



Universiteit
Leiden
The Netherlands

Het elektronisch patientendossier: de overheid als koppelbaas

Mommers, L.

Citation

Mommers, L. (2008). Het elektronisch patientendossier: de overheid als koppelbaas. *Tijdschrift Voor Internetrecht*, 1(5), 119-123. Retrieved from <https://hdl.handle.net/1887/13230>

Version: Not Applicable (or Unknown)

License: [Leiden University Non-exclusive license](#)

Downloaded from: <https://hdl.handle.net/1887/13230>

Note: To cite this publication please use the final published version (if applicable).

Het elektronisch patiëntendossier: de overheid als koppelbaas

L. Mommers

De overheid geeft nog altijd blijk van een groot vooruitgangsgeloof als het gaat om informatie- en communicatietechnologie. Dat geldt ook voor de invoering van het elektronisch patiëntendossier. Weliswaar moest de overheid haar ambities temperen na de moeizame plaatselijke en regionale ontwikkeling van EPD's, toch kiest zij er nu voor om een landelijke infrastructuur te introduceren. Het gaat 'slechts' om een koppelingsmechanisme, dat bestaande en toekomstige lokale en regionale EPD's met elkaar verbindt. Toch gaat zij daarmee voorbij aan belangrijke bezwaren tegen zo'n infrastructuur, zoals het feit dat die nog steeds sterk centralistisch van aard is, met alle privacy- en beveiligingsrisico's van dien. Dit artikel behandelt de belangrijkste bezwaren tegen de koppelingsinfrastructuur die het landelijk EPD in Nederland behelst, en de risico's die daaruit voortvloeien voor de vertrouwelijke omgang met medische gegevens.

1. Inleiding

Onder meer ter voorkoming van medische fouten wordt dezer dagen een koppelingsinfrastructuur voor elektronische patiëntendossiers ingevoerd. 'Kennis, in de zin van dossierkennis en feitenkennis, is essentieel voor het verlenen van goede zorg', aldus de Memorie van Toelichting bij de Wijziging Wet gebruik burgerservicenummer in de zorg.¹ Deze MvT vervolgt met de redenering dat een verantwoord zorg, zoals die wordt geëist door de Kwaliteitswet zorginstellingen en de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG), kan worden ondersteund door voortschrijdende mogelijkheden in de informatie- en communicatietechnologie. Met name de verbeterde mogelijkheden voor informatievoorziening dragen daaraan bij. De norm van 'verantwoorde zorg' zou aldus ook strenger worden. Het eerste voorbeeld dat de MvT noemt, is de mogelijkheid om elkaar uitsluitende medicaties snel te signaleren en zodoende medicatiefouten te voorkomen.² Bovendien zou volgens de MvT onderzoek uitwijzen dat de helft van de patiënten klaagt over gebrekkige gegevensuitwisseling tussen zorgaanbieders. Helaas vermeldt de MvT niet de bron van dat onderzoek.

Anekdotisch bewijs is er in elk geval voldoende voor de noodzaak van een betere gegevensuitwisseling in de zorg. Zo worden identieke onderzoeken bij een transfer van het ene ziekenhuis naar het andere vaak overgedaan, zonder dat daar enige noodzaak toe is. Bovendien worden er inderdaad regelmatig medicatiefouten gemaakt. Dat ligt echter vaak niet aan het ontbreken van een ICT-voorziening, maar simpelweg aan het ontbreken van goede communicatie tussen zorginstellingen. De fout die vaak gemaakt wordt, is te denken dat ICT-voorzieningen bestaande 'bad practices' kun-

nen verbeteren. Maar wanneer een organisatie van goede 'analoge' communicatie ontbreekt, zal een ICT-voorziening alleen (zonder organisatorische veranderingen) geen heilzame werking hebben. Ook het niet-gebruiken of interpreteren van aanwezige informatie is debet aan veel fouten. Zo gaat met name in de daadwerkelijk toediening van medicijnen veel mis. Daarop heeft het landelijk EPD niet of nauwelijks invloed, omdat het slechts de uitwisseling van informatie tussen instellingen faciliteert, niet het correcte gebruik ervan binnen instellingen. Zo lijkt het EPD als een middel voor alle kwalen te worden geïntroduceerd, terwijl het EPD *hoogstens* als conditio sine qua non voor die kwalen beschouwd kan worden.

