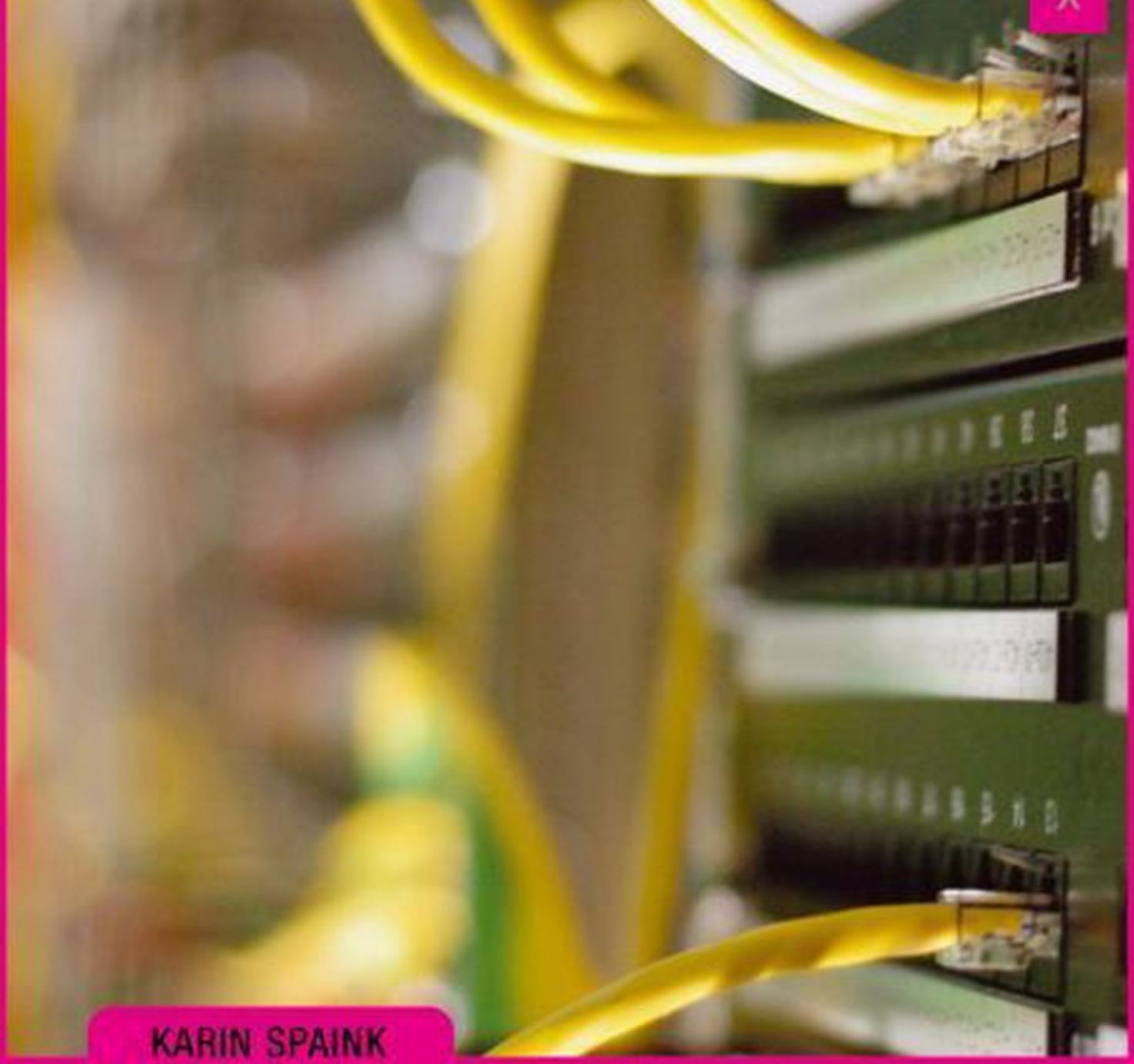

KARIN SPAINK

MEDISCHE GEHEIMEN

RISICO'S VAN HET ELEKTRONISCH PATIËNTENDOSSIER

NIJGH & VAN DITMAR // XS4ALL INTERNET

Inhoudsopgave

Zieke computers 4
Elektronische dossiers voor iedereen 4
Automatisering is geen panacee 5
Geschiedenis, grofweg 6
Doelstellingen 7
Mislukte centralisatie 9
Google voor medici 10
Schaalbaarheid, monopolies en beheer 11
Tussen regie en commercie 12
Er is niet niks... 13
De illusie van het gemeenschappelijk datamodel 14
...maar er moet ineens een heleboel 16
Identificatie en autorisatie van zorgverleners 17
Identificatie van patiënten 18
Inzagerecht voor patiënten 20
EPD als wegbereider voor eNIK 21
Patiëntenprivacy en opsporing 22
Marktwerking 23
Medische missers 24
Technologische oplossingen, of organisatorische? 26
Nieuwe systemen, nieuwe fouten 28
Databescherming, virussen en meekijkers 29
Conclusies 31
Met dank aan: 33
Noten 34
Literatuur 38

Medische geheimen

Risico's van het elektronisch patiëntendossier

Karin Spaink

Karin Spaink © 2005 / Nijgh & Van Ditmar
1e druk september 2005 (7000 ex)
2e druk november 2006 (2000 ex)

Zieke computers

Als er één ding is dat ziekenhuizen vrezen, is het een uitbraak van resistente bacteriën. Sommige strepto- en stafylokokken zijn in de afgelopen jaren immuun geworden voor penicilline; verspreidt zo'n bacterie zich in een ziekenhuis, dan zit er niets anders op dan de besmette afdelingen tijdelijk te sluiten en de patiënten in quarantaine te houden.

In maart 2005 maakte een Nederlands ziekenhuis voor het eerst bekend dat een modernere, maar niet minder ingrijpende besmetting had toegeslagen: het Spaarne Ziekenhuis in Hoofddorp kampte met een computervirus. Vanaf vrijdag 4 maart raakten de centrale servers gaandeweg overbelast en werkten al maar trager. Medewerkers konden elkaar amper berichten sturen en nog slechts mondjesmaat het internet raadplegen. [1]

Vooral in de poliklinieken veroorzaakte het virus chaos. Op de kop af een half jaar eerder, op 4 oktober 2004, waren de poliklinieken van het Spaarne overgestapt op elektronische patiëntendossiers. Sindsdien gaat niets meer op papier. Alle informatie over patiënten wordt sinds de instelling van de 'archiefloze poli' elektronisch uitgewisseld, geraadpleegd en bijgehouden. Diagnoses, recepten, verwijsbrieven, röntgenfoto's, uitslagen van laboratoriumonderzoek, correspondentie met andere artsen: alles zit in dat elektronische dossier en staat op de centrale servers. [2]

Vier dagen na de besmetting was het virus nog altijd niet verwijderd. Tijdens de opschoningsactie ontstond een nieuwe uitbraak. Het netwerk werd traag als stroop. 'In de loop van dinsdag [8 maart 2005] was het computerprogramma waarmee de gegevens van de patiënten op de poliklinieken op het beeldscherm verschijnen, zo verstoord dat de wachttijden onverantwoord lang werden,' deelde de woordvoerster van het ziekenhuis mee. De poliklinieken moesten een deel van de afspraken met patiënten afzeggen. Omdat hun informatie niet beschikbaar was, had het in een aantal gevallen sowieso geen zin dat de patiënten op de poli verschenen. Maar 'sommige specialisten hadden nog papieren dossiers die ze konden gebruiken.' [3] Uiteindelijk moesten 150 afspraken op de polikliniek (eenzesde van het totaal) worden verzet.

Pas een week na de besmetting waren de aangesloten computers weer virusvrij: alle negenhonderd pc's en laptops in het netwerk werden met de hand gecontroleerd en ge-update. De bron van het virus - een variant die uitsluitend op Windowsmachines toeslaat - kon niet worden achterhaald. 'De vraag is ook of we daar ooit achter zullen komen. Het baart ons natuurlijk zorgen dat er zomaar ergens een besmetting in het systeem heeft kunnen plaatsvinden, omdat alle computers een virusscanner hebben. Maar dat soort dingen kan nu eenmaal gebeuren. Ook bij ons,' meldde de woordvoerder van het Spaarne enigszins berustend. [4] Internet- en e-mailverkeer werd ook na de grote schoonmaak uit voorzorg nog niet toegestaan, wat tot gevolg had dat de polikliniek tijdelijk moest terugvallen op pen, papier en telefoon. De elektronische patiëntendossiers zouden later worden bijgewerkt, beloofde het ziekenhuis.

Het Spaarne benadrukte dat de spoedeisende hulp, de verpleegafdelingen, de intensive care, de hartbewaking en de operatiekamers geen gevolgen hadden ondervonden van de besmetting, en dat er evenmin patiëntengegevens verminkt of verloren waren geraakt. Maar wat zou er zijn gebeurd als het héle ziekenhuis inmiddels papierloos was, en afhankelijk zou zijn van een elektronisch archief?

Elektronische dossiers voor iedereen

Die vraag wordt steeds belangrijker. De komende jaren zullen alle ziekenhuizen, alle huisartsen en alle apothekers van papieren dossiers moeten overstappen op elektronische patiëntendossiers (EPD). Dat proces is circa tien jaar geleden in gang gezet en vordert traag, maar redelijk gestaag. De eerste fase van de invoering van

zo'n landelijk EPD is voor 1 januari 2006 gepland en behelst de verplichte ingebruikname van het elektronisch medicatiedossier (EMD), waarin alle medicijnen staan vermeld die iemand in de loop der jaren voorgeschreven heeft gekregen.

Ook het elektronisch waarneemdossier voor huisartsen moet per 1 januari 2006 overal in gebruik zijn genomen. Via dat waarneemdossier kunnen huisartsen een samenvatting van iemands patiëntendossier [5] naar de vervangend huisarts sturen. De waarnemer op zijn beurt kan een waarneem-retourbericht naar iemands vaste huisarts terugsturen, waarin hij vertelt wat hij heeft gedaan.

De ironie wil dat juist op de dag dat de virusbesmetting bij het Spaarne bekend werd, de Tweede Kamer met de minister van VWS over de landelijke invoering van het elektronisch patiëntendossier debatteerde. Het parlement stond in dat debat geen moment stil bij de risico's van de automatisering van het medisch bedrijf, die uitgerekend die dag zo treffend werden geïllustreerd. De Tweede Kamer vond unaniem dat het ministerie een voortvarender aanpak in het veld moest afdwingen. Om die reden eisten de politieke partijen garanties van minister Hoogervorst dat het elektronisch medicatiedossier inderdaad per 1 januari 2006 overal in het land zal worden ingevoerd. Hoogervorst beloofde 'met ijzeren vuist te zullen regeren'. Indien noodzakelijk zou hij de vereiste samenwerking in de sector wettelijk afdwingen: 'Als het niet goedschiks gebeurt, dan kwaadschiks, maar vanaf 1 januari werkt iedereen mee.' [6] Het parlement heeft ondertussen meermalen aangegeven dat het eigenlijk vindt dat op die datum niet alleen het EMD maar het hele EPD al volledig zou moeten functioneren.

De realiteit haalde Hoogervorst overigens al snel in. In een nota van juni 2005 over de invoering van het EMD was hij al een stuk minder stellig: 'De planning is dat in het eerste kwartaal van 2006 vijf tot tien procent van de ziekenhuizen, apotheken en centrale huisartsenposten het elektronisch medicatiedossier […] gaan gebruiken.'[7]

Automatisering is geen panacee

Opmerkelijk is het grote vertrouwen in automatisering dat het parlement en de overheid in deze en eerdere debatten over het onderwerp tentoonspreidden. Voor zover er kritiek is of vragen zijn, beperken die zich tot de traagheid van de invoering van het EPD en enigszins gratuite bezorgdheid over de privacy van patiënten. Allerwegen lijkt men te verwachten dat elektronische patiëntendossiers de gezondheidszorg efficiënter, goedkoper en veiliger zullen maken. Niemand in de regering of het parlement zet vraagtekens bij de schaal van de operatie, noch bij de premisses ervan.

Het staat buiten kijf dat de medische sector veel slimmer en efficiënter met patiëntengegevens kan omspringen dan nu gebeurt. Invoering van een landelijk dekkend EPD is echter een buitengewoon complexe operatie. In het verleden hebben we door schade en schande moeten ervaren dat de problemen die met grote automatiseringsprojecten gepaard gaan, systematisch worden onderschat. Recente voorbeelden zijn:

- De chaos bij de studiefinanciering. Duizenden studenten kregen een verkeerd bedrag of zelfs helemaal geen beurs, en tienduizenden studenten bleken verkeerd in de computer te staan en kregen hun gegevens met geen mogelijkheid gecorrigeerd.
- De mislukte poging begin jaren negentig om de politie-informatie deels te automatiseren en de lokale systemen aan elkaar te knopen. De software is uiteindelijk afgeschaft en de hele operatie werd van voren af aan overgedaan.
- De aanvankelijke mislukking van C2000, het digitale netwerk voor hulpdiensten, [8]waardoor ambulances plotseling de eerste hulp niet meer konden bereiken en naar de zojuist afgeschafte mobilofoon moesten teruggrijpen.

- De sociale diensten van de grote steden, die minstens eens per week kampen met een netwerk dat plat ligt (waardoor gegevens niet kunnen worden opgezocht), en waar geregeld blijkt dat de gegevens van de cliëntèle slecht beschermd zijn. [9]

Het zijn pijnlijke voorbeelden van grote projecten die ofwel in schoonheid sneefden, ofwel lang kwakkelden en aanzienlijk meer kostten dan begroot was voordat ze enigszins aan de verwachtingen konden voldoen.

Automatisering is geen sinecure. De vraag is of het optimisme van het kabinet en het parlement over de invoering van het EPD terecht is. Juist bij de automatisering van patiëntendossiers dien je buitengewoon behoedzaam te werk gaan. De erin vervatte gegevens handelen per definitie over lijf en leden, en maken zodoende soms het verschil uit tussen leven en dood. Daarnaast is privacy juist in de gezondheidszorg een niet te onderschatten factor: patiënten moeten er volledig op kunnen vertrouwen dat hun artsen, specialisten, apothekers en verplegers buitengewoon discreet met hun gegevens omspringen. Wie zou nog een aids-test laten doen als hij weet dat de uitslag in verkeerde handen kan vallen, wie zou nog met zijn huisarts durven praten over zijn chronische ziekte als hij vreest dat die informatie bij zijn aanstaande werkgever belandt?

Daarnaast lijken tal van randvoorwaarden en vooronderstellingen onvoldoende doordacht. Zijn ziekenhuizen en huisartsen wel klaar voor zo'n alles omvattende operatie? Zijn hun computernetwerken erop berekend, en zijn hun computers voldoende beschermd tegen virussen, die trouwens steeds venijniger worden? Hoeveel informatie moet een EPD eigenlijk minimaal (of maximaal) bevatten om metterdaad nuttig te zijn? Zijn de voordelen van een elektronisch dossier boven een papieren dossier zo groot als wordt verondersteld? Is het inderdaad zo dat het EPD, zoals men in de politiek fervent hoopt, het percentage medische missers doet afnemen, bijvoorbeeld doordat medicatiefouten ermee worden voorkomen? Kun je een dergelijke vergaande vorm van automatisering wel invoeren zonder veranderingen in de organisatiestructuur van de gezondheidszorg aan te brengen?

Wat die patiënten (of beter: burgers, want we zijn allemaal patiënt, van tijd tot tijd) intussen van het EPD vinden, weet eigenlijk niemand. Want hoewel de politiek en, zoals dat zo mooi heet, 'het veld' zich al bijna tien jaar bezig houden met de voors en tegens ervan, de ins en outs, de kosten en de baten, de belangen en de conflicten, de aanpak en de fasering, de hobbels en de bottle-necks, en al doende nota op nota produceren, is er tot op heden geen enkele publieke discussie geweest over het elektronisch patiëntendossier; niet over de voordelen en niet over de risico's ervan. Invoering van het EPD wordt hoofdzakelijk als een technische aangelegenheid beschouwd, niet als een maatschappelijk of politiek vraagstuk.

Geschiedenis, grofweg

Tijdens het ministerschap van Els Borst (1994-2002) is het technologiebeleid in de zorg in de steigers gezet. Borst constateerde dat de zorg nogal achterliep met het toepassen van ICT en riep de hulp in van de Raad voor de Volksgezondheid en Zorg (RVZ). Die publiceerde in september 1996 de nota *Informatietechnologie in de zorg*. De RVZ bepleitte drie onderling samenhangende zaken: invoering van een chipkaart, verzamelen van alle relevante informatie over patiënten in één elektronisch dossier, en gebruikmaking van de elektronische snelweg. [10] De toelichting van de RVZ is nog altijd heel verhelderend:

> 'Wanneer de patiënt gebruik maakt van de diensten van meerdere zorgverleners, dan worden er op verschillende plaatsen gegevens over de patiënt vastgelegd: de onderzoeken die zijn verricht, de therapie die is ingesteld, de resultaten die zijn behaald, e.d.

Deze gegevens kunnen ook van groot belang zijn voor andere zorgverleners dan degene die over deze gegevens beschikt. Zo kan overbodig onderzoek worden voorkomen, kunnen ongewenste interacties tussen therapieën worden voorkomen, kan sneller inzicht worden verkregen in de patiëntencarrière, enz. Om dit te bewerkstelligen, dient de informatie die door verschillende zorgverleners is vastgelegd, beschikbaar te zijn voor andere zorgverleners die deze informatie voor hun taakuitoefening nodig hebben.

Met de huidige papieren dossiers kan in veel gevallen niet aan deze eis worden voldaan. Ze zijn moeilijk toegankelijk voor andere zorgverleners, zeker wanneer zij in een andere organisatie werkzaam zijn. Bovendien is vaak onbekend dat op een andere locatie voor de zorgverlening relevante gegevens beschikbaar zijn. Om hierin te voorzien, zijn er drie dingen belangrijk. In de eerste plaats dient - voorzover de patiënt hiervoor toestemming heeft verleend - de zorgverlener na te kunnen gaan waar welke informatie over de patiënt elders aanwezig is.

