelen in een preventieprogramma, in zoverre ze daarvoor moeten kunnen beschikken over persoonsgegevens van een zorggebruiker.¹⁸⁸

Verder zijn nog de volgende definities van belang:

- Vlaams gezondheidsbeleid: het beleid met betrekking tot het geheel van de aangelegenheden, bedoeld in artikel 5, §1, I, van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen¹⁸⁹.
- pseudo-identiteit: een reeks tekens die verwijst naar een natuurlijke persoon of een organisatie, maar slechts op indirecte wijze toelaat om de identiteit van die persoon of organisatie te bepalen, bijvoorbeeld een identificatiecode of erkenningsnummer.¹⁹⁰

¹⁸² Artikel 13, §1 Decreet GIS.

¹⁸³ Van Gossum 2008, p. 16.

¹⁸⁴ Een beroepsbeoefenaar van de gezondheidszorg, die zorg verleent (artikel 2, 23° Decreet GIS).

¹⁸⁵ Een geheel van samenhangende activiteiten die op initiatief van de Vlaamse Regering of met haar steun of goedkeuring georganiseerd worden, die gericht zijn op de bestrijding van een of meer ziekten of aandoeningen en die tot doel hebben de gezondheid te bevorderen, te beschermen of te behouden door een of meer van de volgende methodieken toe te passen (artikel 2, 16° Decreet GIS).

¹⁸⁶ Een door de Vlaamse Regering erkende of door haar op enerlei wijze gefinancierde organisatie die op het terrein opdrachten uitvoert, methodieken toepast of diensten levert ter invulling van het Vlaamse gezondheidsbeleid, of een organisatie die dergelijke opdrachten vervult krachtens een wet of een decreet (artikel 2, 12° Decreet GIS).

¹⁸⁷ Een openbaar bestuur, instelling van openbaar nut, rechtspersoon of feitelijke vereniging die door de Vlaamse Regering erkend wordt voor uitvoering van de coördinatie van de onderlinge gegevensuitwisseling (artikel 2, 9° Decreet GIS).

¹⁸⁸ Een natuurlijke persoon die het voorwerp is van handelingen van zorgverlening of van een preventieprogramma (artikel 2, 20° Decreet GIS). Ook wel patiënt genoemd.

¹⁸⁹ Artikel 2, 19° Decreet GIS.

¹⁹⁰ Artikel 2, 17° Decreet GIS.

4.2.1 Het individueel gezondheidsdossier

Artikel 7 Decreet GIS bepaalt welke gegevens het individuele gezondheidsdossier ten minste moet bevatten. Hierbij kan worden gedacht aan de identiteit, het geslacht, de geboortedatum van de patiënt en een chronologisch overzicht van de uitgevoerde activiteiten van zorgverlening. Artikel 12 Decreet GIS bepaalt dat - behoudens andersluidende wettelijke bepaling - het individuele gezondheidsdossier gedurende dertig jaar wordt bewaard. Artikel 8 Decreet GIS bepaalt dat elke zorgverlener die bij de zorgverlening betrokken is, persoonlijke notities over de patiënt mag bijhouden. Dit zijn aantekeningen die door de beroepsbeoefenaar afzonderlijk worden opgeborgen en nodig zijn voor het persoonlijk gebruik van de zorgverlener.¹⁹¹

4.2.2 De verantwoordelijkheid voor het dossier

De verantwoordelijkheid voor een individueel gezondheidsdossier ligt bij een beroepsbeoefenaar in de gezondheidszorg. Dit is een beoefenaar, zoals bedoeld in het koninklijk besluit nummer 78 van 10 november 1967 betreffende de uitoefening van de gezondheidszorgberoepen, alsmede de beroepsbeoefenaar van een niet-conventionele praktijk, bedoeld in de wet van 29 april 1999 betreffende de niet-conventionele praktijken inzake de geneeskunde, de artseneijbereidkunde, de kinesitherapie, de verpleegkunde en de paramedische beroepen.¹⁹² Als de zorgverlening plaatsvindt in het kader van een organisatie met terreinwerking, wordt het individuele gezondheidsdossier bijgehouden door een organisatie met terreinwerking, onder verantwoordelijkheid van een beroepsbeoefenaar in de gezondheidszorg.

4.2.3 De uitwisseling van gegevens in het operationele systeem

Tussen zorgverleners en organisaties met terreinwerking kunnen de gegevens in het dossier alleen worden uitgewisseld, indien de patiënt hiervoor toestemming heeft verleend en de gegevens noodzakelijk zijn om de continuïteit en de kwaliteit van de zorgverlening te verzekeren (artikel 19, §1 Decreet GIS). Het Grondwettelijk Hof heeft echter in een arrest van 14 februari 2008 artikel 19, §1 Decreet GIS vernietigd, in zoverre het niet voorziet in een schriftelijke toestemming van de patiënt. Het Hof was van oordeel dat “de voorwaarde in artikel 4 Decreet GIS dat stelt dat de gegevensuitwisseling noodzakelijk moet zijn om de continuïteit en de kwaliteit van de zorgverlening te verzekeren, dermate ruim is dat zij onvermijdelijk ook gegevensuitwisselingen zal betreffen die niet onder de in artikel 7, §2 Wet Verwerking Persoonsgegevens (WVP) vermelde uitzonderingen vallen, zodat voor deze verwerkingen die niet in artikel 7, §2 WVP voorkomen, de schriftelijke toestemming

¹⁹¹ Artikel 2, 14° Decreet GIS.

¹⁹² Artikel 2, 3° Decreet GIS.

van de betrokken persoon vereist is.¹⁹³ Door de algemene bewoordingen waarin het is gesteld, doet artikel 19, §1 Decreet GIS afbreuk aan de bescherming waarin artikel 7, §2, onder a WVP voorziet, door het vereiste van een schriftelijke toestemming van de betrokken patiënt voor de verwerking van gezondheidsgegevens in het leven te roepen.” Het Hof stelt derhalve dat “artikel 19, §1 Decreet GIS vernietigd moet worden in zoverre het niet voorziet in de schriftelijke toestemming van de patiënt.”¹⁹⁴

In artikel 19, §3 Decreet GIS is bepaald dat de patiënt kan verlangen dat zijn toestemming wordt gevraagd voor elke specifieke verzending van gegevens afzonderlijk. Hij kan echter ook aan een zorgverlener of organisatie met terreinwerking toestemming geven voor alle specifieke verzendingen van gegevens in een bepaalde of onbepaalde periode, met dien verstande dat hij die toestemming kan beperken tot bepaalde categorieën van gegevens en bepaalde categorieën van zorgverleners of organisaties met terreinwerking en dat hij ze op elk moment kan intrekken. De Nationale Raad is in zijn advies positief gestemd over het bepaalde in artikel 19, §3 Decreet GIS, inhoudende dat de patiënt kan vragen dat zijn toestemming afzonderlijk wordt gevraagd voor elke specifieke verzending van gegevens. Bij gebrek aan andersluidende overeenstemming is het vanzelfsprekend dat het regime van de “afzonderlijke toestemming” gevolgd dient te worden.¹⁹⁵

Er geldt een vermoeden van stilzwijgende toestemming bij een verwijzing binnen de lopende zorgverlening, bij samenhangende activiteiten of in het kader van een preventieprogramma (artikel 19, §4 Decreet GIS). Indien de uitwisseling van gegevens voldoet aan een gereguleerde aangifteplicht, is geen toestemming vereist. Dit is tevens het geval indien de patiënt krachtens een wet of decreet verplicht onderworpen is aan zorgverlening of een preventieprogramma en de gegevens in het kader daarvan noodzakelijk zijn (Artikel 19, §5 Decreet GIS). Volgens de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL) dient, gelet op de snelle, eenvoudige consulteerbaarheid van elektronische dossiers, elke vorm van impliciete, stilzwijgende toestemming uitdrukkelijk te worden uitgesloten.¹⁹⁶ Vervolgens heeft het Hof artikel 19, §4, 2° en 3° van het Decreet vernietigd. Het Hof oordeelde dat “wat de stilzwijgende toestemming betreft, die veronderstelt wordt bij de verzending van de gegevens in het kader van samenhangende activiteiten van zorgverlening of van een preventieprogramma, artikel 19, §4, 2° en 3° afbreuk doet aan de minimale bescherming die wordt geboden door artikel 7 WVP.”¹⁹⁷

¹⁹³ In principe is de verwerking van 'gezondheidsgegevens' verboden op grond van artikel 7, §1 WVP. Op dit verbod bestaan echter, ingevolge artikel 7, §2 WVP, bepaalde uitzonderingsgevallen zoals de schriftelijke toestemming van de betrokkene.

¹⁹⁴ Grondwettelijk Hof 14 februari 2008, nr. 15/2008, BS 12 maart 2008.

¹⁹⁵ *Advies inzake het Decreet van de Vlaamse Gemeenschap betreffende het Gezondheidsinformatiesysteem* (advies van 16 juni 2006), Brussel: Nationale Raad 2007.

¹⁹⁶ Grondwettelijk Hof 14 februari 2008, nr. 15/2008, BS 12 maart 2008.

¹⁹⁷ *Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer over het voorontwerp van decreet van de Vlaamse Regering betreffende het gezondheidsinformatiesysteem* (advies van 10 mei 2004, 05 / 2004), Brussel: CBPL 2004, p. 6.

¹⁹⁷ Grondwettelijk Hof 14 februari 2008, nr. 15/2008, BS 12 maart 2008.

Bij elke gegevensuitwisseling in het operationele informatiesysteem wordt de pseudo-identiteit van de patiënt en de pseudo-identiteit van de zorgverlener of organisatie met terreinwerking die het individuele gezondheidsdossier bijhoudt, vermeld.¹⁹⁸ Hiermee maakt een persoon die het pseudoniem hanteert zich (her)kenbaar, zonder zijn ware identiteit prijs te geven. Gegevens met een pseudo-identiteit kunnen in bepaalde gevallen (bijvoorbeeld bij een eventuele betwisting) worden omgezet in identificerende gegevens. Een pseudo-identiteit schept dus de mogelijkheid om tegelijkertijd voor de één anoniem te blijven en bij een ander volledig bekend te zijn.¹⁹⁹ De pseudo-identiteit kan het nummer zijn van het rijksregister, van de sociale zekerheid of een andere unieke identificator.²⁰⁰

4.2.4 Kennisgeving, inzage en verzet

In artikel 42, §1 Decreet GIS is de informatieverplichting voor de zorgverlener geregeld. Dit artikel bepaalt dat de verantwoordelijke voor het individuele gezondheidsdossier de patiënt op de hoogte brengt dat een elektronische registratie wordt bijgehouden en dat de gegevens die daarin voorkomen, kunnen worden aangewend in het kader van het operationele en het epidemiologische informatiesysteem.

De artikelen 43 tot en met 46 Decreet GIS geven de regels weer met betrekking tot inzage in het individuele gezondheidsdossier. Aan een verzoek tot inzage in het individuele gezondheidsdossier en de elektronische registratie wordt binnen 45 dagen gevolg gegeven (artikel 46 Decreet GIS). De wijze van toegang geschiedt rechtstreeks of onrechtstreeks via een vrij door de patiënt gekozen beroepsbeoefenaar (artikel 43, §1 Decreet GIS). Gegevens die op een derde betrekking hebben zijn uitgesloten van dat recht van inzage.²⁰¹ De patiënt heeft tevens het recht op inzage in persoonlijke notities die hem betreffen, mits die inzage onrechtstreeks gebeurt door tussenkomst van een vrij door de patiënt gekozen beroepsbeoefenaar (artikel 43, §1, lid 2 Decreet GIS). Door dit onrechtstreekse inzagerecht kunnen de rechten van de patiënt ernstig worden aangetast. Het verdient daarom aanbeveling om in het ontwerp van het Decreet in één enkel inzagerecht te voorzien, zodat geen onderscheid wordt gemaakt tussen de persoonlijke notities en de overige gegevens opgenomen in het gezondheidsdossier.²⁰² Indien de patiënt jonger is dan 14 jaar, wordt het recht in artikel 43, §1 Decreet GIS uitgebreid tot zijn ouders, tenzij de minderjarige zich daartegen verzet.²⁰³ Wanneer sprake is van

¹⁹⁸ Artikel 21 Decreet GIS.

¹⁹⁹ J.E.J. Prins, 'Waken voor kenbaar maken. Over privacy, identiteit en anonimiteit in de informatiemaatschappij', in J.M. Titulaer-Meddens (red.), *Privacy: ons een zorg! De betekenis van privacybescherming voor het V&W-beleid*, Ministerie van Verkeer en Waterstaat 2002, p. 30-42.

²⁰⁰ Handelingen bij het Ontwerp van decreet betreffende het gezondheidsinformatiesysteem, *Parl. St.* VI. Parl. 2005-2006, nr. 531- 5, p. 5.

²⁰¹ Artikel 43, §1, lid 1 Decreet GIS.

²⁰² *Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer over het voorontwerp van decreet van de Vlaamse Regering betreffende het gezondheidsinformatiesysteem* (advies van 10 mei 2004, 05 / 2004), Brussel: CBPL 2004, p. 5.

²⁰³ Artikel 43, §2 Decreet GIS.

een gegevensoverdracht in het kader van het operationele informatiesysteem, kan het bestaan van verschillende systemen van inzage in de verschillende organisaties met terreinwerking tot problemen leiden. Een bepaalde organisatie verleent namelijk inzage in gegevens die via overdracht zijn verkregen, terwijl zij niet deskundig genoeg is om deze gegevens adequaat te duiden naar de patiënt. Het inzagerecht moet derhalve gepaard gaan met een recht op duiding en begeleiding, opdat het inzagerecht voor de patiënt tot een daadwerkelijke meerwaarde zou kunnen leiden.²⁰⁴

Het recht op verzet is in het Decreet GIS niet geregeld voor het individueel gezondheidsdossier. Voor de elektronische registratie is in de artikelen 47 en 48 Decreet GIS wel geregeld dat de patiënt zich, wegens zwaarwichtige en gerechtvaardigde redenen die verband houden met zijn bijzondere situatie, kan verzetten tegen de opname van zijn gegevens in de elektronische registratie. Indien de patiënt jonger is dan 14 jaar, kan het verzet ook worden uitgeoefend door zijn ouders (artikel 47, §3 Decreet GIS).

4.2.5 Toezichtcommissie

Het Decreet GIS (artikel 55-59) stelt een toezichtcommissie in, bestaande uit drie leden van de CBPL, een beroepsbeoefenaar van de gezondheidszorg, een deskundige in het informaticarecht en een deskundige in de informaticatechnologie. De toezichtcommissie is belast met het toezicht op de naleving van het Decreet via onderzoek en controle ter plaatse. Daarnaast heeft de toezichtcommissie een adviserende functie en kan zij klachten behandelen en machtiging verlenen voor de verdere verwerking van gegevens.

De toezichtcommissie wordt opgeheven zodra binnen de CBPL een gemeenschappelijk Sectoraal Comité is opgericht, dat specifiek toeziet op de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens die de gezondheid betreffen. Dit Sectoraal Comité moet zijn opgericht ter uitvoering van een samenwerkingsakkoord tussen de federale overheid, de gemeenschappen en de gewesten (artikel 88 Decreet GIS). Het Sectoraal Comité kan echter niet in de plaats komen van de toezichtcommissie, nu het geen gemeenschappelijk comité betreft en hierover geen samenwerkingsakkoord is gesloten.²⁰⁵

²⁰⁴ Advies van de Algemene Raad over het voorontwerp van decreet betreffende het gezondheidsinformatiesysteem (advies van 16 september 2003, AR/VHE/ADV/001), Brussel: Algemene Raad 2003, p. 6.