Opvallend aan de landelijke introductie van het EPD in Nederland is dat zij volledig afhankelijk is gemaakt van de invoering van het burger service nummer (BSN). Dat blijkt onder meer uit de namen van de relevante wetgevingsdossiers.³ Dit uniek-identificerende nummer werd als noodzakelijke voorwaarde gezien voor de succesvolle uitrol van het EPD.⁴ De invoering van het EPD wordt geregeld via diverse wetten en regelingen, waarvan ik een overzicht geef in paragraaf 2. Vanwege de centrale rol van het BSN bespreek ik in paragraaf 3 een aantal veronderstellingen die ten grondslag lijken te liggen aan het gebruik van dit nummer. In paragraaf 4 bespreek ik de praktische risico's die zullen optreden met het EPD. Ik sluit in paragraaf 5 af met een conclusie.

2. Het wettelijk kader

Het wettelijk kader voor het elektronisch patiëntendossier wordt op het meest algemene niveau gevormd door de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO)⁵, de Wet bescherming persoonsgegevens (Wbp)⁶

1. *Kamerstukken II* 2007/08, 31 466, nr. 3, p. 4.

2. *Idem*, p. 4-5.

3. *Kamerstukken II* 2007-08, 30 380 (Wet gebruik burgerservicenummer in de zorg) en *Kamerstukken II* 2007/08, 31 466 (Wijziging wet gebruik burgerservicenummer in de zorg).

4. Dat moge onder meer blijken uit de naamgeving van de belangrijkste wetgeving rondom het EPD: Wet gebruik burgerservicenummer in de zorg, en de Wijziging Wet gebruik burgerservicenummer in de zorg.

5. Neergelegd in art. 7:446-468 BW, *Stb.* 1994, 837 en 838.

6. *Stb.* 2000, 302.

en de Wet algemene bepalingen burgerservicenummer.⁷ Meer specifiek volgen dan de Wet gebruik burgerservicenummer in de zorg⁸, het Besluit gebruik burgerservicenummer in de zorg⁹, en de Regeling gebruik burgerservicenummer in de zorg.¹⁰

2.1. Wet op de Geneeskundige Behandelingsovereenkomst

De WGBO en de WBP zien in onderlinge samenhang op de bescherming van persoonsgegevens van patiënten.¹¹ De WGBO (titel 7, afdeling 5 boek 7 BW) bevat een aantal artikelen die betrekking hebben op de informatiepositie van behandelaar, patiënt en derden. Art. 7:448 BW bepaalt het recht op informatie van de patiënt over onderzoek, gezondheidstoestand en voorgestane behandeling; art. 7:449 BW bevat het recht om juist informatie te weigeren (bijv. over het terminale karakter van een ziekte). Art. 7:454 BW beschrijft de inrichting van het medisch dossier en luidt als volgt:

‘1. De hulpverlener richt een dossier in met betrekking tot de behandeling van de patiënt. Hij houdt in het dossier aantekening van de gegevens omtrent de gezondheid van de patiënt en de te diens aanzien uitgevoerde verrichtingen en neemt andere stukken, bevattende zodanige gegevens, daarin op, een en ander voor zover dit voor een goede hulpverlening aan hem noodzakelijk is.

2. De hulpverlener voegt desgevraagd een door de patiënt afgegeven verklaring met betrekking tot de in het dossier opgenomen stukken aan het dossier toe.

3. Onverminderd het bepaalde in art. 455, bewaart de hulpverlener de bescheiden, bedoeld in de vorige leden, gedurende vijftien jaren, te rekenen vanaf het tijdstip waarop zij zijn vervaardigd, of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit, tenzij de patiënt een verzoek doet als bedoeld in art. 455.’

De WGBO is daarnaast vrij helder over de mate waarin anderen dan de patiënt en zijn behandelaar toegang kunnen krijgen tot informatie over de behandeling. Art. 455 lid 1 behelst het recht van de patiënt om gegevens te laten vernietigen (tenzij het belang van een andere patiënt of een wettelijke bepaling zich daartegen verzet). Art. 456 bepaalt het recht op inzage voor de patiënt. Art. 457 lid 1 vereist dat voor verstrekking aan derden expliciete toestemming van de patiënt vereist is. Daarop gelden als uitzonderingen in art. 458 lid 1 dat verstrekking in verband met statistieken en wetenschappelijk onderzoek, en bij onmogelijkheid van toestemming, onder bepaalde condities wel toegestaan zijn.