In de tweede plaats dienen de papieren dossiers vervangen te worden door *elektronische patiënten dossiers*. Elke zorgverlener legt de gegevens gestructureerd en gestandaardiseerd in digitale vorm vast. Aanvankelijk zal dit nog veelal in de vorm van vrije tekst zijn, maar er dient naar te worden gestreefd dit naar verloop van tijd in toenemende mate in gecodeerde vorm te doen.

In de derde plaats dient er een *elektronische snelweg* gerealiseerd te worden die continu beschikbaar, betrouwbaar, veilig en snel is. Deze snelweg - die overigens dezelfde kan zijn als de snelweg die ook door andere sectoren gebruikt wordt - moet de zorgverlener in staat stellen via de zorgchip toegang te krijgen tot voor de zorg relevante informatie die elders aanwezig is in de elektronische (deel)dossiers.

Het spreekt vanzelf dat de privacy van de patiënt hierbij gewaarborgd dient te zijn. Patiëntgegevens dienen in versleutelde vorm (cryptografisch) over de elektronische snelweg verzonden te worden. Vastgelegd dient te worden wie wanneer welke patiëntinformatie heeft ingezien en/of gewijzigd, opdat vastgesteld kan worden of iemand onrechtmatig toegang tot patiëntgegevens heeft verkregen. De eis tot waarborging van de privacy is mede reden om geen gebruik te maken van het SOFI-nummer voor zorgdoeleinden. Dit is ook niet nodig door het gebruik van de zorgchip.

Het gebruik van elektronische patiëntendossiers is niet alleen nuttig voor de directe zorgverlening, maar ook voor de ondersteunende processen. Het is mede de basis voor de planning van het zorgproces, voor de financiële afhandeling, voor onderzoek en voor management en beleid, doorgaans door gebruik te maken van geaggregeerde niet-identificerende gegevens.'[11]

Grosso modo is dit voorstel nog steeds waar het om draait. Er zijn wat veranderingen opgetreden: de voorgestelde biometrische chipkaart werd een zorgpas zonder biometrie, de zorgpas werd een patiënt-identificatienummer, het SOFI-nummer wordt wél gebruikt ter identificatie, en de eis om patiëntgegevens versleuteld te versturen is vervallen. De laatste paar jaar ligt het accent in de plannen - geheel in lijn met de politieke ontwikkeling - meer op de mogelijke kostenbesparingen en minder op de mogelijke kwaliteitsverbetering.

Doelstellingen

Over de doelen van het EPD bestaat in principe overeenstemming, maar het zijn er inmiddels wel heel veel geworden. Er kwamen bovendien steeds meer deelbelangen en nevendoelen bij. Een fatsoenlijk en betrouwbaar EPD kan immers niet bestaan zonder ook andere zaken te regelen en te automatiseren, en omgekeerd: als er nu toch grondig geautomatiseerd wordt, kunnen andere zaken ook meteen 'meegenomen' worden, meende men.

Naast het EMD (als eerste stap van het EPD) moet per 1 januari 2006 het elektronisch waarneemdossier (WDH) worden ingevoerd, zodat waarnemende huisartsen snel de gegevens van andermans patiënten kunnen raadplegen. Voorts moeten per 1

januari 2006 ook de declaraties volledig worden geautomatiseerd: alle rekeningen voor verrichtingen van behandelaars moeten vanaf die datum elektronisch bij de verzekeraars worden aangeleverd. [12] Ondertussen zijn er al registers van zorgverleners ingericht, en moet aan alle patiënten een uniek nummer worden toegekend om ze te kunnen identificeren. Ten slotte lijkt het EPD plotseling de wegbereider te moeten worden voor de invoering van een elektronische identiteitskaart voor alle burgers. Het volledige, landelijk dekkende EPD moet begin 2010 klaar zijn.

Om dat complexe, veelkoppige proces te stroomlijnen en te regisseren, werd in december 2001 het NICTIZ opgericht, het Nationaal ICT Instituut in de Zorg. Onder de auspiciën van het NICTIZ worden standaarden geformuleerd, pilots geïnventariseerd en begeleid, aanbevelingen geschreven, plannen ontworpen voor de technische infrastructuur, aanbestedingen gedaan, is er verschrikkelijk veel vergaderd en bergen nota's geproduceerd.

De doelstellingen van de hele operatie zijn grofweg de volgende:

- Centralisatie: zorgen dat de deelinformatie die her en der over een patiënt beschikbaar is, verzameld wordt en vanaf elke plek in Nederland, zo nodig door meerdere medici tegelijkertijd, toegankelijk is.
- Efficiëntie: papieren rompslomp vermijden (zoals het heen en weer sturen van verwijsbrieven, onderzoeksresultaten, deeldossiers, recepten en declaraties), en voorkomen dat onderzoeken dubbel worden uitgevoerd.
- Foutreductie: de kans verkleinen op een verkeerde diagnose of behandeling, door vast te leggen wat een patiënt mankeert of gebruikt (denk bijvoorbeeld aan het voorschrijven van medicijnen die elkaar bijten of waarvoor de patiënt allergisch is).
- Kwaliteitsverbetering: door diagnoses en behandelingen gestructureerd vast te leggen kan beter worden beoordeeld wat het effect is van een bepaalde behandelwijze. Daarnaast kan de informatie uit geaggregeerde (en geanonimiseerde) EPD'S nuttig zijn voor management, planning en budgetbewaking, en tevens voor wetenschappelijk onderzoek.
- Kostenbesparing (minder papierwerk, vermijden van doublures in onderzoek, minder 'medische missers' zoals medicatiefouten, eenvoudiger voorschrijven van gelijkwaardige maar goedkopere middelen, voorkomen van fraude, voorkomen dat patiënten gaan 'shoppen').

Kort gezegd: er wordt flink wat verwacht van het EPD.

Het is de vraag hoe realistisch die hooggespannen verwachtingen zijn. Natuurlijk kan het buitengewoon handig zijn als meerdere specialisten tegelijkertijd toegang hebben tot iemands volledige medische dossier, maar hoe vaak bestaat die behoefte werkelijk? Het is daarnaast de vraag of specialisten bij een nieuwe patiënt minder hoeven door te vragen over wat eraan schort als ze het dossier van zijn huisarts kunnen inzien: het blijft belangrijk zélf iemands anamnese af te nemen, al was het maar omdat de specialist zichzelf ervan moet vergewissen dat andere zorgverleners niets over het hoofd hebben gezien. Het navragen van iemands medische geschiedenis dient tevens altijd een ander doel, namelijk een idee ontwikkelen wie de patiënt is, hoe ernstig zijn problemen zijn, hoe hij met zijn symptomen omgaat, hoeveel eerlijkheid hij aankan of wil hebben.

Voorts zijn er een aantal vragen rond de medische praktijk die in de discussie over het EPD te weinig zijn gesteld. Is het altijd nodig iemands volledige dossier beschikbaar te hebben, of volstaan een aantal kernzaken? Zullen artsen inderdaad minder onderzoek aanvragen als ze de beschikking hebben over de resultaten uit eerder verricht onderzoek? Reduceren het EPD en EMD de kans op medische missers echt? Is bij die inschatting rekening gehouden met de wetenschap dat een geautomatiseerd dossier nieuwe soorten fouten in het leven roept? Hoe kwetsbaar is zo'n volledig geautomatiseerde infrastructuur, hoe gevoelig voor privacy-

inbreuken? Kun je een medisch dossier tegelijkertijd als verslagleggingsmethode, als meet- en planningsinstrument én als efficiencytoets gebruiken?

Mislukte centralisatie

Of het daadwerkelijk mogelijk is om alle medische informatie die over een patiënt bestaat aan elkaar te knopen, is uiteraard het eerste struikelblok. Hoe ga je knopen leggen, op welk niveau doe je dat, en welke problemen ondervind je daarbij in de dagelijkse praktijk?

Via een aantal pilots werd gezocht naar de beste aanpak. Centralisatie van het EPD was niet altijd een bijster goed idee, bleek al snel. Op zich klinkt het logisch en verstandig om patiëntendossiers op een centrale plaats beschikbaar te stellen. Dat is immers de enige aanpak die garandeert dat medici, waar in het land ze zich ook bevinden, daadwerkelijk bij ál iemands patiëntgegevens kunnen. Want hoe weet je in wiens bestanden, en dus wáár, je moet zoeken of er iets bekend is over een patiënt? Een uitgebreide proef met een centrale opzet mislukte echter jammerlijk.

Van mei 2001 tot mei 2002 werd in de regio Eemland (Amersfoort en omgeving), in samenwerking met verzekeraars, aanbieders en een landelijk patiëntenplatform, een grootschalige proef uitgevoerd. Men ging niet over één nacht ijs, de voorbereidingen waren al in juni 1998 begonnen. Er werd een zogeheten zorginformatienetwerk ontwikkeld, een 'neutrale en veilige infrastructuur gebaseerd op internettechnologie, waarmee computers en softwareprogramma's van alle zorgaanbieders en zorgverzekeraars onderling met elkaar kunnen worden verbonden. Binnen dit netwerk kan geautoriseerd informatie worden doorgegeven, onder meer met betrekking tot patiënten en declaratieverkeer. De verzekerden/patiënten ontvangen een zorgpas. Deze zorgpas geeft toegang tot de infrastructuur.' [13]

Er kwam een centrale server met daarop de verzekeringsgegevens van patiënten. Maar liefst 356.880 mensen kregen een met een chip uitgeruste zorgpas van hun verzekeraar, en bij 40 'proefpraktijken' van zorgaanbieders werden kaartlezers geïnstalleerd. Op hun eigen computer kregen deze zorgverleners een informatiesysteem waar de medische informatie in kon worden opgeslagen. Gaf je een zorgverlener je pas, dan kon hij die door zijn kaartlezer halen; op zijn eigen computer kon hij daarmee vervolgens je patiënt- en verzekeringsgegevens ophalen. Daarnaast werden informatiezuilen geïnstalleerd, zowel bij verzekeraars en zorgverleners, als in openbare ruimtes. Als je je kaart daarin stopte, kon je je eigen gegevens bekijken en gegevens toevoegen (bijvoorbeeld de adressen van mensen die in noodgevallen gewaarschuwd moesten worden), Aan de proef deden huisartsen, apothekers, ziekenhuizen, tandartsen, fysiotherapeuten en andere paramedici mee, die allemaal een computer met ISDN-lijn kregen om contact met de centrale server te kunnen maken.

De proef werd een faliekante mislukking. Twee grote verzekeraars meenden dat de beveiliging van het systeem niet voldoende was. [14] Verzekerden maakten amper gebruik van de optie om via de informatiezuilen hun eigen gegevens te bekijken; slechts 4% van de pasdragers deed dat. [15] Geheel onbegrijpelijk is dat niet. Achter zo'n zuil staand, in een publieke ruimte, lees je niet echt op je gemak je persoonlijke gegevens door.

De belangrijkste hindernis was echter dat de techniek erachter niet goed functioneerde. Bij het bijwerken van patiënteninformatie ontstonden geregeld fouten: zo overschreef de software soms bestaande gegevens van mensen met dezelfde geboortedatum. [16] De toegang tot de centrale server werkte evenmin naar behoren. Maar liefst tweederde van de deelnemende zorgverleners maakte melding van technische problemen met de infrastructuur: '...computerstoringen (foutmeldingen, geen verbindingsmogelijkheid, plotseling verbreken van de lijn), haperingen van de software […] en de traagheid van het systeem.'

28% van de zorgverleners maakte gewag van inhoudelijke fouten: ‘foutieve adressen, verschillende nummers voor dezelfde verzekerden.’ Ook belandden gegevens van verzekerden soms in de verkeerde velden. Erger was dat de informatie vaak niet actueel was: ‘De gegevens in de centrale unit [liepen] altijd minimaal een week achter.’ De geconstateerde problemen konden gedurende de proef slechts gedeeltelijk worden verholpen. [17]

De zorgverleners oordeelden na afloop overwegend negatief. Volgens een meerderheid zijn ‘de verwachtingen niet waargemaakt, is de praktijkadministratie niet beter op orde, is de samenwerking tussen zorgaanbieder en zorgverzekeraar niet bevorderd, is de factuurcontrole niet eenduidiger en beter geworden, en heeft het niet tot minder tijd voor de identificatie van verzekerden geleid. […] Bijna de helft vond dat de proef vooral veel tijd, geld en energie heeft gekost.’[18] De proef met de zorgpas kostte 15 miljoen euro, tweemaal zoveel als begroot, en eindigde als ‘niet meer dan een omslachtige manier om te controleren of iemand was verzekerd’. [19] Inmiddels hebben de verzekerden in Amersfoort weer gewone ziekenfondspasjes. De centrale unit staat er werkloos bij.

De conclusie die uit de zorgpasproef werd getrokken, was dat centralisatie niet werkt. Dat lijkt echter wat voorbarig. Dat déze opstelling niet werkte, wil nog niet zeggen dat centrale gegevensopslag per definitie de verkeerde weg is. Want ook aan decentrale gegevensopslag kleven problemen.

Google voor medici

Gelukkig verliepen niet alle proeven zo desastreus als die in Eemland. Hoe eenvoudiger de opzet ervan, hoe beter de testen gewoonlijk uitpakten; een mooie illustratie van het oude programmeursadagium KISS: *Keep it simple, stupid!*

Het Antoniusziekenhuis in Nieuwegein werkt al geruime tijd met een opstelling waarbij huisartsen online de dossiers van specialisten van het ziekenhuis kunnen raadplegen. Momenteel nemen elf huisartsenpraktijken en één gezondsheidscentrum in Nieuwegein en IJsselstein deel aan de proef; het gaat in totaal om ongeveer tienduizend patiënten. Na een proefperiode van drie jaar trad het systeem op 18 maart 2004 officieel in werking. [20] Het systeem heet UPID (Universele Patiënten Identificatie Database).

Het vernuft van dit systeem is dat er geen berichten tussen zorgverleners hoeven te worden uitgewisseld, noch is er een centraal EPD bedacht waarvoor alle zorgverleners hun informatie dienen aan te leveren. Het Nieuwegeinse EPD wordt op basis van ad-hoc inzage bij elke raadpleging ter plekke uit de voorhanden zijnde bronnen samengesteld. De software-ontwikkelaar ervan, Uzorg, spreekt om die reden van een *virtueel* patiëntendossier.

UPID werkt via internet. De deelnemende huisartsen kunnen via een beveiligde internetverbinding en met gebruikmaking van een pasje inloggen op het besloten netwerk van Uzorg en zich daar identificeren.

Op dat netwerk staat een centrale verwijsindex. UPID noemt deze index enigszins pompeus de ‘verkeerstoren’ van het systeem (het NICTIZ noemde hem eerder ook wel de ‘zorgmakelaar’). De huisarts vult het nummer van zijn patiënt in. De verwijsindex laat vervolgens zien waar in het Antonius informatie over de bewuste patiënt voorhanden is: bij polikliniek A of B, het laboratorium, de afdeling radiodiagnostiek. Zodra de zorgverlener specifieke informatie wil zien - labuitslagen, verwijs- en ontslagbrieven, röntgenfoto’s, diagnoses et cetera - maakt de verwijsindex contact met het lokale computersysteem van de specialist of het laboratorium en worden die gegevens van daaruit naar de browser van de huisarts gekopieerd. In de verwijsindex wordt voorts bijgehouden wie welke gegevens heeft opgeroepen, en wanneer. Huisartsen kunnen vooralsnog zelf geen informatie aan het systeem toevoegen.

Alle inhoudelijke informatie blijft derhalve lokaal en staat alleen bij de betreffende specialist in het systeem. De huisarts

raadpleegt de gegevens in real-time, wat garandeert dat hij altijd de meest recente versie krijgt. Deze opzet valt volgens het NICTIZ het best te beschouwen als 'een Google voor patiëntinformatie' [21] waarbij je in decentrale, lokale medische dossiers zoekt. Met één klik op een zoekresultaat haal je vervolgens de gevonden informatie bij een andere zorgverlener op en laad je die in je browser. Iemands patiëntgegevens staan dus niet fysiek op één plaats, maar worden vanaf allerlei locaties bijeengegaard en gecombineerd tot een volwaardig dossier; reden om van een 'virtueel EPD' te spreken.

Toegang van de patiënt zelf tot UPID is niet elektronisch geregeld en moet nog op de 'oude' manier totstandkomen: via een schriftelijke aanvraag. Wel kunnen patiënten bij een informatielijn navragen wie hun gegevens hebben ingezien. [22]

Het UPID wordt in de toekomst aangepast om ook andere zorgverleners, zoals apotheken en fysiotherapeuten, toegang tot het systeem te verlenen. Zij hebben daartoe, net als de huisarts nu, toestemming van de patiënt nodig. En waar UPID momenteel feitelijk eenrichtingsverkeer levert (de huisarts kan wel patiëntgegevens bij het ziekenhuis inzien, maar de specialist niet bij de huisarts) is het uiteindelijk de bedoeling dat het systeem multi-directioneel wordt. Alle daartoe bevoegde zorgverleners in de regio kunnen dan elkaars actuele gegevens over een specifieke patiënt raadplegen. Zodra dat kan, is er feitelijk sprake van een regionaal dekkend EPD.

Schaalbaarheid, monopolies en beheer

In meerdere regio's zijn inmiddels UPID-achtige systemen opgezet. Uiteindelijk moet dit model landelijk worden toegepast, waarbij een Landelijk Schakelpunt (LSP) uiteindelijk de rol van de regionale verwijsindexen of verkeerstorens zal overnemen. Dat zal niet meevallen. NICTIZ-directeur Van Boven: 'Verschillende regionale zorgnetwerken ontwikkelen zich zo snel dat je het gevaar loopt dat er over een jaar zes verkeerstorens zijn. […] Het vergt nogal wat moeite om de medische informatie uit de regio via [het LSP] landelijk beschikbaar te krijgen.'[23]

Niettemin moet het complete LSP in een paar maanden totstandkomen. Het NICTIZ maakt pas in september 2005 bekend wie het systeem mag gaan bouwen, terwijl het LSP al op 1 januari 2006 operationeel moet zijn.