²⁰⁵ J. Put, *Werken met gezondheidsgegevens in de integrale jeugdhulp* (doctoraalscriptie Leuven), 2007, p. 30.

4.3 Het eHealth-platform

Eind december 2004 gaf de Ministerraad groen licht voor de oprichting van BeHealth. Wegens het gebrek aan vertrouwen tussen de betrokken partijen duurde het tot 27 december 2006 voordat de oprichting van BeHealth bij wet werd afgekondigd.²⁰⁶ De wet tot oprichting van BeHealth kreeg echter niet onmiddellijk gevolg, maar leidde tot de wet van 21 augustus 2008 waarin het eHealth-platform werd opgericht. De 'B' is weggefallen, ter aanduiding dat het platform niet enkel beperkt is tot het federale niveau.²⁰⁷ Terwijl het Decreet GIS slechts gelding heeft binnen de Vlaamse Gemeenschap, blijft het eHealth-platform voor zijn werking niet tot het federale niveau beperkt. Daarnaast wordt het eHealth-platform, in tegenstelling tot het Decreet GIS, niet verplicht gesteld.²⁰⁸

4.3.1 Inrichting

Het eHealth-platform wordt opgericht als een openbare instelling van sociale zekerheid en krijgt een Beheerscomité van 31 leden, bestaande uit vertegenwoordigers van de zorgverleners, zorginstellingen en de overheid. Het Beheerscomité is onafhankelijk, aangezien de personen zeer uiteenlopende belangen vertegenwoordigen zodat een verzoek vanwege een bepaalde actor niet per se zal worden ingewilligd. Daarnaast worden de beslissingen door het Beheerscomité bij volstrekte meerderheid genomen.²⁰⁹ De administrateur-generaal van de Kruispuntbank van de Sociale Zekerheid (KSZ) wordt belast met het dagelijks beheer van het platform. De KSZ is een elektronisch netwerk tussen de instellingen van de sociale zekerheid en het rijksregister en vormt daarmee het kruispunt tussen de verschillende gegevensbanken van deze sociale zekerheidsinstellingen. De concrete uitvoering van wettelijke opdrachten van het platform wordt geregeld in een beheersovereenkomst met de Staat. Binnen het platform wordt een Overlegcomité met gebruikers ervan opgericht. Het Overlegcomité staat het Beheerscomité bij in de invulling van zijn opdrachten.²¹⁰

Op 1 maart 2007 is het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid binnen het CBPL opgericht voor de verwerking van gezondheidsgegevens. Het Sectoraal Comité bestaat uit twee afdelingen: de afdeling sociale zekerheid en de afdeling gezondheid.²¹¹ Elke mededeling van

²⁰⁶ Wet houdende diverse bepalingen van 27 december 2006, BS 28 december 2006.

²⁰⁷ J. Dumortier, 'Recente ontwikkelingen in het privacyrecht 2008-2009', in: *Recht in beweging - 17e VGR Alumnidag*, Antwerpen: Maklu 2010, p. 175.

²⁰⁸ B. Aerts, *Privacybescherming en de elektronische gegevensverwerking in de gezondheidszorg* (doctoraalscriptie Gent), 2010, p. 76.

²⁰⁹ Grondwettelijk Hof 18 maart 2010, nr. 29/2010, BS 18 maart 2010.

²¹⁰ Dumortier 2010, p. 176.

²¹¹ Artikel 52 Wet houdende diverse bepalingen van 1 maart 2007, BS 14 maart 2007 en artikel 37 §2 Wet tot wijziging van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Commissie voor de bescherming van de persoonlijke levenssfeer en tot uitbreiding van haar bevoegdheden van 26 februari 2003, BS 26 juni 2003.

persoonsgegevens die met tussenkomst van het eHealth-platform wordt verricht, vereist een machtiging van het Sectoraal Comité.²¹² Het Sectoraal Comité gaat bij het evalueren van een uitwisseling van persoonsgegevens na of het in overeenstemming is met de wettelijke en reglementaire bepalingen tot bescherming van de persoonlijke levenssfeer. Daarnaast mogen de persoonsgegevens alleen worden uitgewisseld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en dienen zij, uitgaande van deze doeleinden, toereikend, ter zake dienend en niet overmatig te zijn. Hiermee wordt de garantie geboden dat niet meer persoonsgegevens worden uitgewisseld dan deze die relevant zijn in het licht van het beoogde doeleinde.²¹³ Het Sectoraal Comité zal tevens onderzoeken met welke veiligheidsmaatregelen de uitwisseling van persoonsgegevens gepaard gaat. In geval van een gunstige beslissing van het Sectoraal Comité over een bepaalde mededeling van persoonsgegevens dient het platform zijn verwijzingsrepertorium aan te passen opdat de mededeling effectief plaats zou kunnen vinden.²¹⁴

Daarnaast dient door het Sectoraal Comité een informatieveiligheidsconsulent aangewezen te worden, die over de nodige onafhankelijkheid en deskundigheid beschikt om zijn taak naar behoren te vervullen. De informatieveiligheidsconsulent wordt belast met het toezicht op de verwerkingen en uitwisselingen van persoonsgegevens door het eHealth-platform, waarbij hij bijzondere aandacht dient te besteden aan de bescherming van de persoonlijke levenssfeer van de personen op wie de persoonsgegevens in kwestie betrekking hebben. Daarnaast dient het platform tevens een arts aan te wijzen, onder wiens toezicht en verantwoordelijkheid elke verwerking zal gebeuren van persoonsgegevens die de gezondheid betreffen. Het Sectoraal Comité zal, alvorens de aanstelling van de informatieveiligheidsconsulent en de arts, advies verstrekken. Hierbij gaat het comité na of de betrokken kandidaat beschikt over voldoende kennis aangaande het netwerk van de gezondheidszorgsector, de informatica en de beveiligingstechnieken. Daarnaast zal het comité onderzoeken of de kandidaat geen andere activiteiten uitoefent die onverenigbaar zijn met zijn taak als informatieveiligheidsconsulent of arts en of de tijd die hij aan deze taak wijdt wel volstaat.²¹⁵

Het eHealth-platform zal - net als in het EPD - zelf geen inhoudelijke persoonsgegevens centraal opslaan. Een belangrijke taak van het platform bestaat uit het leveren van basisdiensten, zoals het gebruikers- en het toegangsbeheer, het verwijzingsrepertorium, de logging, de codering en het

²¹² Artikel 11 van de Wet houdende oprichting en organisatie van het eHealth-platform van 21 augustus 2008, BS 13 oktober 2008.

²¹³ *Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer met betrekking tot een ontwerp van wet houdende oprichting en organisatie van het eHealth-platform* (advies van 2 april 2008, A/2008/016), Brussel: CBPL 2008, p. 9.

²¹⁴ *Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer met betrekking tot een ontwerp van wet houdende oprichting en organisatie van het eHealth-platform* (advies van 2 april 2008, A/2008/016), Brussel: CBPL 2008, p. 21.

²¹⁵ *Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer met betrekking tot een ontwerp van wet houdende oprichting en organisatie van het eHealth-platform* (advies van 2 april 2008, A/2008/016), Brussel: CBPL 2008, p. 19-20.

anonymiseren, de elektronische datering, een portaalsite en een persoonlijke elektronische mailbox voor elke zorgverlener.²¹⁶ Hieronder zal ik de voor dit onderzoek belangrijkste basisdiensten gaan bespreken.

4.3.2 Verwijzingsrepertorium

Om de uitwisseling van gezondheidsgegevens mogelijk te maken, wordt er een lijst aangelegd waarop een verwijzing wordt opgenomen naar één of meerdere netwerken waarbij de zorgverleners of zorginstellingen die over patiëntgegevens beschikken zijn aangesloten.²¹⁷ Dit is het zogenaamde ‘verwijzingsrepertorium’. In het verwijzingsrepertorium wordt aangegeven bij welke actoren in de gezondheidszorg welke typen van gegevens worden bewaard met betrekking tot welke patiënten. Het verwijzingsrepertorium bevat dus zelf geen gegevens, maar enkel verwijzingen naar plaatsen waar bepaalde typen gezondheidgegevens te vinden zijn. De patiënt dient eerst toestemming te hebben gegeven, voordat de verwijzingsgegevens in het repertorium worden opgenomen.²¹⁸ De toestemming moet een vrije, specifieke en op informatie berustende wilsuiting zijn: de patiënt moet met name vooraf geïnformeerd zijn over zijn rechten en het precieze oogmerk van de verwerking.²¹⁹ Daarnaast moet de toestemming verplicht schriftelijk worden gegeven, aangezien het om gevoelige gegevens gaat.²²⁰ De wet van 21 augustus 2008 op het eHealth-platform hanteert echter de notie ‘akkoord’ in plaats van ‘schriftelijke toestemming’, waardoor het risico ontstaat dat de weg wordt vrij gemaakt voor uitdrukkelijke toestemmingen zonder schriftelijke vorm.²²¹

Er ontstond kritiek op de toestemming van de betrokken patiënten bij aanduiding in een verwijzingsrepertorium waar gezondheidsgegevens over hen worden bewaard. In het arrest van 18 maart 2010 heeft het Grondwettelijk Hof onderzocht of de wet van 21 augustus 2008 op het eHealth-platform het recht op eerbiediging van het privéleven en de bescherming van de persoonsgegevens in het bijzonder schendt.²²² Het Hof overweegt hierbij dat de medische databanken waarin de persoonlijke gezondheidsgegevens worden bewaard en waarvoor de wet van 21 augustus 2008 slechts in een systeem van beveiligde uitwisseling voorziet, onverkort onderworpen blijven aan de wet van 8 december 1992 over de verwerking van persoonsgegevens (WVP). De wetgever heeft in artikel 6 van de wet van 21 augustus 2008 uitdrukkelijk bepaald dat hij niet van de WVP heeft willen afwijken, waardoor de waarborgen van de WVP van toepassing zijn.²²³

²¹⁶ M. Detiége, 'Wetsontwerp houdende oprichting en organisatie van het eHealth-platform', *Belgische Kamer van Volksvertegenwoordigers*, nr. 1257/003-2008, p. 7.

²¹⁷ Zie <www.cozo.be> (Inschrijving in het eHealth verwijsregister).

²¹⁸ Dumortier 2010, p. 176.

²¹⁹ Toestemming in de zin van artikel 1, §8 WVP.

²²⁰ Detiége 2008, p. 12.

²²¹ P. de Hert & R. Saelens, 'eHealth-wet: nog enkele onduidelijkheden', *De Juristenkrant* 2010-207, p. 13.

²²² De Hert & Saelens 2010, p. 12.

²²³ Grondwettelijk Hof 18 maart 2010, nr. 29/2010, BS 18 maart 2010.

Na het verlenen van toestemming door de patiënt, kunnen zijn of haar gegevens elektronisch worden uitgewisseld met een andere zorgverlener die de patiënt behandelt. Er dient wel een behandelrelatie te bestaan tussen de patiënt en de zorgverlener. Alvorens een zorgverlener effectief de patiëntgegevens kan raadplegen, zal worden gecontroleerd of de patiënt in behandeling is bij deze zorgverlener. Daarnaast kan de patiënt - middels het invoeren van een formulier - bepaalde zorgverleners uitsluiten van toegang tot zijn of haar gegevens. De zorgverlener mag de patiëntgegevens enkel gebruiken voor de doeleinden waarvoor ze toegang hebben.

4.3.3 Systeem voor end-to-end vercijfering

Bij het uitwisselen van patiëntgegevens via het platform worden deze gegevens vercijferd tussen de verzender en de ontvanger middels het systeem voor end-to-end vercijfering. Deze basisdienst zorgt voor het overbrengen van de volledige, niet-gewijzigde gegevens van het ene punt naar het andere door ze onleesbaar te maken (vercijfering), zodat niemand anders deze gegevens kan lezen. Om de verzender en de ontvanger de garantie te bieden dat de persoonsgegevens op dezelfde patiënt betrekking hebben, wordt de patiënt in deze vercijferde berichten geïdentificeerd aan de hand van zijn identificatienummer van de sociale zekerheid (INSZ). Dit is een uniek identificatienummer, toegekend aan natuurlijke personen met de Belgische nationaliteit en is vergelijkbaar met het Nederlandse BSN. De eHealth-wet verplicht niet dat het INSZ ook in andere omstandigheden dient te worden gebruikt. Het wordt er enkel in opgenomen voor gegevensuitwisseling via het eHealth-platform.²²⁴

Sommige pleiten voor het gebruik van een specifiek identificatienummer voor de gezondheidssector dat wordt afgeleid van het INSZ.²²⁵ Hierbij moet elke actor over software beschikken om van het INSZ een specifiek gezondheidsnummer af te leiden, wat betekent dat dergelijke software op tienduizenden plaatsen dient te worden geïnstalleerd. Dit is haast onmogelijk, waardoor het risico ontstaat dat actoren bij de uitwisseling van patiëntgegevens niet over hetzelfde afgeleide gezondheidsnummer beschikken en er derhalve geen waarborg bestaat dat de verzender en de ontvanger het over dezelfde persoon hebben.²²⁶ Indien alle burgers met één nummer worden gekoppeld, wordt tevens de basis gelegd voor een controlesamenleving wat bijzonder kwetsbaar is voor misbruik bij bijvoorbeeld hacking.²²⁷ De toepassing van een specifiek identificatienummer voor de gezondheidssector is derhalve niet het meest aangewezen instrument om de bescherming van de persoonlijke levenssfeer te waarborgen. De toepassing van andere privacybeschermende technieken, zoals de creatie van een systeem waarbij de gegevens niet centraal worden opgeslagen en het

²²⁴ Zie <www.ehealth.fgov.be> (INSZ als unieke identificatiesleutel?).

²²⁵ F. Robben, 'De invoering van een elektronisch leesbare sociale identiteitskaart voor alle Belgen', *Computerrecht* 1998-1, p. 14-15.

²²⁶ Zie <www.ehealth.fgov.be> (INSZ als unieke identificatiesleutel?).