2.2. Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens bevat de regels die bepalen onder welke condities persoonsgegevens verwerkt mogen worden. Medische gegevens vallen onder de categorie ‘bijzondere persoonsgegevens’, waarvan aan de verwerking strengere eisen worden gesteld. Verwerking van deze gegevens is verboden tenzij bij of krachtens de Wbp verwerking wordt toegestaan. Er is onder meer een uitzondering

gemaakt voor ‘hulpverleners, 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’ (art. 21 lid 1 onder a).

Een aanvullende bepaling stelt dat gegevens betreffende erfelijke eigenschappen ‘[slechts mogen] worden verwerkt voor zover deze verwerking plaatsvindt met betrekking tot de betrokkene bij wie de betreffende gegevens zijn verkregen [...]’. Hierop gelden als uitzonderingen de situatie waarin een zwaarwegend medisch belang de doorslag geeft, en de verwerking voor wetenschappelijke en/of statistische doeleinden (lid 4 onder a en b). Een uitzondering op het verbod om bijzondere gegevens in het algemeen te verwerken, treedt bovendien onder meer op als ‘dit geschiedt met uitdrukkelijke toestemming van de betrokkene’ (art. 23 lid 1 onder a).

2.3. Wet algemene bepalingen burgerservicenummer

Deze kaderwet bevat de bepalingen waarmee het gebruik van het burgerservicenummer in bredere zin is vormgegeven, zoals de uitgifte van het nummer, en de inrichting van de beheersvoorziening. Met deze wet zijn de belangrijkste randvoorwaarden geschapen voor de invoering van het BSN in 2006.

2.4. Wet gebruik burgerservicenummer in de zorg

De Wet gebruik burgerservicenummer in de zorg regelt – in een voor een wet groot functioneel (technisch) detail – de basis voor het EPD.¹² Gekozen is voor een gedistribueerd model: er is niet één centraal opgeslagen, landelijk EPD, maar alleen een landelijk schakelpunt (art. 13a). Dit schakelpunt beheert een verwijzingsindex op basis van de inhoud van lokale patiëntendossiers. Zo laat zich informatie op verschillende plaatsen terugvinden. In die zin is de verwijzingsindex te beschouwen als een soort internetzoekmachine – die immers ook de informatie op andere servers via een index ontsluit – waarbij uiteraard, anders dan bij zo’n zoekmachine, de toegang niet openbaar is.

De toegang tot de landelijke verwijzingsindex is beperkt tot zorgverleners waarvan het eigen EPD-systeem is gecertificeerd als ‘Goed Beheerd Zorgsysteem’ (GBZ). Toegang tot gegevens is voorbehouden aan beroepsbeoefenaren in de zin

7. Stb. 2007, 288.

8. Stb. 2008, 164.

9. Stb. 2008, 185.

10. Stcrt. 2008, 105.

11. Bonthuis, M.J., ‘Privacy en het landelijk elektronisch patiëntendossier’, in: *Privacy & Informatie*, 2008, nr. 3, p. 119-123.

12. Wet gebruik burgerservicenummer in de zorg, Stb. 2008, 164, gelezen in samenhang met het wijzigingsvoorstel in *Kamerstukken II* 2007/08, 31 466, Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg.

van de Wet BIG.¹³ Deze personen beschikken over een zogeheten UZI-nummer, dat de zorgverlener (een persoon) uniek identificeert. De zorgaanbieder beschikt over een UZI-abonnenummer, een uniek identificatienummer voor die instelling. Ook de patiënt is uniek geïdentificeerd, zoals hierboven beschreven, via het burgerservicenummer.