De voornaamste technische vraag - ook voor de huidige semi-regionale indexen - zal zijn of de verwijsindex goed schaalbaar is. De UPID-index bevat alleen verwijzingen naar locaties binnen het ziekenhuis waar medische informatie over patiënten ligt opgeslagen. Als het systeem multi-directioneel wordt, moet de index duizenden locaties bijhouden, elk met hun eigen patiëntverwijzingen. Ook het aantal uitvragingen - waarbij aan de hand van de centrale verwijsindex links en rechts gegevens uit allerlei lokale computers bijeengesprokkeld worden - zal navenant stijgen.

Meer politiek getinte vragen zijn die naar het beheer, de kwetsbaarheid en het regionale monopolie van het systeem. Alle medische gegevens staan lokaal; de verwijsindex staat echter op een server van Uzorg, de commerciële software-ontwikkelaar van UPID. Dat betekent feitelijk dat het mechanisme dat de deeldossiers tot een volwaardig EPD combineert, de verkeerstoren, de spin in het web, buiten het domein valt waarin het wordt gebruikt en van waaruit het wordt gegenereerd. De zorg beheert haar eigen gegevens, de index erop wordt beheerd door een derde partij. Hoe verstandig is het om een dergelijke, zowel inhoudelijk als organisatorisch steeds vitaler wordende index in handen van een commerciële partij te geven?

Wat als een huisartsenpraktijk of de gezamenlijke regionale vroedvrouwen liever een ander systeem aanschaffen dan UPID? Kan hún toegang tot de andere elektronische gegevens van hun patiënten dan gegarandeerd worden? En omgekeerd: hoe haalt een specialist gegevens van zijn patiënten bij die regionale vroedvrouwen op als die vroedvrouwen niet in de regionale UPID-

verwijsindex staan? Is het verstandig dat een uitbater van een softwaresysteem een regionaal monopolie heeft en tegelijkertijd een zo centrale rol in de medische informatievoorziening speelt?

In een onderzoek naar de invoeringsperikelen rond het EMD dat Ernst & Young kortgeleden afsloot, komt dezelfde vraag naar voren. Tweederde van de huisartsen, driekwart van de specialisten en bijna de helft van de apothekers die bij het onderzoek waren betrokken, waren niet aangesloten bij een regionaal zorgnetwerk (of konden niet vertellen of ze dat waren). [24] Dat betekent dat de overgrote meerderheid van zorgverleners niet op korte termijn op regionale ICT-infrastructuren (zoals UPID) kan worden aangesloten. Nico Huizing, een van de opstellers van het onderzoek, waarschuwt dat het ministerie moet zorgen dat zorgverleners eerst in een regionaal zorgnetwerk terecht komen, want 'Het is voor een zorgverlener technisch complex en financieel onaantrekkelijk om zich zelfstandig aan te sluiten op de landelijke infrastructuur.'[25]

De decentrale aanpak heeft andere nadelen. Het is prettig dat iedereen verantwoordelijk blijft voor zijn 'eigen' informatie en die niet steeds van elders hoeft te halen; dat voorkomt hinderlijke vertragingen zoals zich eerder in Eemland voordeden. Het nadeel ervan is dat overal in de regio lokale databases met patiënten(deel)dossiers komen te staan. Al die databases, samen met de computers en netwerken waarop ze staan, vergen beheer, onderhoud en beveiliging, terwijl niet iedereen die kennis in huis heeft. Grotere instanties, zoals ziekenhuizen, kunnen kennis en menskracht inhuren ten behoeve van hun systeembeheer en netwerkbeveiliging. Hoe een kleine huisartsenpraktijk dat moet gaan regelen, is onduidelijk.

Maar ook grotere systemen kunnen soms uit de lucht zijn, zoals de virusaffaire bij het Spaarne bewees. Hoe betrouwbaar is de verwijsindex als aangesloten lokale systemen tijdelijk uit de lucht zijn, hetzij door een computerprobleem, hetzij door een falende internetverbinding? Hoe wéét je als zoekende arts dat de informatie die de verwijsindex je voorschotelt niet volledig is, hetzij omdat elders een computer buiten werking is, hetzij doordat een andere zorginstantie (nog) niet is aangesloten bij de verwijsindex?

Voorts is de vergelijking met Google die het NICTIZ maakt prachtig, maar niet steekhoudend. Google werkt immers juist zo snel en degelijk omdat de zoekmachine zelf kopieën maakt van alle bezochte en geïndexeerde pagina's - oftewel: omdat Google alle informatie centraal opslaat en vervolgens uit haar cache kan leveren. Die aanpak betekent tevens dat als een database elders plat ligt, Google altijd de laatst geïndexeerde versie kan voorschotelen. Je hebt dan weliswaar niet de garantie dat dat inderdaad de meest actuele informatie is, maar je hebt in elk geval íets.

Tussen regie en commercie

Het NICTIZ, dat de invoering van de elektronische dossiers moet coördineren en dat daartoe een aantal standaarden, richtlijnen en structuren heeft vastgelegd, stelt zulke vragen jammer genoeg niet. Tenminste: niet publiekelijk.

Sowieso is de opstelling van het NICTIZ nogal optimistisch. Alles gaat goed, ICT helpt, geen wolkje aan de lucht. Zo heeft de organisatie eind 2004 een zogenaamd 'versnellingsprogramma' afgerond waarbij vijf regio's extra ondersteuning kregen voor de ontwikkeling van hun EMD. De opzet en resultaten daarvan worden - net zoals die van andere pilots en proefprogramma's - slechts beschreven in zeer algemene termen, die eerder op een programma van uitgangspunten lijken dan op een kritische beschouwing. Volwaardige evaluaties zijn helaas niet via het NICTIZ te vinden. Het instituut houdt het op enigszins dooddoenerige mededelingen als 'Verandering moet vanuit de zorg gedragen worden', 'Evenwichtige belangenbehartiging is noodzakelijk' en 'Vertrouwen is de basis'. [26]

Ter verdediging van het NICTIZ moet worden opgemerkt dat evaluaties over pilots lospeuteren soms ook moeilijk is. Alle pilots worden in samenwerkingsverbanden tussen zorgverlenende

instanties en commerciële partijen (softwarehuizen, en vaak ook zorgverzekaraars) uitgevoerd, en die laatsten zijn - uit eigenbelang - weinig scheutig met informatie. De concurrentie kan daar immers baat bij hebben. De luttele evaluaties die openbaar zijn, komen van universiteiten die na afloop het reilen en zeilen van een proef hebben bestudeerd.

Maar het blijft vreemd dat, omwille van de concurrentiepositie van software-ontwikkelaars, allerlei mogelijk cruciale informatie over fouten, hindernissen en valkuilen in de ontwikkeling van het EPD binnenskamers blijft. Dat steekt des te meer aangezien juist dit soort informatie het publieke en politieke debat over het EPD zou kunnen voeden. Daarnaast blijkt uit het wedervaren op andere terreinen waar wordt geautomatiseerd, dat het nuttig is publiekelijk te kunnen vertellen welke problemen en 'bugs' er zijn: dat helpt om fouten en hebbelijkheden te identificeren, en dus eerder op te lossen.

Er is niet niks…

Het EPD hoeft niet van de grond af te worden opgebouwd. Er is inmiddels al veel patiënteninformatie langs geautomatiseerde weg beschikbaar. De oude groene kaart waarop artsen hun aantekeningen maakten, is grotendeels verdwenen en vervangen door een computerversie. Apotheken houden vrijwel allemaal digitaal bij welke medicijnen ze aan patiënten hebben geleverd.

Wat de uitwisseling van de her en der aanwezige elektronische informatie lastig maakt, is dat allerlei instanties met hun eigen informatiesysteem werken: ziekenhuis-informatiesystemen (ZIS), huisarts-informatiesystemen (HIS) en (ziekenhuis)apotheek-informatiesystemen (AIS / ZAIS). Zowel huisartsen als specialisten gebruiken daarnaast soms een aparte module voor het selecteren en uitschrijven van medicijnen, een elektronisch voorschrijfsysteem (EVS).

Niet alleen heeft zowat elke medische beroepsgroep een eigen systeem, ook daarbinnen is weer de nodige variatie. [27] Veel pakketten zijn in modules opgebouwd. Ziekenhuizen gebruiken steeds vaker de medische module van leverancier A en de declaratiemodule van leverancier B. Binnen de ziekenhuizen hebben de verschillende afdelingen, maatschappen en poliklinieken vaak onderling afwijkende (en op hun behoeften aangepaste) systemen. De oudere (deel)systemen zijn voorts globaal genomen meer gericht op het bijhouden en bewerken van informatie dan op het delen ervan met anderen, en functioneren daardoor min of meer als eilandjes. De nieuwere systemen, die met modules werken, kunnen doorgaans wel redelijk goed met elkaar communiceren.

Maar informatie uitwisselen tussen al die verschillende en oude(re) systemen kan wel degelijk. Net zoals iemand die het tekstverwerkingsprogramma Word gebruikt uitstekend een tekst kan inlezen, bewerken en opslaan die geschreven is met OpenOffice, WordPerfect of LaTex en vice versa, kunnen de verschillende medische systemen in principe met elkaars inhoud overweg. Anders dan tekstverwerkers doen medische informatiesystemen dat echter niet door gegevens op dezelfde manier te organiseren, maar door elkaar onderling berichten te sturen. Elk HIS, ZIS en AIS kan zulke berichten 'verstaan'.

Het berichtensysteem dat daarvoor wordt gebruikt, heet Edifact. Met een Edifact-bericht kunnen recepten elektronisch worden verstuurd, diagnoses worden doorgegeven, onderzoeksresultaten worden vastgelegd et cetera. In Nederland worden in de zorg jaarlijks ettelijke miljoenen van dergelijke berichten heen en weer gestuurd. Een saillant detail is dat Edifact van ver voor het internettijdperk stamt en dus eigenlijk een stokoude technologie is.

Als een HIS of ZIS goed Edifact 'spreekt', kunnen ontvangers de berichten laten vertalen naar een aanvulling op hun eigen informatie en in hun HIS of ZIS importeren. Een groot verschil met een volledig werkend EPD is dat Edifact altijd menselijke tussenkomst vergt: derden kunnen patiënteninformatie niet

zelfstandig raadplegen en moeten wachten tot de zorgverlener in kwestie een Edifact-bericht terugstuurt.

De gedachte dat je iets volstrekt nieuws moet ontwikkelen om elkaars patiënteninformatie te kunnen inzien, overdragen en uitwisselen, is echter onterecht. Vanuit de meeste HISsen en ZISsen kun je elektronisch recepten naar apotheken sturen en aan het eind van de maand alle declaraties volautomatisch laten printen (of ze elektronisch naar de zorgverzekeraars versturen). Veel van de informatie die uiteindelijk in een landelijk dekkend EMD en EPD moet worden opgenomen, is daarom in feite al voorhanden. Indien bestaande gegevensbronnen fatsoenlijk met elkaar leren praten, zijn we al een heel eind op streek.

> 'Voor het meest prangende probleem - het tot stand brengen van een totaal medicatieoverzicht voor de verschillende betrokken behandelaars rondom de patiënt - is geavanceerde ICT functionaliteit helemaal niet nodig. De belangrijkste, eerste stap is het 'aan elkaar knopen' van de verschillende gegevensbronnen omtrent patiëntenmedicatie in de regio. Dat hoeft geen 'hi-tech' oplossing te zijn, noch een fysiek medicatiedossier te omvatten: met behulp van bestaande software en op basis van de vaak al bestaande zorgnetwerken kunnen EDIFACT queries [informatieverzoeken, KS] vanuit een behandelaar naar de regionale apotheken, huisartsen en ziekenhuis worden gestuurd en beantwoord. In veel gevallen is informatie al gecentraliseerd aanwezig - in huisartsenposten, bijvoorbeeld, of in samenwerkingsverbanden van regionale apothekers. Zelfs assortimentslijsten en formularia hoeven niet op elkaar te zijn afgestemd […]. Natuurlijk, daarmee komen relatief rommelige lijstjes tot stand - maar de behandelend arts en de distribuerende apotheker beschikken tenminste over de informatie op basis waarvan zij hun patiënten zorg kunnen leveren. Ook zal dit niet meteen leiden tot volledig complete overzichten, omdat er altijd medicamenten van buiten de regio kunnen zijn, of zelfs vanuit het buitenland [i.e. medicijnen die mensen zelf elders bestellen - KS].
>
> Ook hier is 'best' de vijand van 'beter'. Deze eerste stap levert erg veel winst op. Verdere stappen worden snel exponentieel complexer qua uitvoering, terwijl de extra winst ervan snel afneemt. Zelfs een nationale database zal nooit compleet zijn - medicatie kan uit het buitenland komen, of apotheken en behandelaars kunnen niet aangesloten zijn of informatie niet doorgeven.'[28]

Evenmin hoeven we toe naar één softwarepakket voor alle EMD'S en EPD's. Dat zou ook zonde zijn: artsen en ziekenhuizen hebben, net als de leveranciers, veel geld gestoken in de ontwikkeling van hun huidige systemen. Bestaande systemen plompverloren afschaffen zou neerkomen op een vernietiging van kapitaal, tijd en moeite. Bovendien kost het organisatorisch nogal wat om nieuwe informatiesystemen in te voeren, iedereen er vertrouwd mee te maken en te bezien hoe ze in de praktijk werken.

De illusie van het gemeenschappelijk datamodel

Waar de RVZ en het NICTIZ op aandringen, is niet zozeer dat de diverse modules voor het medische dossier van al die leveranciers in de toekomst dezelfde (open) standaard voor hun berichtenverkeer gebruiken (want dat doen ze meestal al), maar veeleer dat iedereen gaandeweg eenzelfde (open) datastructuur gebruikt. Met zo'n gemeenschappelijk gegevensmodel kunnen alle verschillende systemen écht effectief met elkaar praten, meent men.

Wanneer medische systemen van elkaar weten welke patiëntgegevens waar gestandaardiseerd te vinden zijn en wat de onderlinge relaties tussen al die stukjes data is (betekent die 3 onder het hoofdstukje 'bloed - cholesterol' nu het aantal millimol cholesterol in iemands bloed, of het aantal bloedafnames waarover die gemiddelde waarde is bepaald?), is de rest eigenlijk een peulenschil. 'Wanneer dit [gemeenschappelijk data]model algemeen geldend is voor de gezondheidszorg, dan is het in

principe een kwestie van autoriseren wie voor welk doel welke gegevens nodig heeft,' schrijft de RVZ in een recent advies aan de minister. [29]

Het voordeel van zo'n gemeenschappelijk datamodel is dat je vermijdt dat je voor elk type raadpleging en informatielevering, die nu gewoonlijk via een vooraf gedefinieerd e-mailbericht wordt afgehandeld, een aparte berichtstandaard moet ontwikkelen. Aangezien er nogal wat typen van raadpleging en toevoeging zijn, zit je voor je het weet met tientallen mailstandaarden. Heb je daarentegen een gemeenschappelijke datastructuur, dan kan iedereen die medische informatie wil inzien of toevoegen - na een vastgestelde procedure van identificatie, authenticatie en autorisatie te hebben doorlopen - die gegevens simpelweg rechtstreeks zelf 'halen' of 'brengen'. Je kunt andermans systeem dan raadplegen als was het je eigen systeem.

De RVZ raadt de minister aan te eisen dat alle medische informatiesystemen die na 1 januari 2006 in gebruik worden genomen, met dat gemeenschappelijke model werken. Bestaande systemen kunnen dan ondertussen langzaam aangepast worden, met januari 2010 als uiterste datum waarop ook zij datzelfde gegevensmodel moeten implementeren. Hoogervorst zelf is terughoudender, hij ziet in 2006 slechts de eerste ontwerpen in het verschiet liggen: 'Het streven is eind dit jaar [2005] dergelijke standaarden gereed te hebben, opdat hier begin volgend jaar systeemontwerpen mee gemaakt kunnen worden.'[30]

Het is leuk en aardig om over de invoeringsdatum van gemeenschappelijke datamodellen te spreken, maar die exercitie bekijk je toch met andere ogen wanneer je beseft dat zorgverleners het overgrote deel van hun aantekeningen over hun patiënten nog steeds in de vorm van vrije tekst vastleggen, ook als ze allang met een HIS of ZIS werken. Uit een eerder citaat uit een nota uit 1996 blijkt dat de RVZ dat probleem toen al onderkende. Bijna tien jaar later, in maart 2005, is er met betrekking tot die vrije tekst nog niet veel veranderd, blijkens een opmerking van minister Hoogervorst in zijn plan van aanpak: 'Zorgverleners moeten worden ondersteund bij een gestructureerde verslaglegging met gebruik van eenduidige classificaties (codestelsel), waar er nu verslaglegging plaatsvindt in de vorm van "verhalend proza".'[31] Artsen die wél met zo'n codestelsel werken, zijn daar meestal niet over te spreken: in sterk gestructureerde EPD's kunnen ze minder informatie en nuances kwijt dan ze noodzakelijk vinden.

De constatering dat van een medisch gegevensmodel nog absoluut geen sprake is, laat staan van een gemeenschappelijk gegevensmodel, maakt het streven van de RVZ en het NICTIZ tot een mooi, maar naïef plan. Een gemeenschappelijk medisch datamodel is bovendien een heilige graal waarnaar al een eeuw wordt gezocht, en die na verloop van tijd telkens weer als onmogelijk en onhaalbaar wordt verworpen. Zo is in de Verenigde Staten van 1986 tot 1996 gewerkt aan een dergelijk datamodel, het Unified Medical Language System (UMLS), teneinde medische kennis 'in de computer' te kunnen stoppen. Het was het grootste project op dit terrein ooit; na tien jaar gaf men het op. Het streven is nu om een complete medische thesaurus te maken, maar ook dat project loopt nu al tien jaar. [32]

De onmogelijkheid van een gemeenschappelijk datamodel blijkt ook uit de recente historie rond de DBC's, de diagnose-behandelcombinaties. DBC's zijn per 1 januari 2005 verplicht ingevoerd om beter zicht te krijgen op de kosten en honorering van behandelingen, en worden gebruikt voor declaraties bij de zorgverzekeraars. Daarnaast zouden de DBC's vraagsturing in de zorg moeten bevorderen. De DBC's werken met codes, voor elke behandelcombinatie één. In korte tijd zijn er al 33.000 verschillende DBC's ontwikkeld. Artsen klagen en masse dat ze door de bomen het bos niet meer zien, struikelen over fouten in de software en stuiten op problemen omdat het systeem niet flexibel is: ze kunnen hun werkelijke verrichtingen er vaak niet in kwijt. [33]

…maar er moet ineens een heleboel

Of je nu gemeenschappelijke gegevensmodellen nastreeft of niet: er moeten buitengewoon veel randvoorwaarden worden gedefinieerd en er dient een complete infrastructuur te worden opgezet voordat het EMD en EPD op betrouwbare wijze kunnen functioneren. Buiten cruciale kwesties als identificatie en autorisatie zijn standaarden en terminologie de meest in het oog springende kwesties.