²²⁷ Grondwettelijk Hof 18 maart 2010, nr. 29/2010, BS 18 maart 2010.

machtigingsvereiste door het Sectoraal Comité in combinatie met de aanstelling van een toezichthoudende arts en een informatieveiligheidsconsulent is volgens de CBPL en het Grondwettelijk Hof in zijn arrest van 18 maart 2010 voldoende voor het verhinderen van ongewilde en verboden koppelingen van verschillende databestanden via het eHealth-platform.²²⁸

4.3.4 Geïntegreerd gebruikers- en toegangsbeheer

Via het geïntegreerd systeem van gebruikers- en toegangsbeheer dient een gebruiker, alvorens hij toegang krijgt tot het platform, met zijn elektronische identiteitskaart of een gelijkwaardig middel zich te legitimeren. In betrouwbare gegevensbanken wordt dan nagegaan of hij de juiste hoedanigheden en machtigingen bezit (controle ex ante).²²⁹ De uitwisseling van patiëntgegevens wordt achteraf gelogd, om in geval van klachten, achteraf te kunnen nagaan of de toegang rechtmatig was (controle ex post). Hierbij wordt enkel geregistreerd wie wat wanneer heeft gedaan. De registratie bevat dus geen inhoudelijke gegevens. De patiënt kan zelf de loggegevens inzien, zodat hij kan vaststellen wie zijn persoonsinformatie heeft opgevraagd. In het kader van de wettelijke bescherming van de persoonlijke levenssfeer is het belangrijk dat de toegang van iedere zorgverlener gecontroleerd dient te worden en dat iedere zorgverlener slechts toegang heeft tot de gegevens waarop hij uit hoofde van zijn functie recht heeft.²³⁰

4.4 Oplossing knelpunten: Decreet GIS en het eHealth-platform

In deze paragraaf ga ik onderzoeken of het recht op privacy in het EPD beter kan worden gegarandeerd met de maatregelen die zijn genomen in het Decreet GIS en het eHealth-platform ter bescherming van de privacy van de patiënten. Per aspect zal ik een oplossing proberen te vinden voor de geïnventariseerde technische, juridische en politieke knelpunten.

Schaalgrootte

Teneinde het technische knelpunt van onbevoegde toegang tot het EPD te voorkomen, dient er adequaat toezicht plaats te vinden op een rechtmatige gegevensuitwisseling. Hierbij kan men denken aan het aanwijzen van een toezichtcommissie (zoals in het Decreet GIS²³¹) of een arts, een adviseur informatieveiligheid en het Sectoraal Comité (zoals in het eHealth-platform). Het Sectoraal Comité is vergelijkbaar met het CBP in Nederland. Een FG kan bijvoorbeeld worden belast met het verlenen van

²²⁸ Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer met betrekking tot een ontwerp van wet houdende oprichting en organisatie van het eHealth-platform (advies van 2 april 2008, A/2008/016), Brussel: CBPL 2008, p. 17 en Grondwettelijk Hof 18 maart 2010, nr. 29/2010, BS 18 maart 2010.

²²⁹ Zie <www.ehealth.fgov.be> (Basisdienst Geïntegreerd gebruikers- en toegangsbeheer).

²³⁰ Detiége 2008, p. 22.

²³¹ Artikel 55-59 Decreet GIS.

een machtiging, alvorens tot gegevensuitwisseling mag worden overgegaan.²³² Toezicht door een arts en een deskundige in de informatieveiligheid zorgt er tevens voor dat de afname van de kwaliteit van medische gegevens (politiek knelpunt) wordt opgelost, aangezien er dan nuttig gebruik wordt gemaakt van horizontaal toezicht en specialistische kennis.

De rol van zorgverzekeraars

Teneinde het risico van ‘profiling’ (politiek knelpunt) te voorkomen dient er toezicht te worden uitgeoefend op een rechtmatige gegevensverwerking. Allereerst dient er een, met het eHealth-platform vergelijkbaar, geïntegreerd systeem van gebruikers- en toegangsbeheer te worden ingericht binnen het EPD, opdat de toegang van iedere zorgverlener gecontroleerd kan worden en iedere zorgverlener slechts toegang heeft tot de gegevens waarop hij uit hoofde van zijn functie recht heeft.²³³

Naast controle via het geïntegreerd systeem van gebruikers- en toegangsbeheer dient toezicht te worden uitgeoefend op een rechtmatige gegevensuitwisseling. Het toezicht moet zien op het verlenen van een schriftelijke toestemming door de patiënt voor het registreren en verwerken van de gegevens.²³⁴ De gegevensverwerking dient tevens noodzakelijk te zijn om de continuïteit en de kwaliteit van de zorgverlening te verzekeren en er moet een behandelrelatie bestaan tussen de zorgverlener en de patiënt.²³⁵ Nadat hierop effectieve controle heeft plaatsgevonden, dient de FG een machtiging voor de gegevensuitwisseling te verlenen.²³⁶

“Geen bezwaar”-systeem

Volgens de CBPL dient, gelet op de snelle, eenvoudige consulteerbaarheid van elektronische dossiers, elke vorm van impliciete, stilzwijgende toestemming uitdrukkelijk te worden uitgesloten.²³⁷ In lijn met de CBPL dient het “geen bezwaar-systeem” dan ook te worden omgezet in een uitdrukkelijke toestemming van de patiënt voor het registreren en uitwisselen van zijn of haar gegevens. Hierdoor wordt strijdigheid met artikel 7:457 BW opgelost. De toestemming van de patiënt dient tevens verplicht schriftelijk te worden gegeven, aangezien het om gevoelige gegevens gaat.²³⁸

Daarnaast moet de toestemming van de patiënt een vrije, specifieke en op informatie berustende wilsuiting zijn: de patiënt moet met name vooraf geïnformeerd zijn over zijn rechten en het precieze

²³² Zie Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer met betrekking tot een ontwerp van wet houdende oprichting en organisatie van het eHealth-platform (advies van 2 april 2008, A/2008/016), Brussel: CBPL 2008, p. 19-20.

²³³ Detiège 2008, p. 22.

²³⁴ Dumortier 2010, p. 176.

²³⁵ Zie Advies inzake het Decreet van de Vlaamse Gemeenschap betreffende het Gezondheidsinformatiesysteem (advies van 16 juni 2006), Brussel: Nationale Raad 2007.

²³⁶ Zie Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer met betrekking tot een ontwerp van wet houdende oprichting en organisatie van het eHealth-platform (advies van 2 april 2008, A/2008/016), Brussel: CBPL 2008, p. 17 en Grondwettelijk Hof 18 maart 2010, nr. 29/2010, BS 18 maart 2010.

²³⁷ Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer over het voorontwerp van decreet van de Vlaamse Regering betreffende het gezondheidsinformatiesysteem (advies van 10 mei 2004, 05 / 2004), Brussel: CBPL 2004, p. 6.

²³⁸ Detiège 2008, p. 12.

oogmerk van de verwerking.²³⁹ Hierdoor wordt het politieke knelpunt van een ondoorzichtige registratie van patiëntgegevens opgelost.

Behandelrelatie

De patiënt dient geïnformeerd te worden over de personen of instellingen bij wie de gegevens worden of zullen worden opgevraagd en over de personen of instellingen aan wie de gegevens kunnen worden verstrekt, alsmede de redenen daarvoor. Er dient een informatieverplichting voor de zorgverlener te bestaan in het EPD.²⁴⁰ Nadat de patiënt is geïnformeerd moet de patiënt zijn of haar toestemming verlenen voor de gegevensuitwisseling.²⁴¹ Alleen in dat geval kan het bestaan van een behandelrelatie tussen zorgverlener en patiënt compleet worden gewaarborgd en wordt het technische knelpunt opgelost.

Schending van de doelbinding

Teneinde gegevensuitwisseling binnen de reikwijdte van het noodzakelijkheidsvereiste ingevolge artikel 7:457, tweede lid, BW te brengen, dient in het EPD erop te worden toegezien dat de patiëntgegevens alleen mogen worden uitgewisseld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De persoonsgegevens moeten, uitgaande van deze doeleinden, toereikend, ter zake dienend en niet overmatig te zijn.²⁴² Indien aan bovengenoemde criteria wordt voldaan, dient de FG een machtiging te verlenen voor de gegevensuitwisseling.

UZI-pas

Zowel in het Decreet GIS als in het eHealth-platform wordt geen gebruik gemaakt van een UZI-pas. Wel kan door middel van een sluitend beheer van de gebruikers en van de toegang tot het platform (zoals in het eHealth-platform) worden voorkomen dat degenen die daartoe niet geautoriseerd zijn toegang krijgen tot de databases van de zorgverleners. Hierbij wordt gebruik gemaakt van controle ex ante en controle ex post: in betrouwbare gegevensbanken wordt nagegaan of de zorgverlener de juiste hoedanigheden en machtigingen bezit en de uitwisseling van patiëntgegevens wordt gelogd.²⁴³

Daarnaast dient ‘eerste lijns’ toezicht op het gebruik van de UZI-pas te worden uitgeoefend. Hierbij kan men denken aan toezicht door een arts of een adviseur informatieveiligheid.²⁴⁴

²³⁹ Toestemming in de zin van artikel 1, §8 WVP.

²⁴⁰ In het Decreet Gis is deze informatieverplichting geregeld in artikel 42, §1.

²⁴¹ Dumortier 2010, p. 176.

²⁴² Zie *Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer met betrekking tot een ontwerp van wet houdende oprichting en organisatie van het eHealth-platform* (advies van 2 april 2008, A/2008/016), Brussel: CBPL 2008, p. 9 en artikel 19, §1 Decreet GIS.

²⁴³ Zie <www.ehealth.fgov.be> (Basisdienst Geïntegreerd gebruikers- en toegangsbeheer).

²⁴⁴ Artikel 55-59 Decreet GIS.

Logging

In het eHealth-platform wordt via controle ex post in het systeem van geïntegreerd gebruikers- en toegangsbeheer tevens gebruik gemaakt van logging achteraf. Controle vindt echter alleen plaats in geval van klachten, waardoor mogelijk misbruik niet wordt voorkomen. Het Decreet GIS biedt geen richtlijnen voor een controle op rechtmatige uitwisseling van patiëntgegevens.

Teneinde het technische knelpunt op te lossen en misbruik van inzage in alle patiëntendossiers te voorkomen, dient de toegang van iedere zorgverlener gecontroleerd te worden en moet erop worden toegezien dat iedere zorgverlener slechts toegang heeft tot de gegevens waarop hij uit hoofde van zijn functie recht heeft.²⁴⁵ Dit toezicht dient plaats te vinden door het CBP, een arts en een adviseur informatieveiligheid (zoals in het Decreet GIS en het eHealth-platform). Daarnaast zorgt het instellen van een machtigingsvereiste er tevens voor dat slechts de zorgverlener die een behandelrelatie met de patiënt heeft over de gegevens kan beschikken. Indien adequaat toezicht wordt uitgeoefend kunnen de juridische knelpunten die logging achteraf met zich mee brengt - uitholling van artikel 7:457 BW en strijdigheid met artikel 13 Wbp - worden opgelost.

Recht op inzage

Teneinde het politieke knelpunt van het aanleggen van een “tweede weg” naar informatie uit het EPD op te lossen, dient een onafhankelijk orgaan, zoals een FG, toe te zien op de veiligheid van de informatiesystemen (zie principe 9.4 R (97) 5). Indien naar het voorstel van de minister inzage in de medische gegevens vorm wordt gegeven via de website of portal van de zorgverlener, dient toegang voor de patiënt te worden verleend via de zorgverlener die daartoe geautoriseerd is (zie principe 9.2 onder a) zodat alleen bevoegden inzage hebben in de patiëntgegevens. Daarnaast dienen de zorgverleners onderling toezicht te houden op elkaar, teneinde het politieke knelpunt van de afname van de kwaliteit van patiëntgegevens tegen te gaan.

Teneinde strijdigheid met artikel 35 Wbp en artikel 7:456 BW op te lossen, dient in het EPD te worden opgenomen dat de patiënt rechtstreeks inzage dient te krijgen in zijn of haar gegevens.²⁴⁶ Hierop dient adequaat toezicht te worden uitgeoefend, opdat het politieke knelpunt van de aanleg van “een tweede weg” naar informatie uit het EPD wordt opgelost.

Daarnaast dient het inzagerecht gepaard te gaan met een recht op duiding en begeleiding, opdat de afname van de kwaliteit van informatie wordt voorkomen (politiek knelpunt).²⁴⁷

²⁴⁵ Detiége 2008, p. 22.

²⁴⁶ Artikel 43, §1 Decreet GIS.

²⁴⁷ *Advies van de Algemene Raad over het voorontwerp van decreet betreffende het gezondheidsinformatiesysteem* (advies van 16 september 2003, AR/VHE/ADV/001), Brussel: Algemene Raad 2003, p. 6.

Recht op vernietiging

Teneinde te garanderen dat volledige vernietiging in het dossier plaatsvindt overeenkomstig artikel 36 Wbp en artikel 7:455 BW, dient er toezicht plaats te vinden op een volledige vernietiging van de opgenomen patiëntgegevens in een digitaal dossier.

Toezicht op het EPD

Door middel van het aanwijzen van een toezichtcommissie (zoals in het Decreet GIS²⁴⁸) of een arts, een adviseur informatieveiligheid en het CBP (zoals in het eHealth-platform) vindt horizontaal toezicht plaats en wordt derhalve gebruik gemaakt van specialistische kennis aanwezig bij de veldpartijen. Het horizontaal toezicht levert derhalve schaalvoordelen op en kent een geringe capaciteitsbelasting van de toezichthoudende instanties.²⁴⁹

4.5 Conclusie

In dit hoofdstuk is duidelijk geworden dat zowel in het Decreet GIS als het eHealth-platform maatregelen zijn getroffen ter bescherming van de persoonlijke levenssfeer van patiënten die in het EPD nog (gedeeltelijk) ontbreken. Hierdoor worden duidelijke richtsnoeren geboden voor een oplossing van de geïnventariseerde knelpunten die het EPD kent met betrekking tot het recht op privacy.

Allereerst hanteren het Decreet GIS en het eHealth-platform niet een “geen bezwaar”-systeem. Patiëntgegevens worden alleen uitgewisseld, indien de patiënt hiervoor toestemming heeft verleend en de gegevens noodzakelijk zijn om de continuïteit en de kwaliteit van de zorgverlening te verzekeren.²⁵⁰ Onder toestemming wordt een vrije, specifieke en op informatie berustende wilsuiting verstaan. De patiënt dient met name vooraf geïnformeerd te zijn over zijn rechten en het precieze oogmerk van de verwerking.²⁵¹ Daarnaast dient de toestemming schriftelijk te zijn.²⁵²

Zoals bekend mogen slechts zorgverleners die een behandelrelatie met de patiënt hebben, gegevens raadplegen. Ter waarborging hiervan kan gebruik worden gemaakt van een geïntegreerd systeem van gebruikers- en toegangsbeheer, met een controle ex ante en een controle ex post. In betrouwbare gegevensbanken wordt nagegaan of de zorgverlener de juiste hoedanigheden en machtigingen bezit en de uitwisseling van patiëntgegevens wordt gelogd.²⁵³ Logging achteraf biedt echter alleen voldoende waarborgen om misbruik tegen te gaan, indien hierop adequaat toezicht wordt uitgeoefend. Behalve

²⁴⁸ Artikel 55-59 Decreet GIS.

²⁴⁹ Krabben 2010, p. 9.

²⁵⁰ Artikel 19, §1 Decreet GIS.

²⁵¹ Toestemming in de zin van artikel 1, §8 WVP.

²⁵² Grondwettelijk Hof 14 februari 2008, nr. 15/2008, BS 12 maart 2008.