2.5. Lagere regelingen

Het Besluit gebruik burgerservicenummer in de zorg¹⁴ regelt de nadere invulling van de zogenaamde 'sectorale berichtenvoorziening in de zorg', waaronder de aansluiting van het landelijk schakelpunt op de bestaande beheersvoorziening voor het burgerservicenummer. Uit de toelichting op de Regeling gebruik burgerservicenummer in de zorg¹⁵, die een nadere invulling geeft door de toepasselijke standaarden voor de berichtenuitwisseling te bepalen, blijkt onder meer dat het de bedoeling is om medewerkerspassen uit te geven die niet op naam zijn gesteld. Daarmee wordt gebroken met het idee alle gebruikers van het EPD-systeem uniek te identificeren. De desbetreffende passen zouden echter geen toegang geven tot inhoudelijke gegevens uit EPD's, en daarmee het risico van ontraceerbaar ongeautoriseerd gebruik van het EPD voorkomen. Hiermee moet ook het ontbreken van evenwicht tussen traceerbaarheid van toegang en traceerbaarheid van het onderwerp van het EPD (de patiënt) enigszins hersteld worden.

Het EPD wordt gefaseerd ingevoerd, te beginnen met het elektronisch medicatiedossier en het waarnemingsdossier voor huisartsen. Tijdens de invoering zal een voorlichtingscampagne gevoerd worden over het EPD, waarin onder meer aandacht wordt geschonken aan het recht op verzet tegen de toegankelijkheid van je medische gegevens. In de Wet gebruik burgerservicenummer in de zorg is die mogelijkheid geschapen, terzake van de toegankelijkheid van medische gegevens door andere instellingen. De waarde van dat recht zou in de praktijk tegen kunnen vallen, gezien de druk vanuit zorgverleners om uitwisseling toe te staan.

3. Vooronderstellingen bij het EPD

Voor de juiste koppeling van gegevens aan personen werd het door de wetgever nodig geacht het Burger Service Nummer (BSN) in te zetten bij de totstandbrenging van het EPD. Dat nummer werd in 2006 ingevoerd als 'opvolger' van het SoFi-nummer, onder meer om de toegang tot elektronische overheidsdiensten te vergemakkelijken en koppeling van databestanden door de overheid te faciliteren. De voordelen van zo'n eenduidig persoonsnummer lijken duidelijk: vermindering van administratieve lasten van burger en overheid, en betere controlemogelijkheden voor de juistheid van gegevens. Maar er zijn ook nadelen: het nummer biedt potentieel gevaarlijke mogelijkheden om allerlei gegevens over een persoon te koppelen. Het BSN zelf is niet geheim, maar biedt wel – soms met minimale extra gegevens – een ingang in allerlei databanken.

Aan de mogelijkheid van een verantwoord gebruik van het Burger Service Nummer lijken vier vooronderstellingen ten grondslag te liggen¹⁶, die van direct belang zijn voor de toepassing van het nummer in het EPD. De eerste vooronderstelling is dat de overheden, en de partijen aan wie zij gebruik van het BSN toelaat, in al hun geledingen integer zijn

– en blijven. De verwerkingsmogelijkheden van overheden, instellingen en bedrijven nemen immers toe door het centrale 'scharnierpunt' dat het BSN levert; foutieve of frauduleuze informatie kan gericht worden 'geïnjecteerd' in databanken via het BSN als de beveiliging niet op orde is, evenzo kan ook met niet-legitieme motieven informatie gemakkelijker worden gelokaliseerd met behulp van het BSN. Een aanval op de integriteit van één van de systemen houdt nu sneller een aanval in op de integriteit van alle systemen die eraan gekoppeld zijn. De tweede vooronderstelling is, dat informatie over een burger in alle contexten hetzelfde betekent, zodat die vrij uitgewisseld kan worden zonder consequenties voor de betekenis. Dat is een misverstand. Diverse medische specialismen werken met hun eigen jargon, dat bij ongeleid en ongeclausuleerd gebruik bij andere specialismen tot misverstanden kan leiden.

De derde vooronderstelling is dat de overheid het gebruik van het BSN kan controleren. Ook dit is een misverstand. Het BSN is weliswaar een handig hulpmiddel bij automatisering van gegevensstromen, maar met het BSN is de juiste werking van die gegevensstromen nog niet gegeven. Dat vereist complexe en goed gebouwde ICT-systemen, en het correcte gebruik daarvan, omdat gevolgen van een integriteitsaanval groter zijn dan bij 'stand-alone' systemen. Beide zaken blijken in de praktijk vaak lastig te realiseren. De vierde vooronderstelling is dat de gevolgen van de invoering van het BSN overzienbaar zijn. Dat is niet noodzakelijkerwijs het geval. Het aantal gebruikers van het BSN, en daarmee het aantal koppelingen, zullen groeien, evenals de 'intelligente' verwerkingsmogelijkheden voor persoonsgegevens. Het opstellen van veelomvattende profielen van mensen buiten hun medeweten om zal gemakkelijker worden door de unieke 'sleutel' die het BSN levert.