Standaarden

Voor het vastleggen van patiëntgegevens in het EPD is na veel vijven en zessen gekozen voor de internationaal geaccepteerde standaard HL7 V3 NIM; voor het uitwisselen van medische gegevens (het oude Edifact) voor de HL7 standaard. In die standaarden is precies beschreven hoe informatie moet worden vastgelegd en in welke relatie al die stukjes data tot elkaar staan.

Lang niet alle bestaande systemen gebruiken die HL7-standaarden; die moeten dus eigenlijk worden omgebouwd wil het EPD echt landelijk kunnen functioneren. Intussen is besloten dat bestaande systemen langzaam mogen worden uitgefaseerd en dat alleen nieuwe systemen verplicht uitgaan van de HL7-standaarden. Maar zelfs niet alle lopende proeven en pilots met het EPD zijn gebaseerd op die nieuwe standaard. Om de verwarring nog groter te maken: recent is een (concept) Europese standaard afgesproken, de NEN-EN 13606. Hoewel de norm nog niet helemaal klaar is, wordt nu al gezegd dat dit de nieuwe standaard gaat worden en HL7 dus zal vervangen. Tegelijkertijd is volstrekt onduidelijk of HL7 en NEN-EN 13606 elkaar aanvullen of uitsluiten. [34] Voor softwareontwikkelaars is derhalve niet duidelijk welke standaard gebruikt gaat worden.

Er moet kortom nog veel werk verzet worden willen al die verschillende systemen vanzelfsprekend met elkaars gegevens overweg kunnen en medici elkaars dossiers eenvoudig elektronisch kunnen inzien.

Terminologie

Je moet niet alleen de structuur van gegevens standaardiseren, maar ook de taal ervan, vinden sommige instanties. Zij menen dat voor symptomen, diagnoses, behandelingen en dergelijke een eensluidend vocabulaire moet worden ontwikkeld, zodat er geen verwarring kan ontstaan over de interpretatie van die gegevens. Er bestaan weliswaar codes voor diagnoses en verrichtingen (denk aan de DBC's), maar die volstaan lang niet altijd wanneer het gaat om het vastleggen van de dagelijkse praktijk binnen het zorgproces. Het NICTIZ, sowieso groot voorstander van door hen te implementeren standaarden, tracht daartoe een standaard voor 'zorgbrede terminologie' te ontwikkelen. Het gaat daarbij volgens het NICTIZ om termen voor het hele scala van 'klachten, symptomen, omstandigheden, ziekteprocessen, interventies, diagnoses, resultaten, en de besluitvorming.' [35]

Ga er maar aanstaan, aan een dergelijke codificatie van 'medische momenten'. In Amerika zijn ze daar, via het eerder genoemde UMLS, al tien jaar mee bezig, zonder veel resultaat. Alleen al over het opstellen van farmaceutische formularia (lijsten met medicijnen die kunnen worden voorgeschreven), zitten overal in het land instanties te vergaderen. Gestandaardiseerde termen aan een proces koppelen is nog onnoemelijk veel complexer. De vraag is daarnaast hoe zinnig zo'n onderneming is, gezien de ellende met de DBC's en de grote aarzeling die huisartsen en specialisten nu al hebben om hun vrije tekst los te laten in ruil voor een meer gecodeerde taal.

Je kunt je in gemoede afvragen of het NICTIZ hier niet onmogelijk, ja zelfs contraproductief ambitieus is. Immers, hoe omvattender de eisen die aan een EMD of EPD worden gesteld, hoe kleiner de kans is dat ze ooit ingelost zullen worden. Hoogleraar sociaal-medische wetenschappen Marc Berg, wiens specialisatie ICT

in de zorg is, haalt in dat verband een oude regel uit de informatica aan: *too much ambition kills*. Met een eenvoudige doelstelling behaal je veel succes. Verfijningen en toevoegingen kosten buitenproportioneel veel werk en leveren uiteindelijk weinig op.

Bergs waarschuwing wordt ondersteund door uitvoerig onderzoek van de Standish Group, die aantoonde dat van alle IT-projecten slechts 16% slaagt en 31% volledig mislukt. De resterende 51% is over tijd, te duur of incompleet; [36] gemiddeld bleken ze maar liefst 2,7 maal zoveel geld en 3,3 maal zoveel tijd te kosten als begroot, en slechts 40% van de beoogde functionaliteit te leveren. [37]

De wens van het NICTIZ om het EPD met steeds meer functionaliteiten toe te rusten - van gemeenschappelijk datamodel tot gestandaardiseerde terminologie - vormt derhalve zélf vermoedelijk een obstakel voor het welslagen van het project.

Identificatie en autorisatie van zorgverleners

Cruciaal voor het EPD en EMD is het regelen van identificatie en autorisatie. Je moet bepalen welke mensen zulke systemen mogen inzien, wie er gegevens mogen invoeren, toevoegen, wijzigen en/of berichten aan andere zorgverleners mogen versturen.

Inmiddels is een lijst opgesteld van beroepsgroepen die in aanmerking komen om op enigerlei wijze toegang te krijgen tot het EPD: het zogeheten UZI-register. [38] Zorgverleners kunnen zich sinds 1 januari 2005 laten registreren om hun unieke zorgverlenersidentificatie (UZI-nummer) toegewezen te krijgen. Zorginstellingen zullen op termijn kaartlezers aan hun computers moeten koppelen, en elke zorgverlener dient tegen die tijd over een met een pincode beschermde UZI-pas te beschikken om met EPD's te mogen werken.

In het UZI-register worden iemands bevoegdheden vastgelegd. Bij elke raadpleging of mutatie van het EMD of EPD zal de software eerst bij de centrale servers van het landelijke UZI-register controleren of de betreffende zorgverlener daartoe bevoegd is. Aan zorgverleners kan zo, afhankelijk van hun rol en functie in het zorgproces, op verschillende niveaus toegang worden verleend tot elektronische patiënten- en medicatiedossiers. Een waarnemend huisarts of een laborant zal daarbij een lager toegangsniveau krijgen (en minder gegevens te zien krijgen) dan een specialist of huisarts. Wanneer een andere zorgverlener dan de eigen huisarts of specialist iemands patiëntgegevens wil inzien, zal hij - net als nu het geval is - altijd toestemming moeten krijgen van de bewuste patiënt. Van die toestemming wordt een aantekening gemaakt in het UZI-register, en pas nadat die toestemming is verwerkt, krijgt de desbetreffende zorgverlener daadwerkelijk toegang tot dat specifieke EPD. [39]

Verder zal bij alle raadplegingen of mutaties van elk EPD worden vastgelegd met welke UZI-pas dat is gebeurd. Op die manier is altijd te achterhalen wie welke dossiers wanneer heeft ingezien of bijgewerkt. Het is de bedoeling dat patiënten kunnen opvragen welke zorgverleners hun dossiers hebben bekeken of er informatie aan hebben toegevoegd.

Met de UZI-pas en pincode kunnen zorgverleners zich te zijner tijd digitaal identificeren, een digitale handtekening zetten (voor het elektronisch uitschrijven van recepten aan patiënten en het elektronisch indienen van declaraties bij verzekeraars), e-mails met patiëntgegevens desgewenst versleutelen, en toegang krijgen tot beveiligde websites (bijvoorbeeld sites van beroepsbeoefenaars). Ten slotte wordt er gewerkt aan automatische encryptie van te verzenden patiëntgegevens op basis van de UZI-pas, [40] momenteel nog op vrijwillige basis.

Voorlopig wordt de toegang tot het EPD geregeld met een gebruikersnaam en een wachtwoord. Pas als overal in het land kaartlezers staan en iedereen zijn pas heeft, kan de UZI-pas met pincode daarvoor gebruikt worden. [41] In de toekomst overweegt het UZI-register een biometrische UZI-pas in te voeren. Op de pas komt dan een chip met daarin gegevens over je vingerafdruk, en bij

de computer hoort een apparaatje waarop je je vinger legt. Deze methode moet voorkomen dat een ander met de pas en de code op de loop gaat en zich vervolgens kan voordoen als geautoriseerd gebruiker. Maar, zoals het UZI-register waarschuwt: 'De huidige stand van de techniek (biometrie geeft op dit moment nog te veel fouten, zowel in de vorm van onterechte herkenning als in de vorm van onterechte afwijzing) en de hogere kosten maken toepassing van (fingerprint)biometrie op korte termijn niet wenselijk.'[42]

De opzet is solide, de praktijk roept niettemin vragen op. Voorlopig volstaan een gebruikersnaam met bijbehorend wachtwoord om zorgverleners toegang te geven tot de dossiers van hun eigen en andermans patiënten. Wie op een willekeurige werkplek rondloopt, weet dat gebruikers vaak geeltjes met hun wachtwoord op hun monitor plakken of papiertjes met hun inlog-gegevens in hun bureaula bewaren. Het kost meestal weinig moeite om zulke informatie te achterhalen. Wie andermans gegevens weet te bemachtigen, heeft in één klap toegang tot (en mogelijk zelfs kopieer- en mutatierechten op) alle patiëntengegevens van de betreffende zorgverlener; dat kan oplopen tot duizenden dossiers. Dat in overweging nemend is een biometrische UZI-pas zeker te prefereren boven een simpele bescherming met een wachtwoord.

In ziekenhuizen - bijvoorbeeld op de drukke en hectische eerstehulp-afdelingen - kom je een ander verschijnsel tegen: iemand logt netjes in, maar niet uit en vervolgens werkt iedereen die iets moet opzoeken of invoeren op basis van die inloggegevens. Computers staan daar vaak de hele dag 'open', zodat iedereen meteen aan de slag kan en niet telkens de soms omslachtige inlogprocedure hoeft te doorlopen. In de praktijk fungeert één enkel account daarmee als account voor de hele afdeling. Bij een dergelijke werkwijze wordt het bijhouden van mutatie- en inzagegegevens echter betekenisloos.

In sommige EPD-pilots trachtte men dit probleem te ondervangen door gebruikers na een bepaalde tijd automatisch uit te loggen. Dat zorgt echter weer voor veel irritatie bij de (legitieme) gebruiker, die soms terwijl hij gewoon bezig was uit het systeem gegooid wordt of die - ook al is hij de enige die met de betreffende computer werkt - door de software gedwongen wordt steeds opnieuw in te loggen als hij de muis of het toetsenbord een kwartier niet heeft aangeraakt, bijvoorbeeld omdat hij met de patiënt zelf bezig was.

Niet alle ziekenhuizen zijn gelukkig met de UZI-passen, die nogal wat administratieve rompslomp met zich meebrengen. Er zijn inventievere plannen. Het Spaarne overweegt met RFID's te gaan werken: een kleine herkenningschip die in een polsbandje wordt verwerkt. Zodra de drager met zijn hand bij de computer komt, wordt hij automatisch op het juiste account ingelogd.

Je kunt beveiligen tot je een ons weegt, maar ongeacht de oplossing die je kiest: de gebruiker is altijd de zwakste schakel. Als iemand slordig is met zijn gegevens (wachtwoord, pasje of polsband), is het hele autorisatiesysteem achter het EPD zinloos. Anderzijds wil je de niet dat de autorisatie zelf een bron van ergernis vormt en zodoende de bereidheid ondermijnt om met het EPD te werken. De diverse pakketten zullen steeds, ook qua autorisatie, goed moeten aansluiten bij de omgeving waarin ze gebruikt worden. Maar bovenal zullen artsen en specialisten zich er terdege rekenschap van moeten geven dat hun vertrouwensfunctie zich voortaan ook uitstrekt tot het secuur bewaken van hun eigen inloggegevens. Slordigheid daarmee tast immers de privacy van grote groepen mensen aan op een bijzonder intiem gebied: hun gezondheid.

Identificatie van patiënten

In 1996 besefte minister Borst al dat een eenduidige identificatie van patiënten onontbeerlijk was als we een landelijk dekkend EPD wilden invoeren. Borst was, in navolging van de Raad voor de Volksgezondheid en Zorg, bijzonder duidelijk over het gebruik van het SOFI-nummer voor een dergelijke identificatie: 'Deze nummers

zijn daar niet voor bedoeld.' Gebruik maken van het SOFI-nummer zou te makkelijk leiden tot ongewenste koppeling van allerlei soorten informatie, meenden Borst en de RVZ. [43] Alleen waar inkomensafhankelijke kwesties in de zorg speelden, zoals de vaststelling van eigen bijdragen in de thuiszorg en de administratie van het ziekenfonds, mocht het SOFI-nummer worden gebruikt.

Borst dacht aanvankelijk aan een zorgpas (mogelijk een smartcard), en overwoog later een speciaal te ontwerpen zorgidentificatienummer (ZIN) voor gebruikers in te voeren. Die kaart of dat nummer zou voortaan door alle relevante zorginstanties moeten worden gebruikt. De zorgpasproef in Eemland mislukte echter jammerlijk. Tot eind 2002, onder het ministerschap van Borst, ging VWS uit van een nieuw te ontwerpen ZIN voor iedereen.

In juni 2002 verscheen een advies van de voormalig minister van Binnenlandse Zaken Ed van Thijn over het persoonsnummer, in de wandeling *Advies van de Tafel van Thijn* geheten. [44] Het advies was tot stand gekomen in nauw overleg met topambtenaren van alle ministeries. Al een paar maanden later, in november 2002, noemde de regering van CDA, VVD en LPF het advies 'een doorbraak op het gebied van de gegevenshuishouding van de overheid'. [45] Het kabinet kondigde op grond van Van Thijns advies de invoering van het burgerservicenummer (BSN) aan: een uniek nummer voor elke burger dat voortaan in al het verkeer tussen overheid en burger gebruikt zal worden.

> 'Een moderne overheid die klantgericht met haar burgers omgaat, vermijdt dat de burger in zijn relatie met de overheid voor elke sector of overheidsorganisatie een afzonderlijk nummer moet gebruiken. Dit leidt tot verwarring en irritatie en komt de beeldvorming van een efficiënte en ontkokerde overheid niet ten goede. Het is daarom gewenst dat de burger voor al zijn contacten met de overheid met één persoonsnummer toe kan.
>
> Tevens is het met het oog op een meer klantgerichte, geïntegreerde dienstverlening en een reductie van de administratieve lasten gewenst dat de koppeling van gegevens tussen de overheden op basis van persoonsnummers kan plaatsvinden, mits hiervoor een wettelijke basis is. […]
>
> De inrichting van een overheidsbreed persoonsnummerbeheer is van belang om invulling te geven aan de wens naar betere mogelijkheden voor gegevenskoppeling ten behoeve van de rechtshandhaving en opsporing. Daarbij wordt gedacht aan een verruiming van de wettelijke mogelijkheden binnen de geldende Europese privacy richtlijnen.' [46]

In 2004 sloot minister Hoogervorst zich definitief bij dit plan aan: het BSN wordt voortaan ook in de zorg gebruikt.

> 'Het gebruik van het BSN in de zorg levert namelijk een aantal voordelen op ten opzichte van een apart [zorg]nummer, te weten: de burger wordt niet opgezadeld met meerdere nummers, er hoeven niet twee nummerfabrieken opgetuigd te worden en er hoeft - ten behoeve van intersectoraal verkeer - geen omnummerfabriek BSN-ZIN gebouwd te worden.' [47]

Vanaf 1 januari 2006 zal het BSN in verschillende domeinen worden gevoerd: in de sociale zekerheids- en belastingsector als het vertrouwde SOFI-nummer, in de zorg als zorgidentificatienummer (ZIN) en in het onderwijs als onderwijsnummer. Per domein gelden aparte (juridische) regels, en gegevens uit het ene domein mogen niet zomaar aan gegevens uit het andere domein worden gekoppeld, hoewel die optie uitdrukkelijk achter de hand wordt gehouden. De wetgeving voor de invoering van het BSN moet nog dit jaar worden afgerond. Voor het BSN wordt het huidige SOFI-nummer gebruikt. [48] Met die stap zijn de principiële bezwaren van oud-minister Borst en de RVZ, die het SOFI-nummer juist níet in de zorg wilden gebruiken, zonder pardon van tafel geveegd.

Grondslag voor het uitdelen van SOFI-nummers (en binnenkort het BSN) is de gemeentelijke basisadministratie, de GBA.

Niet-ingezeten kunnen in sommige gevallen voor een specifiek domein (belastingen, zorg of onderwijs) een nummer krijgen, dat dan alleen binnen dat ene domein geldt.

Bij huisartsen en ziekenhuizen geldt daarnaast sinds kort een identificatieplicht, die in het leven is geroepen om verzekeringsfraude te voorkomen. Alleen wie een verzekeringsbewijs en legitimatie kan tonen, wordt er als verzekerde behandeld. Anders gezegd: alleen na een dergelijke controle mag de huisarts of het ziekenhuis de verrichte handelingen bij de zorgverzekeraar declareren, anders moet de patiënt ze zelf betalen. Het is de bedoeling deze identificatieplicht ook uit te breiden naar andere zorginstanties.