²⁵³ Zie <www.ehealth.fgov.be> (Basisdienst Geïntegreerd gebruikers- en toegangsbeheer).

schriftelijke toestemming van de patiënt en autorisatie van de zorgverlener dient in het EPD (in navolging van het eHealth-platform) tevens een machtiging te worden verstrekt voor uitwisseling van de patiëntgegevens. In het eHealth-platform wordt de machtiging - indien het een rechtmatige gegevensuitwisseling betreft - door het Sectoraal Comité verstrekt.²⁵⁴ In Nederland kan men bijvoorbeeld een FG belasten met het controleren van de gegevensuitwisseling en het verstrekken van een dergelijke machtiging. Het verdient tevens aanbeveling om patiëntgegevens bij de uitwisseling te versleutelen, zodat de gegevens onleesbaar zijn voor onrechtmatige zorgverleners. Om de verzender en ontvanger de garantie te bieden dat de gegevens op dezelfde patiënt betrekking hebben, dient de patiënt in deze versleutelde berichten geïdentificeerd te zijn aan de hand van zijn of haar BSN (in het eHealth-platform is dit het INSZ) of een pseudo-identiteit.²⁵⁵

Wanneer de patiënt inzage wil verkrijgen in zijn of haar gegevens dient er sprake te zijn van een rechtstreekse inzage, zodat de patiënt zelfstandig het recht op inzage kan uitoefenen.²⁵⁶ Daarnaast dient het inzagerecht gepaard te gaan met een recht op duiding en begeleiding, zodat het inzagerecht voor de patiënt tot een daadwerkelijke meerwaarde zou kunnen leiden.²⁵⁷

Als overkoepelend toezicht dient controle op de wettigheid van de uitwisseling van patiëntgegevens plaats te vinden door bijvoorbeeld een ingestelde toezichtcommissie (zoals in het Decreet GIS²⁵⁸) of zoals in het eHealth-platform, een arts, een adviseur informatieveiligheid en het Sectoraal comité.²⁵⁹ Zij dienen over de nodige onafhankelijkheid en deskundigheid te beschikken om hun taak naar behoren te vervullen. In het EPD kan het CBP worden belast met het instellen van een dergelijke commissie.

²⁵⁴ *Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer met betrekking tot een ontwerp van wet houdende oprichting en organisatie van het eHealth-platform* (advies van 2 april 2008, A/2008/016), Brussel: CBPL 2008, p. 19-20.

²⁵⁵ Artikel 21 Decreet GIS.

²⁵⁶ *Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer over het voorontwerp van decreet van de Vlaamse Regering betreffende het gezondheidsinformatiesysteem* (advies van 10 mei 2004, 05 / 2004), Brussel: CBPL 2004, p. 5.

²⁵⁷ *Advies van de Algemene Raad over het voorontwerp van decreet betreffende het gezondheidsinformatiesysteem* (advies van 16 september 2003, AR/VHE/ADV/001), Brussel: Algemene Raad 2003, p. 6.

²⁵⁸ Artikel 55-59 Decreet GIS.

²⁵⁹ *Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer met betrekking tot een ontwerp van wet houdende oprichting en organisatie van het eHealth-platform* (advies van 2 april 2008, A/2008/016), Brussel: CBPL 2008, p. 19-20.

5 Regionale opzet van het EPD

5.1 Inleiding

In veel regio's binnen Nederland vindt al geruime tijd uitwisseling van medische gegevens in het kader van de zorgverlening plaats.²⁶⁰ Dit gebeurde vooruitlopend op een wettelijke basis, die er dus niet is gekomen. Het CBP heeft vastgesteld dat de huidige regionale systemen vaak niet voldoen aan de Wbp, waardoor het aanpakken van de regionale EPD's derhalve meer prioriteit lijkt te hebben dan het opzetten van één landelijk EPD.²⁶¹ Zo pleit de Eerste Kamer in een brief aan de minister voor een regionale gegevensuitwisseling en het stopzetten van het LSP. De senatoren eisen dat er nadrukkelijk moet worden gekeken naar de veiligheid van gegevensuitwisseling: "Er moet een juridisch kader worden neergezet, met duidelijke rechten en plichten voor zowel patiënt als zorgaanbieder."²⁶² Ondanks bezwaren van de Eerste Kamer wil de minister regionaal opgeslagen gegevens via het LSP landelijk gaan uitwisselen.²⁶³ Hiermee komt zij tegemoet aan de wens van de Tweede Kamer om het LSP "niet naar de prullenbak te verwijzen".²⁶⁴

In dit hoofdstuk zal ik gaan onderzoeken of het recht op privacy beter wordt gegarandeerd door de bestaande regionale EPD's aan te pakken dan één groot nieuw landelijk EPD op te zetten. In paragraaf 5.2 zal ik het debat uiteenzetten over de voorkeur voor een regionale opzet van het EPD boven de invoering van een private doorstart van het EPD, met behoud van het LSP. Hierin zal ik de voor- en nadelen van een regionaal systeem voor gegevensuitwisseling gaan bespreken, voortgekomen uit de discussie in de Eerste en de Tweede Kamer en de koepel- en brancheorganisaties van zorgverleners en apothekers. In paragraaf 5.3 ga ik mij richten op de bevindingen van het CBP inzake de privacy bij regionale uitwisseling van patiëntgegevens. Aan de hand van een bespreking van de Handreiking van de KNMG, VHN, NHG en KNMP zal worden aangegeven hoe de huidige opzet van regionale systemen dient te veranderen, opdat die in overeenstemming is met het recht op privacy. In paragraaf 5.4 worden de bevindingen uit paragraaf 5.2 en 5.3 gerelateerd aan de geïnterviewde technische, juridische en politieke knelpunten. In paragraaf 5.5 volgt een conclusie.

²⁶⁰ Ploem 2004, p. 282.

²⁶¹ *Rapport CBP inzake de Definitieve bevindingen Centrale Huisartsenpost Gorinchem* (rapport van 18 mei 2009), Den Haag: CBP 2009 en *Rapport CBP inzake de Definitieve bevindingen SPITZ Midden-Holland* (rapport van 18 mei 2009), Den Haag: CBP 2009.

²⁶² *Handelingen I* 2010/11, 20, p. 1-2.

²⁶³ Brief van de minister van VWS aan Eerste Kamer, 'Stand van zaken digitale gegevensuitwisseling in de zorg na aanvaarding van de motie Mulder c.s.', MEVA/ICT-3096140 8 december 2011, p. 1.

²⁶⁴ *Kamerstukken II* 2011/12, 33 000 XVI, nr. 39.

5.2 Landelijk vs. regionaal

Een regionale gegevensuitwisseling is de uitwisseling van patiëntgegevens tussen bij de behandeling van de patiënt betrokken zorgverleners die zich in dezelfde plaats of regio bevinden.²⁶⁵ Het verschilt per regio welke informatie op welke manier door wie wordt uitgewisseld. Hoewel de minister van mening is dat een landelijke invoering prioriteit heeft, wordt er onder druk van de koepels, het zorgveld en regionale initiatieven steeds vaker regionaal gewerkt. In Nederland is de gezondheidszorg voor ruim 90 procent lokaal georganiseerd, waardoor in de meeste gevallen gegevensuitwisseling tussen zorgverleners regionaal is geregeld.²⁶⁶ De overige gevallen betreffen spoedgevallen en situaties waarbij patiënten - voornamelijk met complexe aandoeningen - een behandeling ondergaan buiten de eigen regio. Het is dus niet vreemd dat de Eerste Kamer pleit voor een regionale opzet van gegevensuitwisseling.²⁶⁷

Een veelgehoord argument vóór een regionaal EPD is dat gegevensuitwisseling kleinschaliger is, waardoor het risico op schending van de privacy wordt beperkt en beter is te overzien.²⁶⁸ De kans is namelijk groter dat zorgverleners elkaar kennen, waardoor het houden van toezicht op de inloggers en inloggegevens op een meer adequate wijze zal plaatsvinden, en de preventieve werking van dat toezicht en daarmee het niveau van de bescherming van de inzage van medische gegevens zal toenemen.²⁶⁹ Regionale gegevensuitwisseling berust doorgaans op het principe van push-communicatie, inhoudende dat zorgverleners zelf patiëntgegevens actief en gericht versturen. Een landelijke uitwisseling van gegevens vindt daarentegen meer op de pull-wijze plaats. Hierbij worden gegevens die reeds zijn aangemeld bij het LSP opgevraagd, zonder dat de zorgverlener in wiens systeem die gegevens liggen opgeslagen daar op dat moment een handeling voor verricht.²⁷⁰ Terwijl het actief en gericht versturen van patiëntgegevens redelijk beheersbaar is, is het laten opvragen echter sneller 'out of control'. Het feit dat bij de pull-methode andere zorgverleners delen van de patiëntendossiers kunnen inzien, kan dus als een bedreiging worden ervaren.²⁷¹ Naar schatting bestaat het gegevensverkeer op dit moment voor 95 procent uit pushgegevens.²⁷² Zij die regionale uitwisseling boven landelijke uitwisseling verkiezen, zijn dan ook van mening dat lang niet alle patiëntgegevens geschikt zijn voor pull-uitwisseling.²⁷³

²⁶⁵ Ploem e.a. 2011, p. 17.

²⁶⁶ N. Hugenholtz e.a., 'De logische route naar een landelijk EMD. Van essentie naar perfectie', *Pharmaceutisch Weekblad* 2008-8, p. 18-19.

²⁶⁷ O.a. *Handelingen I* 2010/11, 22, p. 10, *Handelingen I* 2010/11, 20, p. 3, *Kamerstukken II* 2007/08, 31466, nr. 4, p. 3 en *Pluut* 2010, p. 33.

²⁶⁸ *Handelingen I* 2010/11, 20, p. 1-19.

²⁶⁹ *Kamerstukken II* 2007/08, 31466, nr. 4, p. 3.

²⁷⁰ *Pluut* 2010, p. 35.

²⁷¹ Ploem e.a. 2011, p. 72.

²⁷² *Handelingen I* 2010/11, 20, p. 2.

²⁷³ *Pluut* 2010, p. 35.

Aan de andere kant zou een regionale focus berusten op een achterhaalde visie op gegevensuitwisseling. Ook patiënten die geen complexe aandoening hebben, kiezen steeds vaker voor een zorgverlener buiten hun regio.²⁷⁴ In een landelijk EPD is sprake van één logisch overzicht van de patiëntgegevens, waardoor voor de behandelaar alle relevante informatie meteen voorhanden is. Een patiënt hoeft dan tevens niet steeds bij een andere specialist of waarnemend huisarts uit te leggen wat hij of zij mankeert en welke medicijnen hij of zij gebruikt.²⁷⁵

Daarnaast ontstaat er bij een regionale gegevensuitwisseling een lappendeken aan infrastructuren die - onvermijdelijk - onderling gaan afwijken, waarmee ook de kwalificatie van zorginformatiesystemen niet langer efficiënt op één plaats kan plaatsvinden. Voor uitwisseling tussen regio's is er tevens geen beheerder, die zorg draagt voor standaardisatie en beheer.²⁷⁶ In een landelijk EPD bevinden de patiëntgegevens zich niet in van elkaar onafhankelijke informatiesystemen, maar zijn de gegevens op logische wijze geordend.²⁷⁷ Voorstanders van een regionaal EPD vinden dit argument echter niet overtuigend, aangezien eisen geformuleerd kunnen worden voor een regionaal EPD zoals die ook gelden voor een landelijk systeem. Er kunnen specifieke eisen gesteld worden aan systemen en netwerken om eenduidigheid in de onderlinge communicatie, het transport van gegevens en de mate van beveiliging te bewerkstelligen. Zo pleit de Eerste Kamer er tevens voor om wetgeving te realiseren en te handhaven voor regionale systemen.²⁷⁸ Volgens de KNMG leiden het stopzetten van het LSP en het maken en handhaven van wetgeving waar regionale systemen aan moeten voldoen, juist tot een vertraging van de voortgang, tot extra veel kosten en tot onzekerheid voor de zorgverleners die al zijn aangesloten op het LSP.²⁷⁹ Het werken via regionale infrastructuren zou betekenen dat per regio een investering moet worden gedaan om de infrastructuur aan de wettelijke richtlijnen te laten voldoen. Daarnaast moet per regio een organisatie worden ingericht die verantwoordelijk is voor het beheer en onderhoud van het systeem. Er zullen ongeveer dertig regio's nodig zijn om landelijke dekking te realiseren, waardoor er dertig keer zoveel kosten worden gemaakt. De patiënt kan dan tevens niet op één plaats zijn recht op inzage uitoefenen en bezwaar maken, wat voor hem of haar erg nadelig is.²⁸⁰

Doch onderschreef de KNMG eerder nog de 'onrijpheid' van een landelijk systeem voor gegevensuitwisseling. De regionale gegevensuitwisseling werd door de KNMG als een beter alternatief gezien: "De minister blijft vasthouden aan de eigen lijn om het landelijk EPD 'topdown' te

²⁷⁴ Pluut 2010, p. 34.

²⁷⁵ R. van der Staaij, 'Geen belemmeringen voor invoering EPD. Beveiligingsproblemen zijn goed aan te pakken met bestaande methoden', *Automatisering Gids* 2010-4, p. 16.

²⁷⁶ *Handelingen I* 2010/11, 20, p. 6.

²⁷⁷ Van der Staaij 2010, p. 16.

²⁷⁸ *Handelingen I* 2010/11, 20, p. 1-2.

²⁷⁹ A.C. Nieuwenhuijzen Kruseman, 'Stopzetten LSP vertraagt informatieuitwisseling', *KNMG* 2010-6, p. 1.

²⁸⁰ *Kamerstukken I* 2010/11, 31 466, nr. S, p. 18-23.

implementeren. En dat geeft niet veel vertrouwen in het veld.”²⁸¹ In de eerdere discussies over het opzetten van één landelijk EPD gaven - in tegenstelling tot hun huidige opvatting om het LSP te behouden - de VVD, PvdA, SP, GroenLinks, Partij voor de Dieren, SGP en ChristenUnie tevens de voorkeur aan een kleine regionale opzet waarbij het EPD in de praktijk wordt opgebouwd: “Regionale systemen moeten zich van onderop vestigen en ontwikkelen, zodat eventueel later als sluitstuk daarbovenop een landelijke infrastructuur nodig is.”²⁸² Met deze ‘bottum up’ benadering kan worden nagegaan of het werkt, voordat de medewerking van zorgverleners in grootschaligere uitwisselingsystemen wordt gevraagd. Daarnaast houden zorgverleners op deze wijze zoveel mogelijk een greep op het proces. De invoering van het EPD kan derhalve beter niet van bovenaf worden opgelegd. Het volgen van een traject waarin het draagvlak in de praktijk kan groeien, is een beter alternatief.²⁸³

Zo zou voor een aansluiting op de landelijke infrastructuur als voorwaarde kunnen gelden dat zorgverleners alleen van de infrastructuur gebruik mogen maken, indien hun eigen zorginformatiesysteem veilig en betrouwbaar is. Zo wordt gewaarborgd dat de beveiliging van de regionale gegevensuitwisseling op orde is.²⁸⁴ Het zodanig inrichten van de landelijke infrastructuur dat deze voorlopig slechts kan worden benut voor regionale gegevensuitwisseling, lijkt een goed alternatief te zijn. Het vertrouwen van de zorgverleners in het systeem neemt namelijk toe, nu - zoals eerder vermeld – een regionaal EPD minder risico’s ten aanzien van schending van het recht op privacy met zich mee brengt.²⁸⁵ De minister geeft hierbij de voorkeur aan het gebruik van het LSP voor regionale gegevensuitwisseling.²⁸⁶

5.3 Onderzoek CBP bij regionale EPD’s

Zoals reeds als tegenargument tegen de invoering van een regionaal EPD is aangegeven, voldoen regionale systemen voor gegevensuitwisseling nog niet aan de gestelde privacyeisen van de Wbp en de WGBO. Zo toont onderzoek van het CBP, gehouden bij twee regionale systemen, aan dat een regionaal EPD nog ernstig tekort schiet met betrekking tot het recht op privacy.²⁸⁷

De zaak Centrale Huisartsen Post (CHP) Gorinchem betrof een Centrale Huisartsen Post en is met name van belang voor huisartsen en huisartsenposten. De CHP verwerkt persoonsgegevens vanaf het

²⁸¹ M. Katzenbauer, ‘Te vroeg voor landelijk EPD’, *Medisch Contact* 2009-20, p. 4.