De onjuistheid van deze vooronderstellingen voeden de gedachte dat het toegankelijk maken van gegevens via het BSN onvoorziene consequenties kan hebben. Als informatie zo snel en gemakkelijk te verkrijgen is als vandaag de dag via elektronische netwerken, wordt het van groot belang die informatie kunstmatig te 'compartimenteren'. Net als bij een oceaanstomer kan die compartimentering helpen om bij een opgetreden lek alleen een klein onderdeel 'kwijt te raken', terwijl de rest blijft. Naarmate persoonsgegevens gekoppeld worden aan één identificerend nummer, wordt de kans groter dat deze compartimentering niet bewaard blijft. De universele 'sleutel' die het BSN vormt, maakt het namelijk mogelijk om gegevens in allerlei databanken met elkaar te combineren.

13. Wet op de beroepen in de individuele gezondheidszorg, *Stb.* 1993, 655.

14. Besluit gebruik burgerservicenummer in de zorg, *Stb.* 2008, 185.

15. Regeling gebruik burgerservicenummer in de zorg, *Stcrt.* 2008, 105.

16. L. Mommsers, 'Burger Service Nummer: het virtuele dwangbuis van de overheid', in: *Openbaar Bestuur*, 1, p. 34-36.

Weliswaar moet naast die 'sleutel' ook nog daadwerkelijk toegang tot zo'n databank worden verkregen – maar als die toegang er is, bijvoorbeeld voor een bevoegde instantie of een onbevoegde hacker, zijn belangrijke barrières om gegevens te koppelen weggenomen. Compartimentering maakt de beheersorganisatie anders en complexer. Het betekent namelijk dat de koppeling tussen delen van het virtuele dossier moet verlopen via verschillende uniek-identificerende nummers of andere uniek-identificerende kenmerken. Dit betekent in de praktijk dat tussen bijvoorbeeld elk paar instellingen onderling afspraken gemaakt moeten worden over de uitwisseling van gegevens. Er is dan geen centrale verwijsindex nodig. Het delen van gegevens wordt daardoor een aangelegenheid van twee instellingen onderling. Het aantal mogelijke koppelingen wordt daardoor groter, en ook dat houdt risico's in.

De vier vooronderstellingen hierboven gelden voor gebruik van het BSN in het algemeen. Aan de gekozen opzet van het landelijk EPD ligt naar mijn mening nog een aantal andere vooronderstellingen ten grondslag.¹⁷ Ten eerste, dat door de informatie over een patiënt bij verschillende zorginstellingen via het BSN aan elkaar te koppelen, een completer en coherent beeld ontstaat van die patiënt. Ten tweede, dat dit goed is voor de kwaliteit van de zorg, die immers gebaat is bij beschikbaarheid van actuele en betrouwbare gegevens bij alle behandelende partijen.

Aan de beschikbaarheid van medische gegevens zit een keerzijde. Zo leidt digitale beschikbaarheid van gegevens niet automatisch tot een bruikbaar, actueel en consistent beeld van de zorgbehoeften van een patiënt. Gegevens kunnen elkaar tegenspreken. Bovendien is de beschikbaarheid van gegevens nog geen garantie dat deze ook daadwerkelijk gelezen, begrepen en gebruikt worden. In dit verband kan een beknopte, heldere verwijsbrief met de belangrijkste relevante gegevens aanmerkelijk effectiever zijn.

Papieren dossiers op verschillende locaties, en zelfs lokale elektronische patiëntendossiers, hebben de prettige eigenschap dat zij lastig toegankelijk zijn voor mensen van buiten een zorginstelling. Buiten die zorginstelling zijn aanmerkelijk meer mensen die niets met die gegevens te maken hebben, dan mensen die geldige redenen hebben om er inzage in te willen.