Het voordeel van het gebruik van het BSN voor de overheid is dat er, naast het SOFI-nummer, niet een aparte, complexe nummergenerator voor patiënten in het leven hoeft te worden geroepen. Het voordeel voor patiënten is dat zij zich makkelijk kunnen identificeren: 'Door te kiezen voor een BSN - in casu het huidige SOFI-nummer - kan voor de identificatie van patiënten gebruik worden gemaakt van de gebruikelijke identificatiedocumenten (paspoort, rijbewijs e.d.) waar het SOFI-nummer reeds op vermeld staat. Een zorgpas voor identificatiedoeleinden voor patiënten in de zorg is daarom thans niet nodig.' [49] Aangezien Nederland sinds 1 januari 2005 een algemene identificatieplicht kent, kan in de toekomst zelfs als iemand bewusteloos op de eerste hulp wordt binnengebracht, zijn EPD snel worden gevonden: dat is een kwestie van zijn paspoort raadplegen. Want daarin staat zijn SOFI-nummer, en daarmee weet je ook z'n ZIN.

Inzagerecht voor patiënten

Het BSN krijgt ook een elektronische pendant. Op basis van hun SOFI-nummer en adres kunnen burgers sinds 1 januari 2005 een zogeheten DigiD aanvragen, een digitaal identificatiebewijs, waaraan ze zelf een gebruikersnaam en wachtwoord kunnen koppelen. Na controle van de gegevens bij de GBA wordt het DigiD geactiveerd.

Burgers kunnen het DigiD in de toekomst gebruiken voor alle elektronische communicatie met landelijke en gemeentelijke overheden en -diensten: van het opvragen van uittreksels uit het bevolkingsregister tot het aanvragen van een uitkering of vergunning. Momenteel zijn nog maar een handvol gemeentes, de belastingdienst, de Sociale Verzekeringsbank en het Centrum voor Werk en Inkomen bij DigiD aangesloten. [50]

Door verplicht een gebruikersnaam en een wachtwoord 'bovenop' het SOFI-nummer (of het BSN) te zetten, wordt de kans op misbruik van iemands digitale identiteit door derden drastisch verkleind. Met alleen je BSN kan iemand anders - je werkgever, bijvoorbeeld - zich elektronisch als jou voordoen; vanwege het extra wachtwoord kan dat met een DigiD niet meer zo eenvoudig.

Het lijkt logisch om het DigiD in de toekomst ook te gebruiken als identificatiemethode voor patiënten die hun eigen patiëntendossier via internet willen raadplegen. Je DigiD is immers gebaseerd op je SOFI- /BSN- /ZIN-nummer en is beschermd met een persoonlijk wachtwoord, en kan dus goed worden gebruikt als authenticatiemethode. Patiëntenorganisaties dringen er steeds nadrukkelijker op aan dat elektronisch inzagerecht voor patiënten snel wordt geregeld. [51]

Want de toegang van patiënten tot hun eigen EPD blijft voorlopig op oude leest geschoeid, namelijk op basis van een schriftelijk verzoek waarna papieren inzage op locatie volgt. In slechts een enkel experiment - bijvoorbeeld bij de IVF-kliniek van het Radboud in Nijmegen, en de hemofiliekliniek van het Utrechtse UMC - kregen patiënten elektronisch toegang tot hun eigen dossier.

Patiënten willen hun inzagerecht dolgraag via internet verzilveren. Uit recent onderzoek van de RVZ bleek dat maar liefst 96% van de mensen die wel eens internetten, hun medische dossier graag zou willen inzien. Bijna 71% wilde dat liefst thuis via internet

doen, mits deze procedure goed beveiligd was ('vergelijkbaar met telebankieren'). Slechts 15% wilde liever zijn papieren dossier inzien. Mensen met een chronische ziekte en mensen die vaak hun huisarts of specialist bezoeken, waren het meest geporteerd van het gebruik van internet voor inzage van hun medisch dossier (80%). [52]

Er is ook een inhoudelijk argument om patiënten van meet af aan toegang te geven tot hun EMD en EPD: alleen dan is iemands medicatiedossier volledig te krijgen. Apothekers nemen immers alleen voorgeschreven medicijnen in het EMD op, receptvrije medicijnen belanden er qualitate qua niet in. En Nederlanders kopen steeds meer zelfzorgmiddelen: in 1984 gebruikte slechts 16% zelfzorgmiddelen in de twee weken voor de peildatum, in 2005 was dat opgelopen tot bijna 39%. Alleen al tussen 1999 en 2005 liep het percentage op van 33,5 tot 38,6. [53]

Weten wat iemand aan zelfzorgmiddelen slikt, kan van wezenlijk belang zijn voor de verstrekking van receptgebonden geneesmiddelen. Zo tasten maagzuurremmers (Rennies en dergelijke) de opname van antibiotica aan. Soms ook ligt de bron van gezondheidsproblemen in het gebruik van zelfzorgmiddelen. Veel vitaminepreparaten slikken kan bijvoorbeeld tot vergiftiging leiden; langdurig gebruik van pijnbestrijders kan leiden tot chronische hoofdpijn of maagklachten en zelfs tot maagbloedingen.

Om die redenen pleit onder meer het Nederlands Huisartsen Genootschap ervoor sommige zelfzorgmiddelen voortaan alleen via de apotheek te verkopen; de apotheker kan ze dan alsnog in iemands EMD invoeren. Zowel in praktisch als in principieel opzicht is dit een onzalig idee. Het zou betekenen dat je je ZIN bij de apotheek moet opgeven wanneer je zelfzorgmiddelen koopt, en komt daarmee neer op een verplichte legitimatie bij het kopen van receptvrije medicijnen. Daarnaast gaat deze oplossing eraan voorbij dat mensen hun zelfzorgmiddelen ook geregeld via internet aanschaffen, van Viagra tot middelen tegen botontkalking. De enige methode om te verzekeren dat een EMD compleet kan worden, is zorgen dat mensen zelf zulke middelen eraan kunnen toevoegen. Dat veronderstelt echter dat mensen niet alleen toegang hebben tot hun elektronische dossier, maar er ook wijzigen in mogen aanbrengen.

Maar hoewel de eis om patiënten elektronisch toegang te geven tot hun eigen EPD volstrekt legitiem is en zelfs medisch nut oplevert: hij is buitengewoon lastig te realiseren. De beveiliging van dossiers (identificatie, autorisatie en authenticatie) wordt er in één klap een stuk ingewikkelder door, en dat is al zo'n heikel punt.

Daarnaast verandert de functie van een dossier als patiënten daar systematisch toegang toe krijgen. Medische dossiers zijn voor professionals in de eerste plaats werknotities en voortgangsverslagen; als behandelaars weten dat hun patiënten geregeld nalezen wat zij opschrijven, zullen ze minder snel speculaties over diagnoses of behandelingen noteren, hun dossiers meer naar de patiënt toeschrijven en zaken achterwege laten waarvan ze denken dat die schrik of vragen bij de patiënt oproepen. Medische dossiers zijn in de eerste plaats voor behandelaars bedoeld. De gedachte dat de gegevens die zorgverleners in een medisch dossier noteren het eigendom van de patiënt zouden zijn, [54] bewijst weliswaar lippendienst aan het idee van de mondige patiënt, maar is gebaseerd op een verkeerde inschatting van de functie van een professioneel dossier.

EPD als wegbereider voor eNIK

Hoogervorst wil dit elektronische inzagerecht echter graag regelen. Hoewel het DigiD al is ingevoerd en een goed en goedkoop middel voor elektronische identificatie van burgers biedt, maakte de minister in zijn nota van maart 2005 de toegang voor patiënten tot hun EPD afhankelijk van de elektronische identiteitskaart (eNIK) die alle burgers op termijn moeten krijgen. [55] Wanneer die eNIK zal worden ingevoerd, werd pas in zijn 'spoorboekje' van juni 2005 duidelijk: de beoogde invoeringsdatum is oktober 2006. [56]

Het kabinet wilde deze eNIK, die met biometrische gegevens uitgerust moet worden, al langer invoeren, maar kon niet motiveren waarom. Op 17 oktober 2002 deelde minister van Binnenlandse Zaken Remkes de Tweede Kamer nog mee dat 'uit het haalbaarheidsonderzoek naar de mogelijke invoering van een elektronische variant van de Nederlandse identiteitskaart is gebleken dat er in onvoldoende mate elektronische diensten beschikbaar zijn waarvoor elektronische identificatie noodzakelijk is'. [57] De *Voortgangsrapportage Elektronische Overheid 2002* voegde daaraan toe: 'Daarnaast is de contact-frequentie tussen burger en overheid bij veel diensten laag en zijn er praktische belemmeringen geconstateerd, zoals de mate waarin de burger kan worden ondersteund. Tevens is gebleken dat met de ontwikkeling en uitrol van de eNIK relatief hoge kosten gemoeid zijn. Gelet op deze bevindingen is besloten om op korte termijn geen verdere experimenten en proeven uit te voeren met de eNIK. Daarmee wordt gewacht totdat er organisaties zijn die in dit domein identiteitsrijke elektronische diensten gaan ontwikkelen.' [58]

Niettemin bleef het idee van zo'n kaart lokken. 'Het is de bedoeling om biometrische gegevens op de eNIK aan te brengen,' meldde (toenmalig) minister de Graaf op 3 november 2004 in een overleg met de Tweede Kamer. [59] 'Een chipkaart is een van de middelen waarmee het hoogste veiligheidsniveau van authenticatie [van burgers] bereikt kan worden. Dit kan worden gerealiseerd door de plaatsing van een chip op de Nederlandse identiteitskaart, die daarmee een "eNIK" wordt,' schreef Binnenlandse Zaken eind 2004 nog maar weer eens in een rapport. [60] Diensten waarvoor zo'n kaart handig was, lagen ook toen nog amper in het verschiet. De Sociale Verzekeringsbank gaf in haar meerjarenplanning van 2005-2009 aan deel te willen nemen in de eNIK, [61] maar daar bleef het bij.

Totdat minister Hoogervorst in maart 2005 ineens met zijn ei van Columbus kwam en een 'identiteitsrijke' dienst bedacht: we hebben het eNIK nodig om onze elektronische patiëntendossiers te kunnen inzien. Waarom het DigiD, nota bene een door de overheid zelf ingestelde identificatie- en authenticatiemethode, niet zou volstaan, wordt door hem noch door de rest van het kabinet toegelicht. Hoe de overheid wil regelen dat burgers allemaal een kaartlezer aan hun computer thuis hangen - het eNIK is zonder kaartlezer immers nutteloos - verzuimt Hoogervorst eveneens uit de doeken te doen.

De plotseling door het kabinet gevoelde noodzaak om burgers zo'n kaart met biometrische gegevens te verstrekken, onder meer opdat zij hun eigen medische gegevens elektronisch kunnen inzien, verhoudt zich daarnaast slecht tot de eerder aangehaalde sombere evaluatie van een andere overheidsinstelling, het UZI-register: '... biometrie geeft op dit moment nog te veel fouten […]. [Dit maakt] toepassing van biometrie op korte termijn niet wenselijk.' [62]

Patiëntenprivacy en opsporing

Hoewel de overheid belooft om voorwaarden te stellen aan het gebruik van het BSN, kleven er risico's aan een aanpak waarbij in allerlei domeinen hetzelfde persoonsnummer wordt gebruikt. Enerzijds vergroot het de kans op misbruik: het wordt technisch makkelijker om ongewenste koppelingen tussen iemands persoonlijke gegevens tot stand te brengen. Anderzijds wordt het eenvoudiger om mensen in het ene domein (bijvoorbeeld zorg) uit te sluiten, alleen omdat hun in het andere domein (bijvoorbeeld sociale zekerheid) geen nummer is toegewezen. 'Och nee, daar hebben we regels tegen,' is het geijkte antwoord van de regering, maar de geschiedenis leert dat zulke regels veranderen en dat uitvoerders vaak slordig (of zo men wil 'inventief') omgaan met de wettelijke beperkingen op het gebruik van dergelijke gegevens. Het College Bescherming Persoonsgegevens waarschuwde al in 2002: 'Bij de huidige ICT-projecten is [patiënten]privacy niet als designcriterium meegenomen.' [63]

Het BSN is nadrukkelijk ontworpen om, ten behoeve van de

opsporing, eenvoudiger gegevens over personen te kunnen koppelen. In november 2002 - niet zonder reden na de aanval van Al Qa'ida op de Twin Towers en het Pentagon; na die aanval is een fikse serie privacybeperkende maatregelen genomen - sprak het kabinet dat onomwonden uit. 'De inrichting van een overheidsbreed persoonsnummerbeheer is van belang om invulling te geven aan de wens naar betere mogelijkheden voor gegevenskoppeling ten behoeve van de rechtshandhaving en opsporing. Daarbij wordt gedacht aan een verruiming van de wettelijke mogelijkheden binnen de geldende Europese privacy richtlijnen.' [64] Terrorismebestrijding, akkoord. Maar is het niet bizar dat de overheid een identificatienummer dat in de zorg (en in het onderwijs) gebruikt zal worden, zo direct in verband brengt met opsporing?

De kersverse wet Bevoegdheden Vorderen Gegevens - in juli 2006 door de Eerste Kamer aangenomen [65] - stemt wat dat betreft tot nadenken. Door deze wet wordt de toegang tot tal van gegevens voor politie en justitie eenvoudiger. Oude drempels en waarborgen zijn verlaagd.

De wet maakt onderscheid tussen drie categorieën gegevens: identificeerbare gegevens, andere gegevens en bijzondere gegevens. Onder de 'identificeerbare gegevens' vallen naam, adres, woonplaats, postadres, geboortedatum en geslacht, klant-, polis-, bankrekening- en lidmaatschapsnummers. Deze gegevens kunnen nu door iedere agent of opsporingsambtenaar mondeling worden opgevraagd, zonder schriftelijk bevel van de rechter-commissaris, zoals eerder het geval was.

De categorie 'andere gegevens' is omvangrijk. Het gaat vooral om gegevens uit de administratie en logs van bedrijven. Om deze gegevens op te vragen was eerder een gerechtelijk bevel nodig (en dus toetsing door de rechter), maar onder de nieuwe wet volstaat een bevel van de officier van justitie. Alleen voor de 'bijzondere gegevens', zoals godsdienst, ras, politieke gezindheid, gezondheid of seksuele voorkeur, blijft een gerechtelijk bevel noodzakelijk.

Maar niet eerder hebben we een situatie gehad waarin gezondheidsgegevens zo georganiseerd en gestructureerd opgeslagen moeten worden. Juist het omvattende karakter van het EPD (vrijwel alle burgers zullen er een krijgen) maakt deze gegevensverzameling interessant. Je kunt je voorstellen dat bij een onopgeloste moord ook in de verzamelde EPD's zal worden gezocht naar een match met het DNA van de vermoedelijke dader, maar het EPD is daar simpelweg niet voor bedoeld. We hebben strikte (en in de afgelopen paar jaar al fors versoepelde) regels die bepalen onder welke voorwaarden iemands genetische materiaal in een DNA-bank mag worden opgeslagen en voor opsporingsdoeleinden mag worden gebruikt. Het is een onplezierig idee dat het EPD verdere oprekking van die eisen mogelijk maakt.

Marktwerking

Het EPD is inmiddels tevens een rol toebedeeld bij de aanstaande introductie van marktwerking in de zorg. Die marktwerking - een nette manier om te zeggen dat er een zekere mate van concurrentie in de zorg wordt geïntroduceerd - moet bewerkstelligen dat zorgverleners een betere kwaliteit voor een betere prijs leveren. Daartoe mogen verzekeraars het aanbod in de zorg vanaf 1 januari 2006 gaan sturen, onder meer door alleen contracten met zorgverleners af te sluiten die naar hun oordeel een goede prijs/kwaliteit leveren. Alleen verrichtingen van zorgverleners met wie de betreffende verzekeraar een contract heeft, worden aan de verzekerde vergoed. Met andere woorden: het is niet langer de huisarts die bepaalt naar welke specialist je wordt doorverwezen, maar de verzekeraar. Ziekenhuizen zullen in dit model meer moeten gaan specialiseren, en kunnen (of mogen) niet alles meer doen.

Indien hun zorgverzekeraar besluit dat een specifieke behandeling of zorgtaak elders beter of goedkoper kan worden

ingekocht, hebben patiënten twee opties: ze kunnen een verzekeraar zoeken die wel een contract heeft met hun oude behandelaar, of overstappen naar de nieuwe behandelaar. Consumenten zullen in de toekomst derhalve vaker van verzekeraar en/of zorgverlener moeten wisselen.

'Dit brengt het risico met zich mee van verdere "versnippering" van patiëntgegevens: gegevens over één patiënt zullen op nog meer plaatsen vastgelegd worden zonder dat de bij de behandeling betrokken zorgverlener daarvan op de hoogte is, met alle risico's van dien,' waarschuwde de RVZ de minister eerder dit jaar. [66] Door de woordkeuze - de RVZ spreekt over 'alle wisselende contacten tussen patiënt en verschillende zorgverleners en zorgverzekeraars' - dringt zich een beeld op van promiscue, marktwerkende patiënten en van 'versnippering' als een moderne, administratieve geslachtsziekte. Het EPD moet in de ogen van de Raad het antibioticum tegen deze nieuwe zorgziekte vormen: de vers aangewezen zorgverlener kan via het EPD immers elektronisch toegang krijgen tot eerdere en elders vastgelegde gegevens.

De RVZ wijst er verder op dat de concurrentie tussen zorgbehandelaars nare neveneffecten kan hebben. 'De beoogde competitie tussen zorgverleners zal kunnen leiden tot een verminderde animo voor onderlinge samenwerking en het delen van informatie.'[67] Zonder tegenmaatregel (in de vorm van het EPD) kan de verlangde introductie van marktwerking in de zorg betekenen dat behandelaars meer op hun dossiers gaan zitten en patiëntendossiers meer verbrokkeld raken. De RVZ hoopt met andere woorden dat het EPD de scherpe kantjes van de marktwerking weg zal vijlen.

Ook nu is er al een commercieel circuit binnen de gezondheidszorg: de privé-klinieken. Hoe gaan die twee soorten zorg in de nabije toekomst met elkaars patiëntgegevens om? Stappen de commerciële klinieken ook in het EPD? Is het logisch om commerciële instanties gebruik te laten maken van de resultaten van patiëntonderzoeken die met belastinggeld zijn uitgevoerd, of geeft dat ze een onevenredige voorsprong? Mogen commerciële klinieken bijvoorbeeld gebruik maken van de (dure) MRI-scans van publieke ziekenhuizen? Kan VWS commerciële klinieken verplichten hun gegevens aan publiek gefinancierde zorgverleners ter inzage aan te bieden? En wat te doen met het gegeven dat mensen soms juist naar een privé-kliniek gaan opdat er niets in hun huisartsendossier belandt?