²⁸² *Handelingen I* 2010/11, 22, p. 10.

²⁸³ Ploem e.a. 2011, p. 62-63.

²⁸⁴ Ploem e.a. 2011, p. 61.

²⁸⁵ Ploem e.a. 2011, p. 66-67.

²⁸⁶ Brief van de minister van VWS aan Eerste Kamer, ‘Stand van zaken digitale gegevensuitwisseling in de zorg na aanvaarding van de motie Mulder c.s.’, *MEVA/ICT-3096140* 8 december 2011, p. 1.

²⁸⁷ *Rapport CBP inzake de Definitieve bevindingen Centrale Huisartsenpost Gorinchem* (rapport van 18 mei 2009), Den Haag: CBP 2009 en *Rapport CBP inzake de Definitieve bevindingen SPITZ Midden-Holland* (rapport van 18 mei 2009), Den Haag: CBP 2009.

moment dat een huisarts de gegevens van zijn patiënten laat opnemen in de Centrale Patiëntenindex (CPI). Waarneemartsen op de CHP hebben via de CPI de mogelijkheid om professionele samenvattingen van de betrokken patiënten op te vragen uit de systemen van de bij de CHP aangesloten huisartsen.²⁸⁸ De tweede zaak betrof de inrichting van een Regionaal Schakelpunt van de stichting SchakelPunt Informatie Transmurale Zorg Midden-Holland (Spitz-MH). Dit is een regionaal samenwerkingsverband van zorgverleners en is zowel voor (huis)artsen als apothekers van belang.²⁸⁹ Spitz-MH beheert een Regionaal Schakelpunt (RSP), dat zorgt voor de koppeling tussen en integratie van verschillende bronsystemen met patiëntgegevens. Spitz-MH verwerkt persoonsgegevens vanaf het moment dat een zorgverlener persoonsgegevens van zijn patiënten laat opnemen in het RSP. Via het Zorgportal van het RSP heeft een zorgverlener toegang tot alle beschikbare patiëntgegevens van alle andere aangesloten zorgverleners. Zorgverleners hebben toegang tot het Zorgportal door middel van de UZI-pas. Voordat de gegevens van een patiënt beschikbaar zijn, moet de zorgverlener aangeven of er een behandelrelatie is met deze patiënt.²⁹⁰

5.3.1 Bevindingen CBP inzake het recht op privacy

Het CBP constateerde dat zowel de CHP als het Spitz-MH zich niet aan de informatieplicht uit artikel 34 Wbp heeft gehouden. De patiënten waren namelijk niet persoonlijk geïnformeerd over de opname van hun gegevens in de CPI of het RSP, waardoor het kon zijn dat patiënten daarin waren opgenomen zonder dat zij dit wisten.²⁹¹ Daarnaast constateerde het CBP dat zowel de CHP als het Spitz-MH onvoldoende maatregelen nam om te zorgen dat alleen artsen die een behandelrelatie met de patiënt hadden, toegang hadden tot het dossier. Raadplegingen van het systeem werden wel gelogd, maar er werd geen structurele controle uitgevoerd om na te gaan of artsen zonder behandelrelatie onbevoegd toegang hadden gezocht tot een patiëntendossier. Zo toont het Spitz-MH zorgverleners die toegang zoeken tot het systeem een waarschuwingsscherm waarin wordt gevraagd of de zorgverlener een behandelrelatie heeft met de patiënt.²⁹² Door de vraag met “ja” te beantwoorden kan er worden doorgeklikt en zijn de gegevens toegankelijk. Dit is echter onvoldoende om te voorkomen dat een aangesloten zorgverlener via het RSP gegevens inziet van een patiënt die op dat moment niet bij hem in behandeling is.²⁹³ De CHP heeft een gedragscode opgesteld over de toegang tot de dossiers en logt de raadplegingen, maar heeft hiernaast geen maatregelen genomen om te voorkomen dat een waarnemend huisarts gegevens inziet van een patiënt die op dat moment niet bij hem in behandeling

²⁸⁸ *Rapport CBP inzake de Definitieve bevindingen Centrale Huisartsenpost Gorinchem* (rapport van 18 mei 2009), Den Haag: CBP 2009, p. 1.

²⁸⁹ *Rapport CBP inzake de Definitieve bevindingen SPITZ Midden-Holland* (rapport van 18 mei 2009), Den Haag: CBP 2009, p. 1.

²⁹⁰ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 5.

²⁹¹ E.P.M. Thole e.a., 'Operatie landelijk EPD mislukt. Wat nu?', *Tijdschrift voor compliance en zorg* 2011-2, p. 46.

²⁹² CBP, 'Berichten van het College bescherming Persoonsgegevens', *Privacy & Informatie* 2009-4, p. 209.

²⁹³ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 7.

is. Verder maakt dit initiatief gebruik van een externe dienstverlener die de autorisaties van gebruikers van het systeem kan aanpassen, waardoor de mogelijkheden tot onbevoegde inzage onnodig worden verruimd.²⁹⁴ Zowel het CHP als het Spitz-MH is derhalve strijdig met artikel 7:457, tweede lid, BW en artikel 13 Wbp, aangezien zij geen passende veiligheidsmaatregelen hebben getroffen om te voorkomen dat een zorgverlener gegevens inziet van een patiënt die op dat moment niet bij hen in behandeling is.

Uit het onderzoek van het CBP inzake de regionale systemen voor informatie-uitwisseling CHP en Spitz-MH, blijkt dat bij het regionale EPD de waarborging van het recht op privacy op vier punten ernstig in het geding is. Hierbij gaat het om het informeren van de patiënt, de logging van de toegang, de behandelrelatie en de aanmelding van een CPI of RSP bij het CBP. In de ‘Handreiking privacy bij regionale uitwisseling van patiëntgegevens’ van de KNMG, VHN, NHG en KNMP worden naar aanleiding van deze bevindingen van het CBP vier adviezen geformuleerd voor de wijze waarop gehandeld moet worden als sprake is van een elektronische uitwisseling van patiëntgegevens, welke ik in de volgende subparagraaf zal gaan bespreken.²⁹⁵

5.3.2 Handreiking KNMG, VHN, NHG en KNMP

Een eerste belangrijk advies is het informeren van de patiënt over de verwerking van zijn gegevens in een brondossier en de uitwisseling van die gegevens tussen zorgaanbieders. In een regionaal EPD rust de verantwoordelijkheid op de zorgaanbieder (de huisarts of apotheker) die de patiëntgegevens in het brondossier heeft verzameld en daaruit beschikbaar stelt voor anderen. De patiënten dienen persoonlijk te worden geïnformeerd via het toesturen van een informatiebrief en een folder, waarbij volstaan kan worden met één brief per adres. Daarnaast moet van het informeren van patiënten een gezamenlijke en gecoördineerde actie van alle zorgverleners worden gemaakt en dienen er informatiefolders en posters duidelijk aanwezig te zijn bij de huisarts of apotheek.²⁹⁶

Het tweede advies houdt in dat de toegang tot een regionaal EPD wordt gelogd: wie, tijdstip en patiëntendossier.²⁹⁷ De plicht tot logging vloeit voort uit artikel 13 Wbp, op grond waarvan voor de verantwoordelijke de plicht bestaat om passende technische en organisatorische maatregelen te treffen tegen onrechtmatige verwerkingen van persoonsgegevens. Een specifieke wettelijke bepaling die het loggen van de toegang verplicht stelt, bestaat na het afschieten van de wet tot wijziging van de Wet

²⁹⁴ CBP, 'Berichten van het College bescherming Persoonsgegevens', *Privacy & Informatie* 2009-4, p. 209.

²⁹⁵ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 5.

²⁹⁶ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 8-10.

²⁹⁷ Velink & De Die Advocaten, 'Informatie-uitwisseling in zorgketens. Wat mag, kan en moet?', *Achtergrondstudie ten behoeve van de SGZ* 2011, p. 23.

gebruik burgerservicenummer in de zorg in verband met de elektronische informatie-uitwisseling in de zorg echter niet meer. In het rapport ‘Beveiliging van persoonsgegevens’ stelt het CBP tevens logging als eis bij het verwerken van patiëntgegevens: “Elke poging (geslaagd of niet) om toegang te krijgen tot een informatiesysteem met persoonsgegevens wordt vastgelegd in een logbestand. Dit logbestand heeft een voldoende lange bewaartijd, zodat een analyse van bijzonderheden kan worden gemaakt en hierover kan worden gerapporteerd.”²⁹⁸ De logging dient zowel in het geraadpleegde brondossier als op het niveau van een CPI of RSP plaats te vinden en de logbestanden dienen wekelijks en steekproefsgewijs gecontroleerd te worden op onbevoegde raadplegingen.²⁹⁹

Het derde advies wijst erop dat het gebruik van een CPI of een RSP alleen is toegestaan, indien de zorgverlener een behandelrelatie heeft met de desbetreffende patiënt. Het bestaan van een behandelrelatie kan op verschillende manieren gecontroleerd worden, alvorens toegang tot de patiëntgegevens wordt verleend. Ten eerste kan gecontroleerd worden of de patiënt staat ingeschreven in de patiëntenadministratie van de opvragende zorgverlener. Ten tweede kan het bestaan van een behandelrelatie worden afgeleid uit de werkcontext, bijvoorbeeld wanneer de patiënt met de opvragende zorgverlener een behandelafpraak heeft. Een zorgverlener kan tevens worden gevraagd het bestaan van een behandelrelatie en het feit dat de patiënt toestemming heeft verleend voor de raadpleging te bevestigen in een pop-upschermbij. Het enkel tonen van een waarschuwingsschermbij is hierbij onvoldoende. Er dient achteraf toetsing plaats te vinden door de houder van het brondossier of door de beheerder van het regionale samenwerkingsverband, door middel van een verslag aan de houder van het brondossier van de raadplegingen die hebben plaatsgevonden (een zogenoemd snuffelverslag), een declaratieregeling of logging. Daarnaast kan er voor de zekerheid een bevestiging van de toestemming van de patiënt worden gevraagd om zijn of haar gegevens in te zien.³⁰⁰

De Handreiking wijst in haar vierde advies erop dat een geautomatiseerde verwerking van persoonsgegevens (zoals het opnemen van persoonsgegevens in een CPI of RSP) vooraf moet worden gemeld bij het CBP of een door de organisatie aangestelde FG.³⁰¹ Dit kan middels een papieren formulier of elektronisch meldingsprogramma waarop naam en adres van de verantwoordelijke moeten worden ingevuld, het doel of doeleinden van de verwerking en een beschrijving van de categorieën betrokkenen, gegevens en ontvangers. In het Vrijstellingsbesluit Wbp staat of een

²⁹⁸ G.W. van Blarckom & J.J. Borking, ‘Beveiliging van persoonsgegevens’, in: *Achtergrondstudies en Verkenningen*, Den Haag: College bescherming persoonsgegevens 2001, p. 44.

²⁹⁹ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 11-12.

³⁰⁰ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 12.

³⁰¹ Zie artikel 27 Wbp en de bepalingen in het Vrijstellingsbesluit Wbp.

verwerking is uitgezonderd op de meldingsplicht. Hierbij gaat het meestal om verwerkingen waarbij een inbreuk op de rechten en vrijheden van betrokkenen onwaarschijnlijk is.³⁰²

5.4 Oplossing knelpunten: toetsing aan een regionaal EPD

In deze paragraaf ga ik onderzoeken of het recht op privacy beter gegarandeerd kan worden in een regionaal EPD dan in één landelijk EPD. Hiertoe ga ik gebruikmaken van de genoemde voor- en nadelen van een regionaal EPD en een landelijk EPD, en de Handreiking van de KNMG, VHN, NHG en KNMP naar aanleiding van de bevindingen van het CBP inzake de privacy bij een regionale uitwisseling van patiëntgegevens. Per aspect zal ik een oplossing proberen te vinden voor de geïntegreerde technische, juridische en politieke knelpunten.

Schaalgrootte van het EPD

In een regionaal EPD is de kans op ongevoegde toegang tot het systeem kleiner, nu gegevensuitwisseling daar op een kleinere schaal plaatsvindt. Zorgverleners zullen elkaar veelal kennen, waardoor gemakkelijker kan worden nagegaan of er sprake is van een rechtmatige gegevensuitwisseling.³⁰³ Hierdoor wordt tevens het politieke knelpunt opgelost, aangezien zorgverleners hun onderzoeksplicht beter kunnen uitoefenen dan in een landelijk EPD. Aan de andere kant verschillen de regionale systemen in hun huidige opzet onderling nog sterk van elkaar, waardoor er een lappendeken aan infrastructuur ontstaat. Beveiliging kan dan niet op een effectieve wijze plaats vinden.³⁰⁴ Het formuleren van specifieke eisen aan systemen en netwerken om eenduidigheid in de onderlinge communicatie, het transport van gegevens en de mate van beveiliging te bewerkstelligen is derhalve onontkoombaar.³⁰⁵

De rol van zorgverzekeraars

Teneinde te voorkomen dat zorgverzekeraars in de patiëntgegevens gaan kijken, dient de beveiliging in het EPD optimaal te zijn geregeld. Zoals gezegd kunnen de beveiliging en het toezicht in een regionaal systeem adequater plaatsvinden.³⁰⁶ Daarnaast is een regionaal EPD minder omvangrijk, waardoor de kans op inbraak door zorgverzekeraars en de impact daarvan geringer zullen zijn.³⁰⁷ Desalniettemin is de kans dat zorgverzekeraars zich toegang tot de patiëntgegevens zullen verschaffen, nooit helemaal te voorkomen door beveiliging. Noodzaak is derhalve om de medewerking van zorgverzekeraars uit te sluiten bij het private doorstartmodel.

³⁰² Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties (handreiking van september 2010), p. 13-14.

³⁰³ Kamerstukken II 2007/08, 31466, nr. 4, p. 3.

³⁰⁴ Van der Staaij 2010, p. 16.

³⁰⁵ Handelingen I 2010/11, 20, p. 1-2.

³⁰⁶ Ploem e.a. 2011, p. 69

³⁰⁷ Ploem e.a. 2011, p. 53- 65.