Uitgaan van het verantwoordelijkheidsgevoel van mensen die toegang hebben tot gegevens kan gemakkelijk tot misbruik leiden. De zorgverleners die straks in medische gegevens willen bladeren van een patiënt die ze niet behandelen, krijgen daartoe in beginsel toegang. Door de nauwe verbondenheid van verzekeraars met medische instellingen, uit hoofde van bijvoorbeeld budgettering en afrekening op basis van diagnose-behandelingscombinaties, is er ook het risico van 'institutionele nieuwsgierigheid' – de wens om zoveel mogelijk te weten over klanten. Die nieuwsgierigheid mag natuurlijk niet door het EPD gefaciliteerd worden.

Het recht van patiënten om zelf te beschikken over de verspreiding van hun gegevens kent ook z'n grenzen. Patiënten kunnen er volgens het wetsvoorstel Wijziging Wet gebruik burgerservicenummer in de zorg¹⁸ voor kiezen om de toegang tot hun eigen gegevens uit te schakelen voor bepaalde zorgaanbieders. Maar hoe hoog is de irritatiefactor die dat oproept bij de behandelaars van patiënten? Zullen patiënten

zich niet onder druk gezet voelen om toch alle informatie-sluisen open te zetten? Waarschijnlijk wel. Bovendien is uitwisseling de standaard, en moet de patiënt bezwaar maken als hij die uitwisseling niet wil toestaan; een opt-out-regeling dus.¹⁹

De juistheid van de vooronderstellingen die ten grondslag liggen aan de keuze voor een landelijk EPD, meer specifiek een landelijk schakelpunt, kan niet zonder meer bevestigd worden. Bovendien treedt er, in de afweging tussen het belang van privacy en dat van gegevensuitwisseling, een enorme verschuiving op in de richting van het laatste belang. Dat is, zo zal blijken uit de volgende paragraaf, eigenlijk niet goed in overeenstemming te brengen met het bestaande wettelijk kader voor de omgang van persoonsgegevens in de zorg.

4. Risico's in de praktijk

De trage en moeizame ontwikkeling van elektronisch patiëntendossiers leidde, zoals hierboven beschreven, tot de keuze voor een zogenaamde landelijke verwijsindex, die verschillende bestaande EPD-systemen met elkaar verbindt. In theorie ontstaat op nationale schaal straks maximale transparantie in de gezondheidszorg, omdat de verschillende lokale patiëntdossiers op elkaar worden aangesloten. Daarmee wordt voor alle artsen informatie beschikbaar die de behandeling kan verbeteren. Daarvoor moeten zij dan wél verklaren dat zij een behandelrelatie met de desbetreffende patiënt hebben, en dat die patiënt toestemming heeft gegeven om de gegevens in te zien.

Zorgverleners mógen die gegevens dus niet zomaar bekijken, maar ze kunnen het vaak wel. Hun handelen wordt weliswaar geregistreerd, en kan dus ook worden gesanctioneerd, maar de praktijk zal vermoedelijk weerbarstiger blijken, gezien de grote hoeveelheden gelogde informatie die gecontroleerd moeten worden. Toegang tot verschillende informatie-eilanden levert immers niet per definitie een coherent beeld op. Tegengestelde diagnoses blijven naast elkaar bestaan. Artsen zouden bovendien de discipline moeten opbrengen om hun bijdragen aan dossiers beter toegankelijk te maken voor collega's buiten hun eigen specialisme. De 'volledigheid' van een virtueel dossier brengt – in de fase waarin daadwerkelijk veel medische gegevens met elkaar gekoppeld worden via de landelijke verwijsindex – het reële gevaar van 'information overload' met zich mee. Waar moet een raadplegend arts beginnen met lezen om zich snel een beeld te vormen van zijn patiënt?

17. L. Mommers, 'Patiëntdossier is overbodig en gevaarlijk', in: *NRC Handelsblad*, 17 juni 2008, p. 7. Zie ook K. Spaink, *Medische geheimen. Risico's van het elektronisch patiëntendossier*, Nijgh & Van Ditmar/XS4ALL Internet, 2005.

18. *Kamerstukken II* 2007/08, 31 466.

19. De regering spreekt enigszins eufemistisch van 'informed consent', zie: *Kamerstukken II* 2007/08, 31 466, nr. 3, p. 9.