Medische missers

Andere partijen zetten hoog in op het EMD en het EPD omdat daarmee medische missers zouden worden voorkomen. Een van die instanties is de Inspectie voor de Gezondheidszorg (IGZ); die meldt in haar jaarverslagen al geruime tijd dat er in de zorg veel fouten worden gemaakt. De Inspectie wijst erop dat deze 'vermijdbare en verwijtbare fouten' niet alleen veel leed bij de betrokkenen veroorzaken, maar ook leiden 'tot hoge maatschappelijke kosten in de vorm van langdurige aanspraken op zorg, arbeidsongeschiktheid en premies en uitkeringen voor schade.' [68] De voornaamste oorzaak van deze medische missers is gebrekkige communicatie, meent de IGZ: 'Vaak zijn er geen of slechte afspraken gemaakt en is de overdracht tussen verschillende schakels in de zorgverlening niet goed geregeld.' [69]

Hoe vaak medische missers daadwerkelijk voorkomen, is echter niet bekend. Lang niet alle fouten bereiken de Inspectie: er bestaat in Nederland (nog) geen meldingsplicht. Klachten worden gewoonlijk in eerste instantie bij de klachtencommissie van de betreffende instelling of bij de tuchtraad neergelegd. Ook melden zorgverleners incidenten vaak niet, soms uit angst voor sancties, soms om hun collega's te sparen. Gedupeerden op hun beurt kunnen niet altijd vaststellen of er inderdaad sprake was van een vermijdbare fout, oftewel van een situatie die een klacht billijkt. De IGZ vermoedt daarom dat er fors wordt ondergerapporteerd. Omgekeerd zijn er betrekkelijk veel meldingen van gedupeerden

waarbij de Inspectie na onderzoek constateert dat er geen fout is gemaakt, en is er met andere woorden sprake van overrapportage.

In haar jaarrapport over 2002 stelde de Inspectie op basis van extrapolatie van Amerikaans onderzoek dat er in Nederland naar schatting 'tenminste duizend sterfgevallen per jaar [plaatsvinden] die vermijdbaar zijn en een veelvoud daarvan aan niet-fatale vermijdbare schade'. [70] Het jaar erop werd die schatting plotseling fors opgeschroefd, zonder nadere toelichting en nota bene op grond van precies datzelfde Amerikaanse onderzoek. De Inspectie stelde toen dat er 'jaarlijks 1500 tot 6000 patiënten overlijden door vermijdbare incidenten in de zorg'. [71]

Die schatting ligt dusdanig veel hoger dan de circa 100 doden per jaar die bij de Inspectie worden gemeld, dat een grondige onderbouwing bij die cijfers op zijn plaats zou zijn. Die bleef echter achterwege. Die nalatigheid doet zich des te meer voelen daar de Inspectie elders erkent dat de fundamentele verschillen in de gezondheidszorg tussen de Verenigde Staten en Nederland een dergelijke extrapolatie 'onbetrouwbaar' maakt. [72] (De VS werkt bijvoorbeeld in tegenstelling tot Nederland niet met vaste huisartsen, waardoor er geen 'poortwachters' in de zorg zijn en elk overzicht van patiëntgeschiedenissen mist.)

Vermijdbare medische incidenten 2000-2004; bron: IGZ. [73]

el bij patiënt	***2000***		***2001***		***2002***		***2003***		***2004***	
den	83	28,3%	90	28,6%	96	16,5%	122	20,7%	116	19,0%
d letsel	20	6,8%	15	4,8%	22	3,8%	24	4,1%	37	6,1%
letsel	45	15,4%	26	8,2%	75	12,9%	83	14,1%	93	15,2%
elijk letsel elijk	50	17,1%	83	26,3%	120	20,6%	114	19.6%	114	18,7%
tsel	95	32,4%	89	28,3%	240	41,2%	235	39,9%	237	38,8%
nd	-	-	12	3,8%	29	5,0%	11	1.9%	14	2,3%
gemelde dbare incidenten	293	100%	315	100%	582	100%	589	100%	611	100%

Een overzicht van de daadwerkelijk gemelde, door de IGZ als terecht beoordeelde klachten over medische fouten in de periode 2000-2004 staat hiernaast. De meeste én de ernstigste incidenten doen zich voor in de curatieve zorg (ziekenhuizen). De als 'medische misser' beoordeelde incidenten staan echter in geen enkele verhouding tot de eerdere spectaculaire schattingen van de IGZ ('1500 tot 6000 doden per jaar'). Voorts valt op dat er in 30 tot 40% van de incidenten geen letsel is veroorzaakt, ook al zijn er wel degelijk fouten gemaakt. Tenslotte is onduidelijk of de gerapporteerde fouten inderdaad informatiemissers zijn.

Begin 2005 publiceerde de IGZ een rapport over patiëntveiligheid waarin ook gegevens van toezichthouders en registers van zorginstellingen werden opgenomen. Alweer werd melding gemaakt van opzienbarend hoge cijfers. Herstel: potentieel opzienbarende cijfers. 'Uit de resultaten […] blijkt onder meer dat tienduizenden mensen per jaar een recept krijgen dat *mogelijk* schadelijk voor hen is.' [74] Het begeleidende persbericht sprak zelfs van 'honderden doden per jaar', [75] een aantal dat overigens in het persbericht noch in het rapport zelf werd toegelicht of onderbouwd.

Maar wat in hemelsnaam zijn medicijnen die 'mogelijk schadelijk' zijn? Ook verzuimt de IGZ uit te leggen hoe die 'tienduizenden' incidenten zich verhouden tot de slechts 68 meldingen van medicatiefouten (waarbij overigens niemand blijvend letsel opliep) die zij over 2001 afhandelde.

Een tweede partij die de komst van het EPD omhelst als medicijn tegen medische missers is de NPCF, de Nederlandse Patiënten Consumenten Federatie. Samen met het NICTIZ heeft de NPCF onderzoek laten doen naar de consequenties van de gebrekkige uitwisseling van informatie tussen huisartsen, specialisten en apothekers. De uitkomsten waren ook hier sensationeel:

‘De consequenties van deze overdrachtsfouten kunnen voor de patiënt zeer ernstig zijn: (blijvende) lichamelijke gevolgen, emotionele gevolgen en zelfs arbeidsongeschiktheid. Naar schatting zijn 50.000 mensen in de WAO terechtgekomen door medische overdrachtsfouten. Een Elektronisch Patiënten Dossier kan veel problemen voorkomen.

Omgerekend naar de gehele Nederlandse bevolking hebben bijna 800.000 mensen van 18 jaar en ouder met medische overdrachtsfouten te maken gehad. Ze kregen verkeerde medicijnen, een verkeerde operatie of behandeling of ze konden niet worden geholpen omdat medische informatie ontbrak. De fouten hebben grote gevolgen op financieel gebied. De kosten zouden jaarlijks rond de 1,4 miljard uitkomen. Het grootste deel hiervan zijn WAO-kosten.

Nog ingrijpender dan de financiële gevolgen zijn de gevolgen voor de individuele patiënt op emotioneel en lichamelijk gebied. Mensen die dit soort fouten is overkomen voelen zich boos, machteloos of raken in paniek. Een derde van de patiënten (omgerekend zijn dat 250.000 mensen) heeft te maken met lichamelijke gevolgen. Bij de helft van hen zijn de gevolgen blijvend.’ [76]

Deze cijfers hebben betrekking op de vraag hoe vaak mensen ooit met dergelijke fouten te maken hebben gehad; ze zijn cumulatief. Volgens het onderzoek werden over 2003 in totaal 161.000 medische missers gemeld. [77] Hoe het mogelijk is dat, wanneer alleen al in één specifiek jaar 161.000 medische missers worden gerapporteerd, het totaal over alle voorgaande jaren slechts vijfmaal zo hoog is, vermeldt het rapport niet. Dat is licht bevreemdend. Mogelijk staan recente fouten mensen helderder voor de geest, maar de discrepantie is opmerkelijk.

Er vallen meer kanttekeningen te plaatsen. Zo blijkt het onderzoek uitsluitend te zijn gebaseerd op de perceptie van patiënten en is de versie die zij van het incident gaven, niet gecontroleerd. ‘Zo wijten ruim zeshonderd deelnemers aan het onderzoek hun arbeidsongeschiktheid aan de medische overdrachtsfouten die zijn gemaakt. Maar de onderzoekers hebben geen nader dossieronderzoek gedaan. Dan mag de vraag worden gesteld hoe betrouwbaar die uitkomst is,’ schreef de Orde van Medisch Specialisten in een reactie. [78]

De definitie van ‘fout’ is voorts nogal vlottend. Er valt volgens NPCF/NICTIZ nogal wat onder: van een gezonde nier die wordt weggehaald in plaats van de zieke blaas, tot onderzoeksresultaten die op zich laten wachten of een consult dat niet doorgaat. Het eerste is een bloedserieuze, invaliderende en verwijtbare fout; de laatste twee zijn meestal een bagatel en kun je met goed fatsoen niet in verband brengen met mensen die door medische missers in de WAO beland zijn. Er wordt verder geen enkele poging gedaan om aan te tonen dat de geïnventariseerde problemen ook allemaal fouten zijn en inderdaad door gebrekkige informatieoverdracht werden veroorzaakt. Bij zo’n weggehaalde nier is er evident iets drastisch fout gegaan, [79] maar wanneer twee artsen tot verschillende diagnoses komen of een medicijn verkeerd uitpakt, heeft dat gewoonlijk niets met fouten of tekortschietende informatieoverdracht te maken.

Het is goed mogelijk dat het EMD medicatiefouten helpt verminderen, maar de enorme besparingen waarnaar kabinet en parlement reikhalzend uitzien - men hoopt op duizenden WAO’ers en honderden ziekenhuisopnamen per jaar minder - zijn onwaarschijnlijk.

Technologische oplossingen, of organisatorische?

Maar gemaakt worden ze wél, medische fouten. Uit een rapport van het Wetenschappelijk Instituut Nederlandse Apotheken (WinAp) uit 2001 bleek dat 5% van de recepten die artsen uitschrijven, fouten bevat. Ongeveer een kwart daarvan zou kunnen leiden tot problemen voor de patiënt. [80] Het Lareb, een instituut dat de bijwerkingen van medicijnen registreert, krijgt

jaarlijks tussen de 150 en 200 meldingen van patiënten die door verkeerd medicijngebruik zijn overleden.

Bij het verstrekken van medicijnen komen vier soorten fouten voor:

1. voorschrijffout door de arts (een verkeerde indicatie voor een medicijn, het missen van een contra-indicatie of allergie, verkeerde dosis uitschrijven, enzovoort);
2. transcriptie (het verkeerd lezen of interpreteren of overnemen van het recept door de apotheek, of door een intermediair zoals een medisch secretaresse of verpleegkundige die het recept invoert);
3. distributie (fouten gemaakt tijdens het afhandelen van het recept door de apotheek, door verkeerde berekening, bereiding, of afgifte);
4. toediening van medicatie (geen of verkeerde dosis, verkeerde tijd, verkeerd medicijn, verkeerde toedieningsvorm). [81]

Fouten van het eerste type kunnen deels met een EMD worden vermeden, fouten van het tweede type bijna in hun geheel. Alleen al om die reden is het EMD wenselijk.

Toch is het niet zo dat een EMD deze twee typen fouten uitsluit. Zelfs mét een EMD blijken zorgverleners niet precies te weten welke medicijnen een patiënt gebruikt. Een Nederlands onderzoek liet zien dat huisartsen en apothekers onderling tot verschillende lijsten komen van de middelen die hun patiënten gebruiken, ook indien zulke informatie elektronisch werd uitgewisseld. De overeenkomsten tussen de lijstjes was echter wel iets groter bij dergelijke communicatie. [82]

Een EMD is niet het enige middel dat ingezet kan worden tegen medicatiefouten. De beroepsorganisaties hameren erop dat het, juist in het belang van een goede bereiding en aflevering van medicijnen, belangrijk is dat er altijd een gediplomeerd apotheker in de apotheek aanwezig is. Het kabinet wil die eis echter laten vervallen, deels vanwege de beoogde kostenbesparing, deels vanwege de eerder genoemde marktwerking. De wet moet het mogelijk maken dat de zorgverzekeraars hun regierol in de farmaceutische zorg waar kunnen maken zonder gebonden te zijn aan de 'traditionele' apotheek en apotheker.

De Koninklijke Nederlandse Maatschappij ter Bevordering der Pharmacie (KNMP) en de Raad van State hebben ernstige bedenkingen bij het wetsvoorstel. Ze vrezen onder meer dat het zo voor zorgverzekeraars en winkelketens te gemakkelijk wordt om medicijnen aan de man brengen. ‘Zij zouden dan kunnen volstaan met een apotheker ergens op een kantoor in Zaandam of Leusden en in hun apotheken kunnen volstaan met goedkopere assistenten. Maar die apotheker in dat kantoor kan nooit zo goed zicht houden op de kwaliteit van hulpverlening in de apotheken als de apotheker die zelf in de apotheek bij het verstrekken van medicijnen aanwezig is,’ meent Marga van Weelden, voorzitter van de KNMP. [83]

De KNMP wijst erop dat minister Hoogervorst met dit voorstel zijn eigen beleid ondergraaft. Hoogervorst wil op andere punten immers dat de apotheker intensiever betrokken wordt bij het voorschrijven van medicijnen. ‘Van dat voornemen kan niets terechtkomen als patiënten, huisartsen en verzekeraars in de apotheek geen apotheker aantreffen om de zorg te verbeteren als het gaat om zaken als therapietrouw, nepmedicijnen, herhaalmedicatie of doelmatig voorschrijven.’

Een andere, vrij simpele, maatregel die medicatiefouten kan verminderen, is het voorstel om voortaan de diagnose op recepten te vermelden. Apothekers hebben immers een aanzienlijk grotere farmaceutische kennis dan huisartsen. Zij zouden op die manier kunnen helpen beoordelen of een patiënt wel het juiste medicijn kreeg voorgeschreven, wat medicatiefouten helpt voorkomen. Het idee werd, heel inconsequent, geopperd door diezelfde minister Hoogervorst die van de eis van de fysieke aanwezigheid van apothekers af wil. En weer die spierballentaal: Hoogervorst wil op korte termijn met alle betrokken partijen overleggen over het vermelden van de diagnose, ‘en als zij niet vrijwillig meewerken, dwingt de minister het wettelijk af’. [84]

Nieuwe systemen, nieuwe fouten

Waar beleidsmakers buitengewoon weinig rekening mee houden, is dat nieuwe systemen naast veel verbeteringen ook altijd nieuwe fouten introduceren. De optimistisch gestemde verwachtingen van elektronische dossiers zijn niet meer dan dat: verwachtingen. De praktijk is een stuk weerbarstiger. ICT blijkt ook een nieuwe risicofactor te vormen, zoals de Inspectie uiteenzet in haar rapport *ICT in ziekenhuizen*. 'Dit onderzoek bevestigt bevindingen uit de (inter)nationale literatuur, waaruit blijkt dat ICT zowel een bedreiging voor de kwaliteit van zorg kan zijn als een bijdrage aan die kwaliteit kan leveren. […] Ondanks alle voordelen van het gebruik van ICT - zoals de betrouwbare beschikbaarheid van informatie - loopt de patiënt hierdoor mogelijk onnodig gevaar.' [85]

De geconstateerde problemen zijn niet mis:

> De beveiliging van ICT applicaties en apparatuur is onder de maat. De "NEN 7510 Informatiebeveiliging in de Zorg"-norm, die duidelijk aangeeft waar op gelet moet worden, wordt in ziekenhuizen niet systematisch nageleefd. De veiligheid van informatie die in ziekenhuizen aanwezig is, wordt hierdoor bedreigd. Dit betreft niet alleen de beveiliging van de gegevens zodat onbevoegden er geen kennis van kunnen nemen, maar ook de aanwezigheid van de gegevens op het juiste moment bij de juiste persoon. Of de gegevens op zich wel juist zijn (de integriteit van gegevens) is een onderwerp dat eveneens onder de beveiliging van gegevens valt, maar waar onvoldoende aandacht naar uit gaat. [...] De inhoudelijke kant, ook wel aangeduid met het gebruikersaspect, van de ICT-applicatie berust bij applicatiebeheerders die geen deel uitmaken van de zorgafdelingen. De verantwoordelijkheid en deskundigheid is daarmee versnipperd en wat betreft continuïteit bedreigd. [86]

De Inspectie trof onder meer de volgende problemen aan: onjuist ingevoerde gegevens die leiden tot herhalingsfouten bij medicatie, verwisseling van gegevens van patiënten die leidde tot het geven van medicatie aan een naamgenoot, onjuiste protocollen en/of rekenregels waardoor uitkomsten onjuist werden geïnterpreteerd, een verwisseling van bloedgroep met dodelijke afloop, verkeerd voorschrijven van medicijnen vanwege het verkeerd aanklikken in een lijst op een computerscherm, vernietiging van dossiers door een computervirus, problemen bij de verantwoordelijkheid van handelingen door niet-traceerbare gegevensmutaties (vaak omdat meerdere gebruikers via hetzelfde account werken), uitval van apparatuur waardoor gegevens en digitale röntgenfoto's verloren gingen, het gebruik van autonome programma's die zonder sturing zelf gegevens zoeken en verwerken, de opbouw en structuur van programma's die niet aansloten bij de praktijk waardoor fouten werden gemaakt, en een gebrekkige bescherming van de privacy van patiënten.