“Geen bezwaar”-systeem

In het private doorstartmodel is opgenomen dat de patiënt nadrukkelijk zijn of haar toestemming dient te geven voor landelijke uitwisseling van zijn of haar gegevens.³⁰⁸ Op deze manier kan de patiënt bevestigen of sprake is van een behandelrelatie en wordt strijdigheid met artikel 7:457 BW opgelost. Indien de patiënt zijn of haar uitdrukkelijke toestemming geeft, wordt het politieke knelpunt van de ondoorzichtige registratie tevens opgelost. Het is hierbij echter wel van belang dat de patiënt vooraf wordt geïnformeerd over de opname en verwerking van zijn of haar gegevens in het EPD. Van deze informatieverplichting moeten de zorgverleners een gecoördineerde actie maken. Zo dienen informatiefolders en posters duidelijk aanwezig te zijn bij de huisarts of apotheek en moet de patiënt middels het sturen van een informatiebrief en een folder op de hoogte worden gebracht van de opname en verwerking van zijn of haar gegevens in het EPD.³⁰⁹

Behandelrelatie

Teneinde een behandelrelatie tussen de zorgverlener en de patiënt optimaal te garanderen en daarmee het technische knelpunt op te lossen, dient gecontroleerd te worden of de patiënt staat ingeschreven in de patiëntenadministratie van de opvragende zorgverlener. Daarnaast kan het bestaan van een behandelrelatie worden afgeleid uit de werkcontext. Een zorgverlener kan tevens worden gevraagd het bestaan van een behandelrelatie en het feit dat de patiënt toestemming heeft verleend voor de raadpleging te bevestigen in een pop-upschermb. Dit moet achteraf getoetst worden door middel van logging en er dient een bevestiging van de toestemming van de patiënt te worden gevraagd om zijn of haar gegevens in te zien.³¹⁰

Schending van de doelbinding

Middels adequaat toezicht kan worden gewaarborgd dat de zorgverlener slechts de gegevens opvraagt die noodzakelijk zijn voor een goede behandeling van de patiënt, waardoor de gegevensuitwisseling past binnen de reikwijdte van het noodzakelijkheidsvereiste ingevolge artikel 7:457, tweede lid, BW. Dit toezicht kan adequater plaatsvinden in een regionaal EPD, nu gegevensuitwisseling daar kleinschaliger is.³¹¹

³⁰⁸ *Zienswijze over doorstartmodel voor landelijke uitwisseling medische gegevens* (zienswijze van 9 augustus 2011), Den Haag: College bescherming persoonsgegevens 2011.

³⁰⁹ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 8-10.

³¹⁰ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 12.

³¹¹ Ploem e.a. 2011, p. 69 en *Handelingen I* 2010/11, 20, p. 1-19.

UZI-pas

Uit onderzoek van het CBP bij regionale EPD's is niet gebleken dat het risico op onbevoegde raadpleging van patiëntgegevens middels de UZI-pas kleiner is.³¹² Zowel in een landelijk EPD als in een regionaal EPD dienen maatregelen getroffen te worden ter voorkoming van onbevoegde toegang tot de patiëntendossiers. Teneinde het technische knelpunt op te lossen, dient bij voorkeur regionale gegevensuitwisseling plaats te vinden. Het toezicht op het gebruik van de UZI-pas is daar namelijk groter dan in een landelijk EPD, nu de gegevensuitwisseling kleinschaliger is. Daarnaast kunnen kwaadwillenden bij inbraak in een regionaal systeem minder gegevens inzien, waardoor het lastiger is om bijvoorbeeld gegevens van een bekende Nederlander te raadplegen.³¹³

Logging

De logbestanden dienen wekelijks en steekproefsgewijs gecontroleerd te worden op onbevoegde raadplegingen, waardoor de kans groter is dat misbruik van inzage in patiëntendossiers wordt voorkomen (oplossing technisch knelpunt).³¹⁴ Door het nemen van passende veiligheidsmaatregelen kunnen de juridische knelpunten worden opgelost (geen strijdigheid meer met artikel 7:457 BW en artikel 13 Wbp). Hierbij kan gedacht worden aan het informeren van de patiënt over de verwerking en uitwisseling van zijn of haar gegevens, toestemming van de patiënt vragen alvorens tot gegevensuitwisseling wordt overgegaan en adequaat toezicht houden op het bestaan van een behandelrelatie tussen de zorgverlener en de patiënt.³¹⁵ Dit kan in een regionaal EPD op een meer adequate wijze plaatsvinden.³¹⁶

Recht op inzage

In een regionaal EPD is op dit moment geen zicht op welke wijze zorgaanbieders het recht op inzage faciliteren.³¹⁷ Uit de regionale EPD's kunnen derhalve geen oplossingen worden aangedragen om patiënten veilige toegang tot hun gegevens te verschaffen en strijdigheid met artikel 35 Wbp en artikel 7:456 BW op te lossen. Teneinde het politieke knelpunt van de aanleg van "een tweede weg" naar informatie uit het EPD en de afname van de kwaliteit van patiëntgegevens op te lossen, dient adequaat toezicht te worden uitgeoefend. Gebleken is dat het toezicht in een regionaal EPD adequater kan plaatsvinden.³¹⁸

³¹² *Rapport CBP inzake de Definitieve bevindingen Centrale Huisartsenpost Gorinchem* (rapport van 18 mei 2009), Den Haag: CBP 2009 en *Rapport CBP inzake de Definitieve bevindingen SPITZ Midden-Holland* (rapport van 18 mei 2009), Den Haag: CBP 2009.

³¹³ Ploem e.a. 2011, p. 69 en *Handelingen I* 2010/11, 20, p. 1-19.

³¹⁴ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 11-12.

³¹⁵ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 8-12.

³¹⁶ Ploem e.a. 2011, p. 69 en *Handelingen I* 2010/11, 20, p. 1-19.

³¹⁷ Brief van de minister van VWS aan de Tweede Kamer, 'Vragen n.a.v. brief 11 april 2011 inzake stand van zaken EPD', MEVA-U-3061881 2 mei 2011, p. 14.

³¹⁸ Ploem e.a. 2011, p. 69 en *Handelingen I* 2010/11, 20, p. 1-19.

Recht op vernietiging

Er dient sprake te zijn van adequaat toezicht op de vernietiging van de gegevens in het EPD, opdat gegarandeerd kan worden dat alle gegevens worden vernietigd overeenkomstig artikel 36 Wbp en artikel 7:455 BW. In een regionaal EPD is adequaat toezicht sneller mogelijk, nu gegevensuitwisseling daar kleinschaliger is.

Toezicht op het EPD

Om het politieke knelpunt van capaciteitsproblemen op te lossen, dient horizontaal ‘eerste lijns’ toezicht plaats te vinden. Het toezicht dat in het private doorstartmodel wordt uitgeoefend door de VVZ, biedt hierbij een goede oplossing.

5.5 Conclusie

In dit hoofdstuk is getracht een oplossing te vinden voor de vraag of het recht op privacy beter kan worden gegarandeerd in een landelijk EPD of in een regionaal EPD. Gebleken is dat de huidige regionale EPD's onderling nog sterk afwijken, waardoor een lappendeken aan infrastructuur is ontstaan.³¹⁹ Het maken en handhaven van wetgeving voor regionale systemen zou eenduidigheid tussen regionale systemen kunnen scheppen, maar brengt te veel kosten met zich mee.³²⁰ Doch is in dit hoofdstuk duidelijk geworden dat middels regionale gegevensuitwisseling adequater toezicht plaats kan vinden dan in een landelijk EPD. Regionale gegevensuitwisseling is namelijk kleinschaliger - de kans is groter dat artsen elkaar kennen en er zijn minder gegevens beschikbaar voor uitwisseling - waardoor er een beter toezicht plaats kan vinden op schendingen van het recht op privacy.³²¹ Daarnaast wordt via een ‘bottom up’ benadering (eerst een regionaal EPD invoeren, alvorens tot landelijke gegevensuitwisseling wordt overgegaan) meer greep gehouden op het proces, waardoor het vertrouwen van de zorgverleners in het systeem toeneemt.³²² Een goed alternatief lijkt derhalve het zodanig inrichten van de landelijke infrastructuur te zijn, zodat deze voorlopig slechts kan worden benut voor regionale gegevensuitwisseling.³²³ De plannen van de minister om het LSP te gebruiken voor regionale gegevensuitwisseling zijn dan ook zo gek nog niet.³²⁴ Desalniettemin bevat het LSP nog te veel knelpunten met betrekking tot het recht op privacy. Alvorens tot gebruik van het LSP voor regionale gegevensuitwisseling wordt overgegaan, dienen daarvoor derhalve passende (wettelijke) waarborgen en uitgangspunten te gelden.

³¹⁹ *Handelingen I* 2010/11, 20, p. 6.

³²⁰ Nieuwenhuijzen Kruseman 2010, p. 1 en *Kamerstukken I* 2010/11, 31 466, nr. S, p. 18-23.

³²¹ Ploem e.a. 2011, p. 69 en *Handelingen I* 2010/11, 20, p. 1-19.

³²² *Handelingen I* 2010/11, 22, p. 10 en Ploem e.a. 2011, p. 62-63.

³²³ Ploem e.a. 2011, p. 66-67.

³²⁴ Brief van de minister van VWS aan Eerste Kamer, ‘Stand van zaken digitale gegevensuitwisseling in de zorg na aanvaarding van de motie Mulder c.s.’, *MEVA/ICT-3096140* 8 december 2011, p. 1.

In een regionaal EPD is geen zicht op welke wijze zorgaanbieders het recht op inzage faciliteren, waardoor geen oplossingen kunnen worden aangedragen om patiënten veilige toegang tot hun gegevens te verschaffen.³²⁵ De ‘Handreiking privacy bij regionale uitwisseling van patiëntgegevens’ van de KNMG, VHN, NHG en KNMP biedt echter wel goede adviezen voor enkele geïnventariseerde knelpunten in het EPD.³²⁶ De patiënt dient allereerst geïnformeerd te worden over de verwerking en uitwisseling van zijn of haar gegevens. Daarnaast dient de patiënt - in plaats van het “geen bezwaarsysteem” - toestemming te geven voor opname en verwerking van zijn of haar gegevens in het EPD.³²⁷ De geautomatiseerde verwerking van persoonsgegevens dient vooraf te worden gemeld bij het CBP of een door de organisatie aangestelde FG.³²⁸ De controle op het bestaan van een behandelrelatie is tweeledig. Voordat de zorgverlener overgaat tot het uitwisselen van patiëntgegevens, dient de behandelrelatie te worden afgeleid uit de patiëntenadministratie en de werkcontext. Daarnaast moet de zorgverlener de behandelrelatie en de toestemming van de patiënt voor de raadpleging bevestigen in een pop-upschermb. Er dient tevens een bevestiging van de toestemming van de patiënt te worden gevraagd om zijn of haar gegevens in te zien, zodat de patiënt zeker weet wie zijn of haar gegevens wil inzien. Nadat de gegevens zijn uitgewisseld, worden de handelingen van de zorgverlener gelogd, waarbij de logbestanden wekelijks en steekproefsgewijs dienen te worden gecontroleerd op onbevoegde raadplegingen.³²⁹

³²⁵ Brief van de minister van VWS aan de Tweede Kamer, ‘Vragen n.a.v. brief 11 april 2011 inzake stand van zaken EPD’, MEVA-U-3061881 2 mei 2011, p. 14.

³²⁶ Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties (handreiking van september 2010), p. 5.

³²⁷ Brief van de minister van VWS aan de Tweede Kamer, ‘Antwoorden op de vragen van het Kamerlid Omtzigt (CDA) over het College Bescherming Persoonsgegevens (CBP) en patiëntendossiers’, 100163-100046-MEVA 23 september 2011, p. 2.

³²⁸ Zie artikel 27 Wbp en de bepalingen in het Vrijstellingsbesluit Wbp.

³²⁹ Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties (handreiking van september 2010), p. 12.

6 Conclusies en aanbevelingen

6.1 Inleiding

In dit slothoofdstuk worden de bevindingen uit de voorgaande hoofdstukken in hun onderlinge samenhang beschouwd. Het EPD staat op het punt te worden ingevoerd middels regionale systemen met behoud van het LSP, terwijl is gebleken dat het EPD in zijn huidige vorm nog te veel knelpunten bevat met betrekking tot het recht op privacy. Een oplossing van deze knelpunten is derhalve noodzakelijk. In de voorgaande hoofdstukken heb ik getracht een oplossing te vinden voor de geïnterpreteerde knelpunten, welke ik in dit hoofdstuk zal uiteenzetten.

In dit hoofdstuk wordt dan ook antwoord gegeven op de onderzoeksvraag: *Hoe dienen de knelpunten die het huidige EPD bevat ten aanzien van het recht op privacy te worden opgelost zodat het niet meer in strijd is met het recht op privacy?*

Ter beantwoording van deze vraag zal ik in paragraaf 2 per aspect in het EPD mogelijke oplossingen uit de voorgaande hoofdstukken aandragen voor de geïnterpreteerde technische, juridische en politieke knelpunten. In paragraaf 3 volgt ten slotte een overzicht van de aanbevelingen.

6.2 Mogelijke oplossingen

In deze paragraaf zal uiteengezet worden welke maatregelen genomen kunnen worden om de technische, juridische en politieke knelpunten op te lossen, opdat het EPD in overeenstemming is met het recht op privacy. In de subparagrafen zal onderscheid worden gemaakt tussen de verschillende aspecten van het EPD met de geïnventariseerde knelpunten.

6.2.1 Schaalgrootte van het EPD

Gegevensuitwisseling dient plaats te vinden op een regionale schaal. In een regionaal EPD vindt gegevensuitwisseling op een kleinere schaal plaats en is de kans op onbevoegde toegang tot het systeem kleiner (oplossing van het technisch knelpunt). In een regionaal EPD zullen zorgverleners elkaar sneller kennen, waardoor zij gemakkelijker toezicht op elkaar kunnen houden en derhalve hun onderzoeksplicht voldoende kunnen uitoefenen (oplossing van het politiek knelpunt).

6.2.2 De rol van zorgverzekeraars

Bij het private doorstartmodel dient de medewerking van zorgverzekeraars te worden uitgesloten. Indien uitsluiting van de zorgverzekeraars niet mogelijk is (de zorgverzekeraars hebben immers al geld gestopt in de private doorstart van het EPD) dient via een geïntegreerd systeem van gebruikers- en toegangsbeheer binnen het EPD, de toegang van iedere zorgverlener gecontroleerd te worden en heeft iedere zorgverlener slechts toegang tot de gegevens waarop hij uit hoofde van zijn functie recht heeft.³³⁰ Nadat hierop effectieve controle heeft plaatsgevonden door de toezichthouders, dient bijvoorbeeld een FG een machtiging voor de gegevensuitwisseling te verlenen.³³¹ Zo wordt voorkomen dat zorgverzekeraars in de patiëntgegevens gaan kijken (oplossing van het politiek knelpunt).

6.2.3 “Geen bezwaar”-systeem

Het “geen bezwaar” systeem dient te worden verwijderd. De patiënt moet zowel voor het registreren als het verwerken van zijn of haar gegevens uitdrukkelijke toestemming geven. De toestemming dient tevens schriftelijk te worden gegeven.³³² Strijdigheid met artikel 7:457 BW wordt hiermee opgelost (oplossing van het juridisch knelpunt). De toestemming van de patiënt dient tevens een vrije,

³³⁰ Detiége 2008, p. 22.

³³¹ Zie Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer met betrekking tot een ontwerp van wet houdende oprichting en organisatie van het eHealth-platform (advies van 2 april 2008, A/2008/016), Brussel: CBPL 2008, p. 17 en Grondwettelijk Hof 18 maart 2010, nr. 29/2010, BS 18 maart 2010.