Het verzamelen – of in dit geval via één route toegankelijk maken – van gegevens brengt niet automatisch met zich mee dat iemand zich een beeld vormt van de betekenis van die gegevens in hun onderlinge samenhang. Het idee dat het EPD medische fouten gaat voorkomen is dan ook slecht onderbouwd. Sterker, de overmaat aan gegevens kan juist ook een extra risico opleveren. De *veronderstelling* van consistentie kan tot het gebruik van onjuiste gegevens leiden. De introductie van het EPD geeft daarnaast ook risico's op het vlak van de privacy, zoals onrechtmatige verwerking van medische gegevens (toegang voor onbevoegden). Deze vloeien deels voort uit de digitalisering (en daaruit voortvloeiende verspreidingsmogelijkheden) van gegevens, maar ook uit de wijze waarop de organisatie en infrastructuur volgens de wet zullen worden ingericht.

Het voornaamste zwakke punt is te vinden in de zwakke beveiliging van het systeem voor ongeautoriseerde toegang. Door te kiezen voor een relatief 'open' systeem heeft de regering weliswaar veel praktische problemen in de invoering en het gebruik voorkomen, maar ook een belangrijk risico van misbruik geïntroduceerd. Vanuit andere instellingen dan de instelling die een bepaald EPD beheert, kan gemakkelijk toegang worden gezocht tot de gegevens daarin. De wet bepaalt weliswaar dat – in overeenstemming met de WGBO – in de meeste gevallen expliciete toestemming van en een behandelrelatie met de patiënt benodigd zijn, maar het systeem vereist daarvan geen bewijs, alleen een verklaring van de arts.

Het is de vraag of de toegepaste 'logging' van toegang tot dossiers daadwerkelijk voldoende dreiging oplevert om artsen ervan te weerhouden om zonder toestemming gegevens te raadplegen. Wel is 'logging' vanuit het oogpunt van beheersbaarheid van het systeem vooralsnog vermoedelijk het enig werkbare systeem. Tot slot zijn er nog de risico's die niet alleen bij elektronische, maar ook bij papieren dossiers spelen: persoonsverwisseling, onjuiste gegevens, en te sterk vertrouwen op de gegevens in het dossier. Of en hoe het gebruik van het EPD van invloed is op deze risico's, valt vooralsnog niet te bepalen.

5. Conclusie

In de informatiesamenleving is de papieren wetgevingswerkelijkheid van 'waarborgen' en 'beveiliging' al snel een was-sen neus. De technische en organisatorische waarborgen bij de architectuur van het landelijk schakelpunt, bedoeld om onrechtmatige uitwisseling van (bijzondere) persoonsgegevens te voorkomen, zijn te vrijblijvend voor deze categorie van gegevens. Voor mij staat bovendien niet onomstotelijk vast dat de vergaande koppeling van patiëntgegevens werkelijk een concreet doel dient. In beginsel dient de verspreiding van persoonlijke gegevens minimaal te zijn, en de controle van burgers over hun eigen gegevens maximaal. In de categorie van medische gegevens ligt dit beginsel een tikje genuanceerder, omdat de patiënt soms juist níet over bepaalde informatie wil beschikken.

De overheid heeft een belangrijke rol in het verbeteren van de 'digitale weerbaarheid' van haar burgers, en dient het eigen handelen daarop af te stemmen. Als het internet ons iets geleerd zou moeten hebben, dan is het wel dat onge-clausuleerde toegang tot grote hoeveelheden gegevens heel

handig, maar ook bijzonder schadelijk kan zijn. Helaas stelt de overheid al jaren uit pragmatische overwegingen de mogelijkheden van uitwisseling vóór bescherming van persoonsgegevens. Ondanks een negatief advies van de Raad van State zet de regering het wettelijk kader voor een landelijk EPD door.²⁰ De waarborgen in het huidige voorstel kunnen niet verhullen dat er een grove schending plaatsvindt van de privacybeginselen zoals die neergelegd zijn in de WGBO. De praktisch ongeclausuleerde toegang tot medische gegevens geen eigenschap die de overheid zomaar op het conto van werkbaarheid en de vage belofte van betere medische zorg mag bij schrijven.

20. Kamerstukken II 2007/08, 31 466, nr. 4.