Officiële gegevens uit Amerika wijzen uit dat momenteel maar liefst 20% van alle gerapporteerde medicatiefouten te wijten zijn aan automatisering en foutief ingevoerde of verwerkte gegevens, en dat dit percentage fors stijgt. Verkeerde computergegevens zijn inmiddels in rang de vierde oorzaak van medicatiefouten. Van de 235.159 onderzochte meldingen resulteerde 1,2% in fysieke schade voor de patiënt, gelukkig meestal van tijdelijke aard. 40 mensen hielden permanente schade over, 74 mensen balanceerden op de rand van de dood en 24 mensen overleden. [87]

Een deel van de fouten werd veroorzaakt doordat de computersystemen onhandig of niet intuïtief waren ingericht, of doordat het medisch personeel onvoldoende vertrouwd was met het gebruik ervan. Ander onderzoek wijst erop dat artsen die nog niet zo behendig met computers zijn, door het gebruik van EPD's feitelijk minder informatie voorhanden hebben dan voorheen. [88] Soms is het ook gebrekkige software die voor fouten zorgt: een software-update in St. Mary's Mercy ziekenhuis in Grand Rapids,

Michigan, veranderde in 2003 de status van 8500 patiënten van 'ontslagen' in 'overleden'. [89]

Uit een buitengewoon gedetailleerd onderzoek - de onderzoekers bivakkeerden in een ziekenhuis waar ze met zorgverleners spraken en meeliepen - kwam naar voren dat het EMD maar liefst 22 nieuwe soorten fouten introduceert. [90] Een greep uit de nieuwe fouten die werden aangetroffen:

- Behandelaars krijgen geen coherent beeld van de patiënt doordat de informatie gefragmenteerd over verschillende schermpagina's wordt weergegeven;
- Overzichten van beschikbare doseringen worden vaak als doseringsadvies begrepen, wat geregeld tot het voorschrijven van een te lage dosis leidde;
- Functionele onderdelen zijn in de programma's uit elkaar getrokken, zodat er dubbel wordt voorgeschreven;
- De gebruikte programma's zijn weinig flexibel, wat tot verkeerde of ontbrekende gegevens leidt.

Driekwart van de geobserveerde zorgverleners meldde dat zij minimaal eens per week op elk van de onderscheiden tweeëntwintig fouten waren gestuit.

De onderzoekers benadrukken dat ook de negatieve effecten van het EMD moeten worden besproken en onderzocht, en roepen beleidsmakers op niet langer één kant van de medaille te belichten. Waar ze vooral op wijzen, is dat het gebruik van het EMD in de organisatie moet zijn ingebed. Technologie wordt nu vaak opgedrongen en verwordt tot een doel op zich, terwijl ICT veeleer een ondersteunende rol zou moeten innemen. Een betere kennis van de dagelijkse medische praktijk zou de programmatuur daarnaast een stuk veiliger maken. Veel fouten en hebbelijkheden in de programmatuur zijn eenvoudig op te lossen, maar programmeurs zien ze niet omdat ze de praktijk niet kennen. Zorgverleners trachten op hun beurt om zulke tekortkomingen en onhandigheden heen te werken, in plaats van ze bij de software-ontwikkelaars te melden.

Papier heeft in de loop der tijd zijn nut terdege bewezen, en we hebben een grote handigheid verworven in het interpreteren ervan. Je weet dat nieuwe toevoegingen altijd voor in het dossier liggen, je ziet meteen hoe omvangrijk (en dus: complex) het dossier is, je kunt makkelijk twee velletjes naast elkaar leggen voor een snelle vergelijking, uit het handschrift of briefhoofd kun je aflezen van welke collega een notitie afkomstig is, uit de plaats waar het dossier ligt - links of rechts op je tafel - weet je of je het afgehandeld hebt of niet. [91] Voordat we aan elektronische bestanden met een enkele blik dergelijke 'situationele' kennis kunnen afleiden, moeten zowel wij als het EPD nog flink evolueren en zijn we vermoedelijk een decennium verder.

Databescherming, virussen en meekijkers

De virusbesmetting in het Spaarne Ziekenhuis was de eerste waarvan melding gemaakt werd in de pers. Het is echter beslist niet de eerste keer dat een computervirus in een Nederlands ziekenhuis rondwaart. Diverse bronnen verwijzen naar ziekenhuizen die het voor kortere of langere tijd zonder röntgenfoto's moesten stellen, omdat de computers waarmee zulke foto's digitaal worden bekeken door een virus waren uitgeschakeld. [92]

De overlast door virussen neemt bovendien toe. Het CBS heeft becijferd dat 32% van de Nederlandse bedrijven in 2003 schade heeft ondervonden door computervirussen. In 2002 was dat percentage al gestegen tot 45%, ook al gebruikte 91% een virusscanner. [93] Virusbestrijder McAfee berichtte onlangs dat aanvallen met zogeheten 'bots' die andermans computer overnemen, explosief zijn gestegen: 'Alleen al in het eerste en tweede kwartaal van 2005 is het aantal computers dat misbruikt werd via achterdeurtechnieken - in vergelijking tot de eindcijfers over 2004 - met 63% gestegen.' [94] Zulke besmettingen en computerkapingen worden zelden gemeld, maar lekken niettemin

geregeld uit. Een greep uit de pers:

- In november 2001 werd het merendeel van de negentien ziekenhuizen in Noord-Ierland door een virus geteisterd; [95]
- Het Beth Israel ziekenhuis in Boston kon in november 2002 vier dagen lang zijn computers niet gebruiken vanwege een virus; [96]
- In oktober 2002 lagen de computers in een kinderziekenhuis in Texas een week plat vanwege het Bugbear-virus, wat vervolgens wel betekende dat ze 'minder last' hadden van het Blaster- en Sobig-virus van een jaar later; [97]
- Datzelfde Blaster-virus zorgde voor een 'code oranje' - de een-na-hoogste staat van paraatheid - in het Sir Charles Gairdner Hospital in Perth, Australië, en besmette het Cooley Dickinson ziekenhuis in Northampton, Massachusetts; [98]
- In januari 2003 lag de elektronische communicatie in het academische Vanderbilt ziekenhuis in Nashville, Amerika, plat door een besmetting met het W32.Slammer-virus; [99]
- In maart 2003 werd een deel van de medische dossiers van een ziekenhuis in Toronto door een fout of virus gewist, zonder dat iemand begreep waardoor dat kwam; [100]
- In augustus 2003 woedde het Nachi-virus in verschillende ziekenhuizen in Glasgow, Schotland; één ziekenhuis moest 15 uur lang alle computers uitzetten; [101]
- In mei 2004 bezocht het Sasser-virus het Anderson Cancer Centrum in Texas; de EPD's moesten worden uitgeprint want elektronisch waren ze niet langer toegankelijk; [102]
- Hetzelfde overkwam het Asan Medical Center, een van de grootste ziekenhuizen in Seoul, Korea. [103]

Vrijwel alle artikelen dienaangaande melden dat 'de zorg voor patiënten er niet onder te lijden had', een frase die bezwerend is bedoeld maar zich moeizaam verhoudt tot al die keren dat wordt vermeld dat alle computers uit moesten, dan wel dat de elektronische dossiers 'uitgeprint moesten worden'.

Sommige virussen - SirCam, bijvoorbeeld - hebben als extra hebbelijkheid dat ze documenten van besmette computers plukken en rondmailen. [104] Bijna alle moderne virussen zijn ontworpen om de makers op afstand toegang te geven tot de besmette machines. De gegevens die op een besmette computer staan, kun je daarom eigenlijk niet meer vertrouwen: er kan immers mee gerotzooid zijn. Zoiets mag nooit gebeuren met medische informatie. Zowel vanuit het oogpunt van veiligheid van de bedrijfsvoering van ziekenhuizen en huisartsen, als dat vanuit de privacy van patiënten, moet je alles in het werk stellen om medische computers lek- en virusvrij te houden.

Computerbesmettingen zijn nooit helemaal te voorkomen, maar er zijn een paar constanten te onderscheiden in de genoemde voorvallen. Systemen (werkstations en servers) bleken niet up-to-date te zijn (het Spaarne Ziekenhuis meldde na de besmetting alle virusscanners te hebben bijgewerkt), en door softwarehuizen verstrekte updates waren in de praktijk lang niet altijd geïnstalleerd. Die laksheid zorgt voor extra kwetsbaarheid.

Wat opvalt is dat alle virussen die worden genoemd, Windowsvirussen zijn. Tevens zijn alle momenteel ontwikkelde EPD's en EMD's Windowsprogramma's. Nu zijn andere besturingssystemen ook niet vlekkeloos, en, zoals het hoofd automatisering van het Spaarne terecht stelt: 'Als andere systemen populairder waren, zouden ook daar virussen voor worden geschreven.' [105]

Sommige gebruikersprogramma's schieten echter notoir tekort waar het de beveiliging tegen virussen betreft. Als het HIS van huisartsen op een computer draait waarop ook Outlook of Internet Explorer zijn geïnstalleerd, is dat een risico. Beide programma's hebben geregeld maanden achtereen lekken gehad voordat Microsoft een verbeterde versie vrijgaf. Via zulke lekken kunnen buitenstaanders eenvoudig binnendringen en gegevens kopiëren, of zelfs veranderen. Dat een website voor huisartsen een artikel wijdt aan de vraag hoe je van pop-ups, virussen en spyware

op je computer kunt afkomen, stemt evenmin gerust. [106]

De klassieke mededeling: 'Windows is een fout tegengekomen', die bij gebruikers bekend staat als *the blue screen of death*, moet vooral een metafoor blijven. Ook Windowssystemen zijn goed te beveiligen, en binnen een goed opgezet netwerk is het niet eens nodig om alle updates te installeren omdat 'fout' verkeer het netwerk dan helemaal niet in kan komen. Maar dat vergt kennis en goed beheer.

Juist omdat we het medisch bedrijf zo afhankelijk maken van elektronische gegevens, is het zaak om ziekenhuisnetwerken en huisartsencomputers bovengemiddeld te beveiligen. In ziekenhuisnetwerken kun je nu nog makkelijk je laptop aansluiten, of je kunt van huis meegebrachte CD's, USB-sticks of floppies in je werkstation steken. Dat is vragen om moeilijkheden; ook het Spaarne vermoedt dat daar de oorzaak van hun besmetting heeft gelegen.

Niemand die bij een bank werkt, zou erover piekeren zijn eigen spullen in het bedrijfsnetwerk te hangen; daar zijn strikte regels tegen. Moeten ziekenhuizen niet een hoger niveau van beveiliging nastreven (inclusief jaarlijkse audits), een die meer lijkt op de strikte procedures die de financiële wereld toepast? Daar hoort dan wel een passend budget bij. Grotere bedrijven reserveren gewoonlijk gemiddeld 8% van hun begroting voor automatisering, banken en verzekeringsbedrijven gemiddeld 12. Ziekenhuizen mogen echter maar 2% van hun budget aan automatisering besteden.

Hoe gaan huisartsen trouwens zorgen voor goede back-ups van hun patiëntendossiers? Goede back-ups worden elders bewaard. Voor ziekenhuizen behoren goede back-uproutines (inclusief het off-site bewaren ervan) inmiddels tot de normale bedrijfsvoering, maar is het fair om van alle huisartsen te verwachten dat zij individueel maatregelen treffen, en de integriteit van het patiëntenbestand daarmee afhankelijk te maken van hun besef van veiligheid? Is het niet verstandiger om daarvoor een infrastructuur te ontwikkelen waarbij standaard 's nachts een kopie van het actuele bestand wordt getrokken, die op een centrale plaats wordt bewaard en beveiligd?

Conclusies

Elektronische opslag van patiëntendossiers kan het medisch proces helpen stroomlijnen, en kan bevorderen dat informatie snel en adequaat kan worden uitgewisseld. Maar de gedachte, die op dit moment sterk overheerst bij de politiek, dat elektronische medische dossiers het antwoord zijn op een breed scala aan problemen in de gezondheidszorg wordt zeker niet gestaafd, nog daargelaten dat invoering van zulke dossiers op zich weer nieuwe problemen (en fouten) met zich meebrengt. Een extra risico daarbij is dat mensen sterk geneigd zijn computergegevens meer te vertrouwen dan gegevens op papier, juist omdat het medium een distantie en objectiviteit suggereert die het echter niet heeft. Dat 'iets in de computer zit' maakt het nog niet volledig of foutloos: het is en blijft mensenwerk.

De leidende gedachte is dat het medisch bedrijf er efficiënter door wordt, dat spoedeisende hulp sneller kan worden verleend en dat 'medische missers' kunnen worden voorkomen. Die verwachtingen zijn nogal overtrokken, deels omdat de inschatting van het huidige aantal missers onrealistisch hoog is, deels omdat er geen rekening wordt gehouden met nieuwe soorten fouten die via het EMD/EPD worden geïntroduceerd.

Maar het streven om alle informatie die binnen de medische praktijk over een lichaam wordt verzameld, te structureren, ten alle tijde opvraagbaar te maken en voor andere zorgverleners te ontsluiten, verandert ook iets in de medische praktijk. Doordat er al een corpus aan informatie klaar ligt waarmee de arts zich moet verhouden, worden zorgverleners gestimuleerd meer naar de verslaggeving over iemands klachten te kijken en minder naar dat problematische lichaam zelf. Het vastleggen, beheersen,

stroomlijnen en coördineren van informatie krijgt een belangrijker plaats toegekend dan het daadwerkelijk kijken, betasten, voelen, kloppen en luisteren. Informatiemanagement neemt de plaats in van lichamelijkheid.

De narratieve en biografische elementen komen op een lager plan: bij doorverwijzingen hoeft een patiënt niet meer te vertellen wat hem scheelt, de anamnese ligt klaar. Het vertellen en duiden van klachten wordt minder belangrijk. Daarmee wordt ook iemands verhaal - de lijn die hij zelf aanbrengt in zijn klachten, het inkijkje in zijn persoonlijkheid dat hij al vertellend geeft, zijn geschiedenis, zijn zienswijze - gedevalueerd.

Papier is geduldiger dan elektronische informatiedragers. Het laat zich niet zo makkelijk massaal vernietigen (behalve door brand) en is minder makkelijk massaal te muteren of te stelen. Een papieren dossier kun je nog wel van een tafel wegnemen, maar duizenden dossiers stop je niet zo makkelijk in je binnenzak. Informatisering maakt dat juist wel mogelijk: er is meermalen op gewezen dat elektronische opslag van patiëntendossiers spionage en diefstal in de hand werkt. In het recente verleden zijn gevallen gemeld van medewerkers die medische informatie aan derden verkochten, van chantage om massaal medische gegevens openbaar te maken, en van inbraken op of lekken in computersystemen waardoor duizenden - in een geval zelfs één half miljoen - dossiers voor het oprapen lagen. [107] Reken maar dat roddelbladen geïnteresseerd zijn in het medisch dossier van Balkenende of Maximá, en dat bedrijven die verwikkeld zijn in een overnameslag, graag willen weten hoe het met de gezondheid van de betrokken directeuren is gesteld.

Vanwege het grotere risico op verlies of corruptie van elektronische data, lijkt het aanhouden van papieren kopieën raadzaam. Redundantie is altijd belangrijk, maar in het medisch domein eens te meer. Een goede aanbeveling is voorts om het medisch geheim uit te breiden naar vakgroepen die beroepsmatig met elektronische dossiers werken, zoals datatypisten en systeembeheerders. Zij hebben immers toegang tot gegevens die voor artsen en verpleegkundigen onder hun beroepsgeheim vallen, en het is vreemd dat die plicht niet voor administratief en computertechnisch personeel geldt.

Het elektronisch patiëntendossier rijst uit de diverse bronnen op als de panacee voor het managen van de zorg. Het elektronisch vastleggen en dito opvraagbaar maken van ieders medische bestand zou de zorg transparanter én efficiënter maken, kosten en activiteiten in de gezondheidszorg transparant, beter beheersbaar en planbaar maken, en daarnaast foutreductie, kostenbesparing, fraudebestrijding, marktwerking en bevolkingsonderzoek een cruciale duw in de goede richting geven. Uit dit streven naar informatisering van het medisch bedrijf spreekt een fascinatie voor beheersing, controle en planning, de droom van een transparant, volmaakt, gereguleerd en risicoloos bestaan. De gedachte dat met standaarden risico's en fouten kunnen worden uitgebannen is echter een illusie, temeer daar de overheid vergeet dat die standaarden zelf telkens weer inzet zijn van een belangenstrijd tussen de diverse ruziënde of concurrerende partijen (artsen versus apothekers, beleidsmakers versus het veld).

Waar automatiseringsprojecten voortkomen uit problemen die zorgverleners in de dagelijkse praktijk ondervinden, en de voordelen ervan voor alle partijen helder zijn, verloopt informatisering vrij vlot en vlekkeloos. Denk bijvoorbeeld aan het waarneemdossier voor huisartsen, dat vrij spontaan tot stand is gekomen, en zich zonder enige landelijke sturing snel heeft verspreid, en aan het elektronisch declareren. Zodra er echter sprake is van door derden opgelegde eisen - de DBC's zijn daarvan een navrant voorbeeld - wordt informatisering een struikelblok, en, wat erger is, ervaren zorgverleners het als een belasting bij hun werk in plaats van als ondersteuning ervan.

Het EPD optuigen met steeds meer functionaliteiten, verwachtingen en vereisten helpt ook al niet. Juist uit een

eenvoudige aanpak is de meeste winst te behalen. Te overwegen valt om het landelijk dekkende EPD te beperken tot de belangrijkste informatie over patiënten in plaats van alle informatie over alle patiënten te allen tijde toegankelijk te maken. Uitbreiden van het waarneemdossier tot een applicatie waarin ook informatie van specialisten is vervat, lijkt een veel praktischer aanpak, eentje die bovendien voortbouwt op wat de praktijk zelf heeft voortgebracht.

Hoe ICT-plannen struikelen, is inmiddels genoegzaam bekend. 'Te ambitieuze doelstellingen, te weinig reflectie op de consequenties van eenmaal gemaakte keuzes, te weinig ruimte voor inbreng van mensen die echt met de systemen moeten gaan werken en de neiging om tijdens het ontwikkellingstraject de specificaties van het te bouwen systeem aan te passen.' [108]

Het EPD hoort geen technodroom van managers en beleidsmakers te zijn. Technologie is een groot goed, maar mag de gang van zaken nooit dicteren. Beter is om de invoering van elektronische dossiers rustig en stapsgewijs te laten verlopen. Dat garandeert bovendien een betere afstemming op de praktijk, en dat is juist in medische zaken van groot belang. Wie dat negert, maakt het EPD tot een nachtmerrie voor zorgverleners en patiënten.