³³² Detiége 2008, p. 12.

specifieke en op informatie berustende wilsuiting te zijn: de patiënt moet met name vooraf geïnformeerd zijn over zijn of haar rechten en het precieze oogmerk van de verwerking. Van deze informatieverplichting moeten de zorgverleners een gecoördineerde actie maken. Zo moeten er informatiefolders en posters duidelijk aanwezig zijn bij de huisarts of apotheek en moet de patiënt middels het sturen van een informatiebrief en een folder op de hoogte worden gebracht van de opname en verwerking van zijn of haar gegevens in het EPD.³³³ Zo wordt een ondoorzichtige registratie van patiëntgegevens in het EPD tegengegaan (oplossing van het politiek knelpunt).

6.2.4 *Behandelrelatie*

De patiënt dient vooraf door de zorgverlener geïnformeerd te worden over welke collega's ooit als medebehandelaar of medewerker zullen optreden. Nadat de patiënt is geïnformeerd moet de patiënt zijn of haar uitdrukkelijke schriftelijke toestemming verlenen voor de gegevensuitwisseling. De zorgverlener dient het bestaan van een behandelrelatie en het feit dat de patiënt toestemming heeft verleend voor de raadpleging te bevestigen in een pop-upschermb. De patiënt dient zo nodig een bevestiging van de toestemming te geven om de gegevens in te zien.³³⁴ Door middel van logging wordt achteraf getoetst of de raadpleging rechtmatig is geweest. Controle vooraf en achteraf maakt het derhalve mogelijk dat het bestaan van een behandelrelatie een sluitende voorwaarde vormt voor het uitwisselen van patiëntgegevens. Op die manier wordt het technische knelpunt van de onduidelijke beschikbaarheid van de (mede)behandelaar opgelost.

6.2.5 *Schending van de doelbinding*

Zorgverleners mogen de patiëntgegevens alleen opvragen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden: “de goede behandeling of verzorging van de patiënt”.³³⁵ Hierop dient door een FG toezicht te worden gehouden. Indien gebleken is dat de zorgverlener de patiëntgegevens slechts opvraagt die noodzakelijk zijn voor een goede behandeling van de patiënt, verleend de FG een machtiging voor de gegevensuitwisseling waarna de zorgverlener de gegevens kan raadplegen. Hierdoor past de gegevensuitwisseling binnen de reikwijdte van het noodzakelijkheidsvereiste ingevolge artikel 7:457, tweede lid, BW (oplossing van het juridisch knelpunt).

³³³ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 8-10.

³³⁴ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 12.

³³⁵ *Kamerstukken II 2007/08, 31 466, nr. 3, p. 27.*

6.2.6 UZI-pas

In een regionaal EPD zullen minder UZI-passen in omloop zijn dan in een landelijk EPD, waardoor er minder patiëntgegevens door onbevoegde toegang worden geraadpleegd. Het is echter wel van belang de zorgverleners bewust te maken van de risico's van een onzorgvuldige omgang met de UZI-pas en hen daartoe adviezen te geven. Enkele voorbeelden van maatregelen die kunnen worden genomen zijn: de fysieke afscherming van het gebruikte systeem, het beveiligen van toegang tot de pc met een schermbeveiliging met wachtwoord bij het verlaten van de werkplek, het nalaten van uitlening van de UZI-pas en het wijzigen van de pincode wanneer het vermoeden bestaat dat anderen deze kennen. Daarnaast kunnen onder mogelijke maatregelen het plaatsen van een apart numeriek toetsenbord dat kan worden afgeschermd bij het invoeren van de pincode en meer controle op virussen worden verstaan.³³⁶ Toezicht door een FG of collegiale controle op een zorgvuldige omgang met de UZI-pas kan tevens bijdragen aan afname van het risico dat onbevoegd patiëntgegevens worden geraadpleegd (oplossing van het technisch knelpunt).

6.2.7 Logging

Logbestanden dienen niet enkel gecontroleerd te worden indien een vermoeden van misbruik bestaat, maar alle raadplegingen moeten wekelijks en steekproefsgewijs gecontroleerd worden.³³⁷ Hierdoor wordt misbruik van inzage in patiëntendossiers in zoveel mogelijk gevallen opgelost (oplossing van het technisch knelpunt). Daarnaast dient toezicht vooraf plaats te vinden op een rechtmatige raadpleging van de patiëntgegevens. Dit toezicht kan worden uitgeoefend door een FG of een arts en adviseur informatieveiligheid (oplossing van de juridische knelpunten).

6.2.8 Recht op inzage

Opdat de patiënt het inzagerecht zelfstandig kan uitoefenen, dient in het EPD te worden opgenomen dat de patiënt inzage in de medische gegevens dient te krijgen via de website of portal van de zorgverlener.³³⁸ Hierdoor is er een toegangsmiddel voorhanden waarmee patiënten hun recht op inzage kunnen uitoefenen, waardoor strijdigheid met artikel 35 Wbp en artikel 7:456 BW wordt opgelost (oplossing van het juridisch knelpunt). Hierop dient adequaat toezicht plaats te vinden en dient het

³³⁶ Zie <www.uziregister.nl> (veilig gebruik UZI-pas).

³³⁷ *Handreiking van KNMG, VHN, NHG en KNMP naar aanleiding van bevindingen van het CBP bij twee regionale situaties* (handreiking van september 2010), p. 11-12.

³³⁸ *Kamerstukken II* 2010/11, 27 529, nr. 71, p. 20.

inzagerecht gepaard te gaan met een recht op duiding en begeleiding (oplossing van de politieke knelpunten).³³⁹

6.2.9 Recht op vernietiging

In het EPD dient duidelijk te worden vastgelegd dat bij een verzoek tot vernietiging de gegevens uit het brondossier moeten worden verwijderd alsmede de gegevens die door een zorgverlener uit een andere instelling zijn geraadpleegd en aldaar zijn opgeslagen. Daarnaast moet in het EPD worden bepaald dat de gegevens niet worden vernietigd, indien zij anoniem zijn gemaakt, er een verplichting bestaat tot archivering of verwijdering strijdig is met hogere legitieme belangen.³⁴⁰ Teneinde de volledige vernietiging van patiëntengegevens te garanderen, dient hierop toezicht te worden uitgeoefend (oplossing van het juridisch knelpunt).

6.2.10 Toezicht op het EPD

Teneinde de capaciteitsproblemen die reeds bestaan bij het uitgeoefende toezicht door het CBP en de IGZ op te lossen, dient horizontaal toezicht plaats te vinden. Horizontaal toezicht levert schaalvoordelen op en kent een geringe capaciteitsbelasting van de toezichthoudende instanties.³⁴¹ Voor de versterking van onafhankelijk zelftoezicht en het optimaliseren van de mogelijkheid voor horizontaal toezicht door de formele toezichthouders, dient een FG op grond van artikel 62 Wbp te worden aangesteld en dient het CBP een arts en een adviseur informatieveiligheid aan te wijzen, die worden belast met het toezicht op de verwerkingen en uitwisselingen van persoonsgegevens door het EPD (oplossing van het politiek knelpunt).³⁴²

³³⁹ *Advies van de Algemene Raad over het voorontwerp van decreet betreffende het gezondheidsinformatiesysteem* (advies van 16 september 2003, AR/VHE/ADV/001), Brussel: Algemene Raad 2003, p. 6.

³⁴⁰ Principes 10.2 en 10.3 R (97) 5.

³⁴¹ Krabben 2010, p. 5.

³⁴² Krabben 2010, p. 8.

6.3 Aanbevelingen

In de voorgaande subparagrafen is een aantal aanbevelingen gedaan, welke hieronder bij wijze van samenvatting nog eens op een rijtje gezet zullen worden.

1. De infrastructuur moet - in lijn met het voorstel van de minister - zodanig worden ingericht, zodat deze voorlopig slechts kan worden benut voor regionale gegevensuitwisseling.
2. Via deze ‘bottom up’ benadering wordt meer greep gehouden op het proces, waardoor het vertrouwen van de zorgverleners in het systeem toeneemt.
3. De medewerking van de zorgverzekeraars bij het private doorstartmodel dient te worden uitgesloten.
4. Naast toezicht door het CBP en de IGZ dient horizontaal toezicht plaats te vinden. Dit levert namelijk schaalvoordelen op en kent een geringe capaciteitsbelasting van de toezichthoudende instanties. Hiertoe dient een FG te worden aangesteld (op grond van artikel 62 Wbp) en moet door het CBP een arts en adviseur informatieveiligheid worden aangewezen. Zij worden belast met het toezicht op de verwerkingen en uitwisselingen van persoonsgegevens door het EPD.
5. De geautomatiseerde verwerking van persoonsgegevens dient vooraf te worden gemeld bij het CBP of FG.
6. Middels adequaat toezicht door een FG dient erop te worden toegezien dat zorgverleners de patiëntgegevens alleen opvragen voor “de goede behandeling of verzorging van de patiënt”.
7. Er dient een geïntegreerd systeem van gebruikers- en toegangsbeheer binnen het EPD te worden ingericht, teneinde de toegang van iedere zorgverlener te controleren. In dit systeem vinden een controle ex ante en een controle ex post plaats: autorisatie en authenticatie van de zorgverlener en logging.
8. Zorgverleners dienen bewust te worden gemaakt van de risico’s van een onzorgvuldige omgang met de UZI-pas. Er dienen daartoe adviezen te worden gegeven en maatregelen te worden genomen. Er dient tevens toezicht door een FG of collegiale controle plaats te vinden op een zorgvuldige omgang met de UZI-pas.
9. De patiënt dient zowel voor het registreren als het verwerken van de patiëntgegevens zijn of haar uitdrukkelijke toestemming te geven. De toestemming dient schriftelijk te geschieden.
10. Alvorens de patiënt zijn of haar uitdrukkelijke toestemming geeft voor het registreren en/of verwerken van de gegevens, dient de patiënt door de zorgverlener geïnformeerd te zijn over zijn of haar rechten en het precieze oogmerk van de verwerking. De patiënt dient tevens te worden geïnformeerd over welke zorgverleners ooit als medebehandelaar of medewerker zullen optreden.
11. Zorgverleners moeten van hun informatieverplichting een gecoördineerde actie maken. Zo moeten er informatiefolders en posters duidelijk aanwezig zijn bij de huisarts of apotheek en

moet de patiënt middels het sturen van een informatiebrief en een folder op de hoogte worden gebracht van de opname en verwerking van zijn of haar gegevens.

12. Voordat de zorgverlener de patiëntgegevens kan raadplegen, dient hij het bestaan van een behandelrelatie en het feit dat de patiënt toestemming heeft verleend voor de raadpleging te bevestigen in een pop-upscherm. De patiënt dient zo nodig de behandelrelatie expliciet te bevestigen.
13. De FG dient alvorens tot gegevensuitwisseling mag worden overgegaan, een machtiging te verlenen.
14. Bij de uitwisseling dienen de patiëntgegevens te worden gecijferd, zodat de gegevens onleesbaar zijn voor onrechtmatige zorgverleners. De patiënt dient in deze gecijferde berichten geïdentificeerd te zijn aan de hand van zijn of haar BSN.
15. Logbestanden moeten wekelijks en steekproefsgewijs gecontroleerd worden, opdat misbruik van inzage in de patiëntgegevens zoveel mogelijk wordt voorkomen.
16. De patiënt dient inzage in zijn of haar gegevens te krijgen via de website of portal van de zorgverlener. Dit inzagerecht dient gepaard te gaan met een recht op duiding en begeleiding van de zorgverlener, zodat de patiënt ook echt iets aan het inzagerecht heeft.
17. Bij vernietiging van de patiëntgegevens op verzoek van de betrokkene dient in het EPD te worden vastgelegd dat de gegevens uit het brondossier, alsmede de gegevens die door een zorgverlener uit een andere instelling zijn geraadpleegd en aldaar zijn opgeslagen, worden verwijderd.

Literatuurlijst

Geraadpleegde literatuur

Aerts 2010

B. Aerts, *Privacybescherming en de elektronische gegevensverwerking in de gezondheidszorg* (doctoraalscriptie Gent), 2010.

Algemene Raad 2003

Advies van de Algemene Raad over het voorontwerp van decreet betreffende het gezondheidsinformatiesysteem (advies van 16 september 2003, AR/VHE/ADV/001), Brussel: Algemene Raad 2003.

Van Blarkom & Borking 2001

G.W. van Blarkom & J.J. Borking, 'Beveiliging van persoonsgegevens', in: *Achtergrondstudies en Verkenningen*, Den Haag: College bescherming persoonsgegevens 2001, p. 1-60.

Bonthuis 2007

M.J. Bonthuis, 'Privacy en het landelijk Elektronisch Patiënten Dossier (EPD). Een onderzoek naar het Landelijk EPD op basis van een juridisch raamwerk van de Wet Geneeskundige Behandelingsovereenkomst, de Wet Bescherming Persoonsgegevens en de NEN 7510', *Advies en Implementatie van het privacyrecht* 2007, p. 1-51.

Bonthuis 2008

M.J. Bonthuis, 'Privacy en het landelijk elektronisch patiëntendossier', *Privacy & Informatie* 2008-3, p. 119-123.

Bonthuis 2008

M.J. Bonthuis, 'Het EPD en privacy', *Journaal Privacy Gezondheidszorg* 2008-7, p. 1-7.

CBP 2005

Rapport Landelijk Schakelpunt en artikel: 7:457 lid 2 BW (rapport van 11 oktober 2005), Den Haag: College Bescherming Persoonsgegevens 2005.

CBP 2007

Advies over wijziging Wet gebruik BSN in de zorg (advies van 14 juni 2007), Den Haag: College bescherming persoonsgegevens 2007.

CBP 2009

CBP, 'Berichten van het College bescherming Persoonsgegevens', *Privacy & Informatie* 2009-4, p. 208-209.

CBP 2009

Rapport CBP inzake de Definitieve bevindingen Centrale Huisartsenpost Gorinchem (rapport van 18 mei 2009), Den Haag: CBP 2009.

CBP 2009

Rapport CBP inzake de Definitieve bevindingen SPITZ Midden-Holland (rapport van 18 mei 2009), Den Haag: CBP 2009.

CBP 2010

Informatieblad De functionaris voor de gegevensbescherming (informatieblad van 16 september 2010), Den Haag: College Bescherming Persoonsgegevens 2010.

CBP 2011

Zienswijze over doorstartmodel voor landelijke uitwisseling medische gegevens (zienswijze van 9 augustus 2011), Den Haag: College bescherming persoonsgegevens 2011.

CBPL 2004

Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer over het voorontwerp van decreet van de Vlaamse Regering betreffende het gezondheidsinformatiesysteem (advies van 10 mei 2004, 05 / 2004), Brussel: CBPL 2004.

CBPL 2008

Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer met betrekking tot een ontwerp van wet houdende oprichting en organisatie van het eHealth-platform (advies van 2 april 2008, A/2008/016), Brussel: CBPL 2008.

Cuijpers 2007

C. Cuijpers, 'Privacy in context', in: J.M.A. Berkvens & J.E.J. Prins, *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2007, p. 7-24.

Detiége 2008

M. Detiége, 'Wetsontwerp houdende oprichting en organisatie van het eHealth-platform', *Belgische Kamer van Volksvertegenwoordigers*, nr. 1257/003-2008, p. 1-73.

Dierickx 2005

L. Dierickx, *Het recht op afbeelding*, Antwerpen: Intersentia 2005, p. 1-345.

Doppegieter 1993

R.M.S. Doppegieter, 'Regelgeving aangaande informationele en ruimtelijke privacy', *Nederlands Tijdschrift voor Geneeskunde* 1993-137, p. 14.

Dumortier 2010

J. Dumortier, 'Recente ontwikkelingen in het privacyrecht 2008-2009', in: *Recht in beweging - 17e VGR Alumnidag*, Antwerpen: Maklu 2010, p. 157-182.

Ekker 2010

A. Ekker, *Vertrouwensmodel landelijke infrastructuur voor gegevensuitwisseling*, ID nummer 10041, Nictiz 2010, p. 1-52.

Europa decentraal

Factsheet Rechtstreekse werking van bepalingen uit Europese richtlijnen: Regels en risico's (factsheet van december 2009), Den Haag: Europa decentraal 2009, p. 1-11.

Van Gossum 2008

K. van Gossum, 'Het Elektronisch gedeeld patiëntendossier in België: stand van zaken', *Privacy & Informatie* 2008-1, p. 15-26.

Groothuis 2007

M. Groothuis, 'Het elektronisch patiëntendossier in een veellagige rechtsorde', in: A.C. Hendriks & H.M.Th.D. Ten Napel (red), *Volksgezondheid in een veellagige rechtsorde*, Alphen a/d Rijn: Kluwer 2007.

Harden 2001

I. Harden, 'Citizenship and Information', *EPL* 2001, p. 165-193.

De Heij & Versmissen 2002

J.A.G. Versmissen & A.C.M. de Heij, 'Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid', in: *Achtergrondstudies en verkenningen*, Den Haag: College bescherming persoonsgegevens 2002, p 1-83.

Hendriks 2000

A.C. Hendriks, *Gelijke toegang tot de arbeid voor gehandicapten; een grondrechtelijke en rechtsvergelijkende analyse* (diss. Amsterdam UvA), Deventer: Kluwer 2000, p. 1-375.

De Hert & Saelens 2010

P. de Hert & R. Saelens, 'eHealth-wet: nog enkele onduidelijkheden', *De Juristenkrant* 2010-207, p. 12-13.

Hugenholtz 2008

N. Hugenholtz e.a., 'De logische route naar een landelijk EMD. Van essentie naar perfectie', *Pharmaceutisch Weekblad* 2008-8, p. 18-19.

Jacobs e.a. 2008

B. Jacobs e.a., 'Beveiligingseisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Electronisch Patiëntendossier', rapport in opdracht van VWS uitgevoerd door PriceWaterhouseCoopers, Universiteit Nijmegen, en Universiteit van Tilburg 2008.

Katzenbauer 2009

M. Katzenbauer, 'Te vroeg voor landelijk EPD', *Medisch Contact* 2009-20, p. 1-4.

Krabben 2010

J.A.L. Krabben, *Toezichtkader EPD: in opdracht van Ministerie van VWS*, 2010-1.1, p. 1-48.

Kranenborg 2007

H.R. Kranenborg, *Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie. Over de openbaarheid van persoonsgegevens*, (diss. Leiden), Deventer: Kluwer 2007, p. 1-365.

Nationale Raad 2007

Advies inzake het Decreet van de Vlaamse Gemeenschap betreffende het Gezondheidsinformatiesysteem (advies van 16 juni 2006), Brussel: Nationale Raad 2007.

Nictiz 2011

Doorstartmodel landelijke infrastructuur (model van 17 juni 2011, V1.0) Nictiz 2011.

Nieuwenhuijzen Kruseman 2010

A.C. Nieuwenhuijzen Kruseman, 'Stopzetten LSP vertraagt informatieuitwisseling', *KNMG* 2010-6, p. 1.

Van 't Noordende 2010

G. J. van 't Noordende, 'A Security Analysis of the Dutch Electronic Patient Record System', *Conference on Computers, Privacy and Data Protection*, Brussel 2010.

Overkleeft-Verburg 2000

G. Overkleeft-Verburg, 'Het grondrecht op eerbiediging van de persoonlijke levenssfeer', in: A.K. Koekkoek (red), *De Grondwet, Een systematisch en artikelsgewijs commentaar*, Deventer: Kluwer 2000, p. 155-178.

Ploem 2004

M.C. Ploem, *Tussen privacy en wetenschapsvrijheid. Regulering van gegevensverwerking voor medisch-wetenschappelijk onderzoek*, (diss. Amsterdam UvA) Den Haag: Sdu 2004, p. 1-312.

Ploem e.a. 2011

M.C. Ploem e.a., 'Vertrouwen van zorgverleners in elektronische informatie-uitwisseling en het landelijk EPD. Een juridische en sociaal-wetenschappelijke studie naar de positie van zorgverleners', *AMC/NIVEL* 2011, p. 1-90.

Pluut 2010

B. Pluut, 'Het Landelijk EPD als blackbox. Besluitvorming en opinies in kaart', in: *WRR-Rapport iOverheid*, Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid 2010, p. 1-76.

Prins 2002

J.E.J. Prins, 'Waken voor kenbaar maken. Over privacy, identiteit en anonimiteit in de informatiemaatschappij', in J.M. Titulaer-Meddens (red.), *Privacy: ons een zorg! De betekenis van privacybescherming voor het V&W-beleid*, Ministerie van Verkeer en Waterstaat 2002, p. 30-42.

Prinssen 2004

J.M. Prinssen, *Doorwerking van Europees recht: de verhouding tussen directe werking, conforme interpretatie en overheidsaansprakelijkheid* (Europese monografieën nr. 73), Deventer: Kluwer 2004, p. 1-275.

Put 2007

J. Put, *Werken met gezondheidsgegevens in de integrale jeugdhulp* (doctoraalscriptie Leuven), 2007, p. 1-67.

De Raaij 2008

C.C.M. de Raaij, 'Noot bij EHRM 17 juli 2008 (I. tegen Finland). Onvoldoende beveiliging van elektronisch patiëntendossier', *Privacy & Informatie* 2009-2, p. 89-90.

Robben 1998

F. Robben, 'De invoering van een elektronisch leesbare sociale identiteitskaart voor alle Belgen', *Computerrecht* 1998-1, p. 14-19.

Van der Staaij 2010

R. van der Staaij, 'Geen belemmeringen voor invoering EPD. Beveiligingsproblemen zijn goed aan te pakken met bestaande methoden', *Automatisering Gids* 2010-4, p. 16-17.

Thole e.a. 2011

E.P.M. Thole e.a., 'Operatie landelijk EPD mislukt. Wat nu?', *Tijdschrift voor compliance en zorg* 2011-2, p. 43-49.

Velink & De Die Advocaten 2011

Velink & De Die Advocaten, 'Informatie-uitwisseling in zorgketens. Wat mag, kan en moet?', *Achtergrondstudie ten behoeve van de SGZ* 2011, p. 1-45.

Verhey 1997

L.F.M. Verhey, 'De EG-richtlijn bescherming persoonsgegevens: uitgangspunten en hoofdlijnen', *NJCM-Bulletin* 1997, p. 239-256.

Verhey 2011

L.F.M. Verhey, 'Grondrechten in het digitale tijdperk: driemaal is scheepsrecht?', *TVCR* 2011, p. 152-167.

Parlementaire stukken

Kamerstukken II 1997/98, 25 892, nr. 3.

Kamerstukken II 2007/08, 31 466, nr. 3.

Kamerstukken II 2007/08, 31466, nr. 4.

Kamerstukken II 2006/07, 27 529, nr. 29.

Kamerstukken II 2011/12, 33 000 XVI, nr. 39.

Kamerstukken II 2010/11, 27 529, nr. 67.

Kamerstukken II 2010/11, 27 529, nr. 71.

Kamerstukken II 2010/11, 27 529, nr. 73.

Kamerstukken II 2010/11, 27529, nr. 74.

Kamerstukken II 2010/11, 27529, nr. 75.

Handelingen II 2010/11, 8 november 2011.

Handelingen II 2010/11, 84, p, 51.

Handelingen II 2010/11, 99, p, 4.

Kamerstukken I 2010/11, 31 466, nr. 1.

Kamerstukken I 2008/09, 31 466, nr. C.

Kamerstukken I 2009/10, 31 466, nr. C.

Kamerstukken I 2009/10, 31 466, nr. F.

Kamerstukken I 2010/11, 31 466, nr. V.

Kamerstukken I 2010/11, 31466, nr. X.

Kamerstukken I 2010/11, 31 466, nr. Y.

Kamerstukken I 2010/11, 31 466, nr. 20.

Kamerstukken I 2010/11, 32 761, nr. 1, Bijlage Leidraad afstemmen van wetgeving op de Wet bescherming persoonsgegevens, p. 1-96.

Handelingen I 2010/11, 20, p, 1-19.

Handelingen I 2010/11, 22, p, 10.

Handelingen bij het Ontwerp van decreet betreffende het gezondheidsinformatiesysteem, *Parl. St.* VI. Parl. 2005-2006, nr. 531- 5, p. 5 (België).

Brief van de minister van VWS aan de Tweede Kamer, ‘Vragen n.a.v. brief 11 april 2011 inzake stand van zaken EPD’, *MEVA-U-3061881* 2 mei 2011, p. 1-15.

Brief van de minister van VWS aan de Tweede Kamer, 'Antwoorden op de vragen van het Kamerlid Omtzigt (CDA) over het College Bescherming Persoonsgegevens (CBP) en patiëntendossiers', 100163-100046-MEVA 23 september 2011, p. 1-4.

Brief van de minister van VWS aan Eerste Kamer, 'Stand van zaken digitale gegevensuitwisseling in de zorg na aanvaarding van de motie Mulder c.s.', MEVA/ICT-3096140 8 december 2011, p. 1-3.

Brief VVZ i.o. aan de minister van VWS, 8 december 2011, p. 1.

Brief CBP aan VVZ, 'Doorstart landelijke infrastructuur', 18 januari 2012, p. 1-2.

Elektronische bronnen

<www.cozo.be> (Inschrijving in het eHealth verwijsregister).

<www.ehealth.fgov.be> (Basisdienst Geïntegreerd gebruikers- en toegangsbeheer).

<www.ehealth.fgov.be> (INSZ als unieke identificatiesleutel?).

<www.ehealth.fgov.be> (nr. 8: optreden als onafhankelijke derde voor het coderen en anonimiseren van persoonsgegevens m.b.t. de gezondheid voor bepaalde, in de wet opgesomde instanties, ter ondersteuning van het wetenschappelijk onderzoek en het beleid).

<www.infoepd.nl> (Wettelijke basis voor het landelijke EPD).

<www.informatiepuntepd.nl> (E-learningmodule mandate).

<www.uziregister.nl> (veilig gebruik UZI-pas).

<www.wetenschap.infonu.nl/recht-en-wet/71544-werking-van-het-europees-recht-in-de-nationale-rechtsorde.html> (werking van het Europees recht in de nationale rechtsorde).

M. Chavannes, 'Schippers orkestreert iedereen over de elektronische snelweg', *NRC Handelsblad* 17 december 2011 <www.weblogs.nrc.nl/opklaringen>.

Toegang elektronisch patiëntendossier beter geregeld. Behandelrelatie voorwaarde voor toegang dossier, Den Haag: CBP 2011 (www.cbpweb.nl/Pages/pb_20080428_toegang_epd.aspx).

Wetten

Decreet van 16 juni 2006 tot oprichting van het Gezondheidsinformatiesysteem (België).

Wet bescherming persoonsgegevens.

Wet op de beroepen in de individuele gezondheidszorg.

Wet op de geneeskundige behandelingsovereenkomst.

Wet houdende diverse bepalingen van 27 december 2006 (België).

Wet houdende diverse bepalingen van 1 maart 2007 (België).

Wet houdende oprichting en organisatie van het eHealth-platform van 21 augustus 2008 (België).

Wet verwerking persoonsgegevens (België).

Wetboek van Strafrecht.

Wet tot wijziging van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Commissie voor de bescherming van de persoonlijke levenssfeer en tot uitbreiding van haar bevoegdheden (België).

Verdragen

Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (1951).

Internationaal Verdrag inzake burgerrechten en politieke rechten (1966).

Verdrag betreffende de werking van de Europese Unie (1957).

Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (1981).

Richtlijnen

Richtlijn 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 23 november 1995 inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. (*PbEG 1995, L 281*).

Aanbevelingen

Aanbeveling no. R (97) 5 van het Comité van Ministers van de Lid-Staten betreffende de bescherming van medische gegevens, Stcrt. 1998, 38.

Jurisprudentielijst

Europees Hof voor de Rechten van de Mens

EHRM 6 september 1978, nr. 5029/71, A-28, r.o. 58 (*Klass tegen Duitsland*).

EHRM 26 maart 1987, nr. 9248/81, r.o. 48 (*Leander tegen Zweden*).

EHRM 28 oktober 1994, nr. 14310/88, A-300-A, r.o. 91, r.o. 93 (*Murray tegen het Verenigd Koninkrijk*).

EHRM 25 januari 1997, nr. 22009/93, RJD 1997-I, r.o. 96, r.o. 103 (*Z. tegen Finland*).

EHRM 25 juni 1997, nr. 20605/92, RJD 1997-III, r.o. 45 (*Halford tegen het Verenigd Koninkrijk*).

EHRM 4 mei 2000, nr. 28341/95, RJD 2000-V, r.o. 41, r.o. 46, r.o. 57. (*Rotaru tegen Roemenië*).

EHRM 28 januari 2001, nr. 44647/98, RJD 2003-I, r.o. 59 (*Peck tegen het Verenigd Koninkrijk*).

EHRM 25 september 2001, nr. 44787/98, RJD 2001-IX, r.o. 57 (*P.G. en J.H. tegen het Verenigd Koninkrijk*).

EHRM 24 juni 2004, nr. 59320/00, RJD 2004-VI, r.o. 52 (*Von Hannover tegen Duitsland*).

EHRM 25 oktober 2005, nr. 2428/05, p. 11 (*Wypych tegen Polen*).

EHRM 6 juni 2006, nr. 62332/00, r.o. 90 (*Segerstedt-Wiberg e.a. tegen Zweden*).

EHRM 4 januari 2007, nr. 39658/05, p. 4 (*Smith tegen het Verenigd Koninkrijk*).

EHRM 17 juli 2008, nr. 205II/ 03 (*I tegen Finland*).

Europees Commissie voor de Rechten van de Mens

ECRM 19 mei 1994, nr. 15225/89, r.o. 48 (*Friedl tegen Oostenrijk*).

Hof van Justitie

HvJ EG 15 juni 1964, nr. 6/64, Costa/ENEL, *Jur.* 1964, p. I-1199.

HvJ EG 13 november 1990, nr. C-106/89, Marleasing, *Jur.* 1990, p. I-4135.

HvJ EG 15 december 1995, nr. C- 415/93, Faccini Dori, *Jur.* 1995, p. I-3325.

Hoge Raad

HR 9 januari 1989, NJ 1987, 928 (Edamse bijstandmoeder).

Grondwettelijk Hof (België)

Grondwettelijk Hof 14 februari 2008, nr. 15/2008, BS 12 maart 2008.

Grondwettelijk Hof 18 maart 2010, nr. 29/2010, BS 18 maart 2010.