Karin Spaink
april-juli 2005

Met dank aan:

Marc Berg	hoogleraar Sociaal Medische Wetenschappen Erasmus Universiteit
Michel Bouquet	hoofd automatisering Spaarne Ziekenhuis
Arjen Kamphuis	ICT consultant
Leon Kuunders	beheerder www.cvib.nl
Joris Verhaar	huisarts, ex-secretaris Landelijke Huisartsen Vereniging (LHV)

Noten

1. ‘Computervirus verlamt “Spaarne”’, *Haarlems Dagblad*, 10 maart 2005; ‘Virus zorgt voor chaos bij Spaarne Ziekenhuis’, *Webwereld*, 10 maart 2005, <www.webwereld.nl/articles/30920/spaarne>, ‘Ziekenhuis zegt afspraken af door computervirus’, *Planet*, 10 maart 2005, <www.planet.nl/planet/show/id=69412/contentid=557682/sc=9a0ea0>.
2. ‘Spaarne Ziekenhuis het eerste met “archiefloze polikliniek”’, persbericht Spaarne Ziekenhuis, 4 oktober 2004, <www.spaarneziekenhuis.nl/nieuws/index.php?art=2004/041004_03>. De term ‘papierloos’ zou beter zijn gekozen, want uiteraard heeft het Spaarne archieven. Ze zijn alleen volledig gedigitaliseerd.
3. ‘Computervirus verlamt “Spaarne”’, *Haarlems Dagblad*, 10 maart 2005.
4. ‘Ziekenhuis verlost van computervirus’, *Haarlems Dagblad*, 15 maart 2005.
5. De zogeheten ‘professionele samenvatting’.
6. Citaten Hoogervorst uit een verslagje over het debat in *de Volkskrant*, ‘Hoogervorst verplicht medici patiëntgegevens uit te wisselen’, 11 maart 2005.
7. VWS: *ICT in de zorg. Implementatieplan EMD/WHD*, p. 1.
8. Zie bijvoorbeeld de serie artikelen op <www.project.nl/automatiseringgids/site/page.liones.php?sid=34fgy6dggh77jhgr&pointer=1-2-20-127-449-2337>.
9. De Inspectie Werk en Inkomen publiceerde op 14 februari 2005 een rapport waaruit bleek dat de meeste gemeenten weinig doen om de gegevens van bijstandsontvangers te beveiligen: *Beveiliging Stuwinet bij gemeenten*, Den Haag, februari 2005.
10. De RVZ bedoelde niet noodzakelijkerwijs het internet; er is gespeeld met de gedachte aan een besloten netwerk voor vitale informatie. Engeland legt momenteel voor hun EPD zo’n besloten netwerk aan.
11. RVZ: *Informatietechnologie in de zorg*, p. 10-11.
12. Het College voor Zorgverzekeringen (CVZ) schat de besparing van een volledig elektronische afhandeling van declaraties op een bedrag tussen de 3 en 30 miljoen; zie het rapport *Resultaatgericht de administratieve lasten reduceren; aanpak van de declaratiecasus* (28 augustus 2003) dat het CVZ op verzoek van minister Hoogervorst opstelde.
13. Uit de evaluatie van de proef die in opdracht van het NIVEL (Nederlands instituut voor onderzoek van de gezondheidszorg) is uitgevoerd: J.B.F. Hutten et al., *De zorgpas in Eemland*, p. 7.
14. *De zorgpas in Eemland*, p. 43.
15. *De zorgpas in Eemland*, p. 31-36.
16. Peter Verkooijen, ‘Proefdraaien. ICT in de zorg’, *FEM de week*, 23 oktober 2002.
17. *De zorgpas in Eemland*, p. 34.
18. *De zorgpas in Eemland*, p. 40-41.
19. ‘Proefdraaien. ICT in de zorg’.
20. JL van Duivenboden, ‘Randvoorwaarden voor een virtueel patiëntdossier, ervaringen uit de praktijk: het UPID project’, in *Huisarts, specialist en het Elektronisch Medisch Dossier*. Zie voorts <www.uzorg.nl/downloads?file=56&> en <www.nictiz.nl/kr_nictiz/uploaddb/downl_object.asp?atoom=1624&VolgNr=1>.
21. Gert-Jan van Boven, directeur van het NICTIZ, in een interview in *Computable*, 28 januari 2005; <http://www.computable.nl/artikels/archief5/d04sf5ia.htm>.
22. <www.antonius.net/geel/mijndossier/mijndossier.php>.
23. ‘Een Google voor patiëntinformatie’, *Computable*, 28 januari 2005,
24. Ernst & Young: *eMedicatiedossier*. p. 4.
25. Uit het persbericht van Ernst & Young naar aanleiding van het rapport. (Cursivering van mij.)
26. NICTIZ: *Het regioneel versnellingsprogramma. Lessons learned*, zonder datum, <www.nictiz.nl/kr_nictiz/default.asp?datoom=3578>.
27. Er zijn zeven HISsen; hoeveel ZISsen er precies zijn is niet te zeggen. Ziekenhuizen werken vaak met combinaties van (soms op maat gemaakte) pakketten. Er zijn ongeveer tien softwarebedrijven die een (gedeeltelijk) ZIS aanbieden. De functionaliteit daarvan loopt sterk uiteen. Sommige behelzen een

compleet ZIS, andere zijn niets dan een 'schil' om andere programma's heen. De voornaamste HISsen zijn Elias, MicroHis, Promedico en MacHis; de voornaamste ZISsen HisCom, Chipsoft en McKesson.

28. Marc Berg: *Bytes op recept?*, p. 32-33.
29. RVZ: *Standaardisering Elektronisch Patiënten Dossier*, p, 6.
30. VWS: *Van Elektronisch Medicatie Dossier naar Elektronisch Patiënten Dossier*. p. 4.
31. VWS: *Van Elektronisch Medicatie Dossier naar Elektronisch Patiënten Dossier*, p, 9.
32. Zie onder meer <www.nlm.nih.gov/archive/20040831/pubs/cbm/umlscbm.html>.
33. Veel ziekenhuizen zijn overigens in grote problemen gekomen door de verplichte invoering van DBC's: omdat de regelgeving verschillende keren werd veranderd, was veel software niet op tijd af of onvoldoende getest, wat weer tot gevolg had dat ze hun verrichtingen niet kunnen declareren. Diverse ziekenhuizen in Nederland kampen dientengevolge momenteel met liquiditeitsproblemen. 'Margreet Fogteloo, 'Gekmakend', *de Groene Amsterdammer*, 22 april 2005; Ester Schop, 'Softwarefouten bij invoering van DBC's', *Automatisering Gids*, 22 april 2005.
34. Ernst & Young: *eMedicatiedossier*, p. 16.
35. NICTIZ: *Zorgbrede terminologie*, zonder datum, <www.nictiz.nl/kr_nictiz/default.asp?datoom=1917>.
36. Standish Group: *The Chaos report (1994)*, <http://www.standishgroup.com/sample_research/chaos_1994_1.php>.
37. Barry Calogero, 'Who is to blame for ERP failure?', *Serverworld*, juni 2000; <http://www.serverworldmagazine.com/sunserver/2000/06/erp_fail.shtml>.
38. De lijst is gebaseerd op de wet Beroepen in de Individuele Gezondheidszorg (BIG). Het BIG-register wordt bijgehouden door het Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG), een uitvoeringsorgaan van het ministerie. Datzelfde orgaan houdt het UZI-register bij. Zie voorts <www.uzi-register.nl>. De open directory <www.uzi-register.nl/pdf/> bevat een aantal adviezen en handleidingen.
39. Het is niet duidelijk hoe lang een dergelijke toestemming geldt. In de oude situatie krijgt een andere zorgverlener na toestemming een kopie van (een deel van) iemands patiëntendossier, of een briefje met wat gegevens van diens arts. De toestemming tot inzage is derhalve eenmalig. In het UZI-register wordt bij mijn weten niet met een eenmalige toestemming gewerkt.
40. Een aantal ziekenhuizen werkt thans met Izemail, een systeem dat encryptie 'on the fly' biedt, en het mogelijk maakt om via beschermde e-mail over internet te communiceren, in plaats van via het (dure) Edifact-netwerk. Izemail werkt niet met de UZI-passen zelf, maar met de achterliggende PKI-infrastuctuur. Zie <*http://www.izecom.com/dutch.html*>.
41. In Zeeland is eind 2004 een proef met UZI-passen met pincodes succesvol afgesloten (proeftuin Zorgring Zeeland).
42. UZI-register: *Veel gestelde vragen*, <www.uzi-register.nl/fr_content.htm>.
43. RVZ: *Informatievoorziening in de zorg*, p. 37.
44. Advies van de Tafel: *Persoonsnummerbeleid in het kader van identiteitsmanagement*, Den Haag 2002, <http://www.stroomlijningbasisgegevens.nl/pdfs/Nummertafel.pdf> en <http://www.stroomlijningbasisgegevens.nl/pdfs/Nummertafelbijlage.pdf>.
45. Aanbiedingsbrief *Advies van de Tafel*, Kamerstukken II 2002-2003, 28 600 VII nr. 21, p. 1.
46. Aanbiedingsbrief *Advies van de Tafel*, p. 3-4.
47. *Fraudebestrijding in de zorg*, brief van de minister van VWS, 23 april 2004; Kamerstukken II 2003-2004, 28 828, nr. 14, p. 2.
48. Zie voorts <www.burgerservicenummer.nl>.
49. *Wijziging van de Algemene Wet Bijzondere Ziektekosten, de Wet op de toegang tot ziektekostenverzekeringen 1998 en de Ziekenfondswet in verband met invoering van een identificatieplicht bij het verkrijgen van zorg* (etc), nota naar aanleiding van het verslag, Kamerstukken II 2003-2004, 29 623 nr. 7, p. 6.
50. Zie <*www.digid.nl/burger/over-digid/wie-doen-mee/*>.

51. In een gezamenlijk persbericht op 2 juni 2005 bekritiseerden het NPCF en de RVZ de diverse softwaremakers van EPD's, omdat zij onvoldoende rekening zouden houden met het inzagerecht van patiënten, hun wens om zelf te bepalen wie erbij mag, na te gaan wie hun dossier heeft opgevraagd en er zelf gegevens aan toe te voegen.
52. RVZ: *Internetgebruiker en de veranderingen in de zorg*, Rijswijk 2005, p.21.
53. CBS: *Steeds meer mensen gebruiken medicijnen*, 21 april 2005, <www.cbs.nl/nl/publicaties/persberichten/2005/pb05n048.pdf>.
54. Ook Hoogervorst is die mening toegedaan, getuige onder meer zijn uitspraken in een debat in de Tweede Kamer op 23 maart 2005; zie het stenogram van de vergadering op <www.cvib.nl/cvibnew/050325110832.shtml>.
55. VWS: *Elektronisch medicatie dossier in de Zorg*, p. 10.
56. VWS: *ICT in de zorg. Implementatieplan EMD/WHD*, p. 4.
57. Brief van de minister van Binnenlandse Zaken over de implementatie van Public Key Infrastructuur, Kamerstukken II, 2002-2003, 28600, nr 7, p. 2.
58. *Elektronische Overheid (ELO), Eind-/Voortgangsrapportage 2002*, 1 april 2003, p. 9, <www.minbzk.nl/contents/pages/4391/voortgangsrapportage2002.pdf>.
59. Overleg vaste kamercommissies BiZa, EZ, Financiën, SoZa op 3 november 2004 over onder meer de notitie *Op weg naar de elektronische overheid*, Kamerstukken II, 2004-2005, 26387 nr. 24.
60. Ministerie van Binnenlandse Zaken: *Voortgangsrapportage programma Andere Overheid*, 17 december 2004, p. 19-20, <www.andereoverheid.nl/NR/rdonlyres/ 9073A6F7-0B54-4339-BC15-228C0BDA8001/0/Voortgangsrapportage.pdf>.
61. Sociale Verzekeringsbank: *Meerjarenplanning 2005 t/m 2009*, Amstelveen, september 2004, p. 15.
62. UZI-register: *Veel gestelde vragen*, <www.uzi-register.nl/fr_content.htm>.
63. CPB: *Privacy bij ICT in de zorg*, ZM Magazine nr. 11, november 2002, p. 6, <www.cbpweb.nl/downloads_artikelen/art_tho_2002_ict_zorg.pdf?refer=true&theme=purple>.
64. Aanbiedingsbrief bij *Advies van de Tafel*, Kamerstukken II 2002-2003, 28 600 VII nr. 21, p. 3-4.
65. Kamerstukken 29 441 e.v., <www.eerstekamer.nl/9324000/1f/j9vvgh5ihkk7kof/vguza935lou9>.
66. RVZ: *Standaardisering Elektronisch Patiënten Dossier*, p. 2.
67. Ibid.
68. IGZ: *Jaarrapport 2002*, p. 77.
69. IGZ: *Jaarrapport 2001*, p. 86.
70. IGZ: *Jaarrapport 2002*, p. 76 en p. 103.
71. IGZ: *Jaarrapport 2003*, p. 79. De enige literatuur waarnaar de Inspectie ter onderbouwing in beide jaarrapporten verwijst, is het boek *To err is human: towards a safer health system* onder redactie van Linda Kohn, Janet Corrigan, en Molla Donaldson van het Institute of Medicine, verschenen bij de National Academy Press, Washington 1999. Het boek is in zijn geheel te downloaden op <books.nap.edu/html/to_err_is_human/>.
72. IGZ: *Staat van de Gezondheidszorg 2004. Patiëntveiligheid*, p. 20.
73. Deze tabel is samengesteld uit de jaarrapporten van de IGZ; de cijfers voor persoonlijke fouten (door het medisch personeel), organisatorische fouten en toepassingsfouten zijn opgeteld. Problemen door productfouten zijn niet meegeteld, deze vallen buiten het domein van de *medische* missers. De categorie 'onbekend' werd in 2000 niet gevoerd.
74. IGZ: *Staat van de Gezondheidszorg 2004*, p. 7; cursivering van mij.
75. IGZ: *Tienduizenden mensen per jaar krijgen recept dat schadelijk kan zijn*, persbericht 20 januari 2005, <www.igz.nl/standaard.php?pagid=377>.
76. Persbericht NPCF en NICTIZ: *Gebrekkige communicatie tussen zorgverleners leidt tot veel medische fouten*, 19 februari 2004, <www.nictiz.nl/kr_nictiz/uploaddb/downl_object.asp?atoom=2593&VolgNr=5>.
77. TNS NIPO: *Fouten worden duur betaald. Een onderzoek naar medische overdrachtsfouten*, februari 2004,

<www.nictiz.nl/kr_nictiz/uploaddb/downl_object.asp?atoom=2593&VolgNr=7>. Voorafgaand aan dit cijfermatige onderzoek werd een kwalitatief onderzoek uitgevoerd, TNS NIPO: *Patiënten over fouten in medische informatie overdracht. Een verkennend onderzoek*, december 2003, <www.nictiz.nl/kr_nictiz/uploaddb/downl_object.asp?atoom=2593&VolgNr=8>.

78. 'Twijfel over onderzoek overdrachtsfouten. Instellingen en artsen zijn in het geheel niet bevraagd,' *Medisch Contact*, 3 maart 2004, <www.wcs-nederland.nl/nieuws/toonmeer.php?id=374>.
79. Zelfs daarbij kun je je afvragen of een EPD nu wel de zaligmakende oplossing is. In het papieren dossier staat immers óók aangegeven welke nier dient te worden uitgenomen, en toch werd die informatie over het hoofd gezien. Beter lijkt het om, zoals sommige ziekenhuizen tegenwoordig doen, met watervaste viltstift het zieke lichaamsdeel te markeren.
80. H Buurma, PGAM de Smet, OP van den Hoff', ACG Egberts: 'Prescriptiewijzigingen door openbare apotheken. Aard, frequentie en determinanten', *Pharmaceutisch Weekblad*, 136 (2001) 1159-60.
81. Overgenomen uit Marc Berg: *Bytes op recept?*, p. 5.
82. WJ van der Kam, B Meyboom de Jong, TF Tromp, PW Moorman en J van der Lei: 'Effects of electronic communication between the GP and the pharmacist. The quality of medication data on admission and after discharge', *Family Practice*, 18 (2001) 605-609.
83. 'Apotheker op afstand ziet fouten niet', *NRC Handelsblad* 1 december 2004, <www.knmp.nl/leden/pers/extra.asp?mID=4776&rID=1717&inhoud=1www.knmp.nl/leden/pers/extra.asp?mID=4776&rID=1717&inhoud=1>.
84. 'Hoogervorst wil diagnose op recept', *de Volkskrant* 17 maart 2005.
85. IGZ: *ICT in ziekenhuizen*, p. 3.
86. IGZ: *ICT in ziekenhuizen*, p. 9.
87. United States Pharmacopeia: *Computer entry a leading cause of medication errors in US heath systems. Percentage of reported errors steadily increase from 1999 to 2003*, persbericht USP 20 december 2004, <vocuspr.vocus.com/VocusPR30/Publish/148/vcsPRAsset_148_95578_%7B354B19F2-1F7A-447D-A81A-604A7EAF1D4E%7D_MedMarx_Teleconference_Media_Kit.pdf>; 'Data entry is a top cause of medication errors', *AMNews* 24 januari 2005, <www.ama-assn.org/amednews/2005/01/24/prsa0124.htm>.
88. Peter C Smoth et. al.: 'Missing Clinical Information During Primary Care Visits', *Journal of the American Medical Association*, 5 (2005) 565-571; abstract op <jama.ama-assn.org/cgi/content/abstract/293/5/565>.
89. 'Hospital revives its "dead" patients', *Baseline*, 10 februari 2003, <www.baselinemag.com/article2/0,3959,880881,00.asp>.
90. Ross Koppel et. al.: 'Role of computerized physician order entry systems in facilitating medical errors', *Journal of the Americam Medical Association*, 10 (2005) 1197-1203.
91. Zie ook het prachtige boekje *De nacht schreef rood.*
92. Zie bijvoorbeeld het rapport van de IGZ: *ICT in ziekenhuizen*, en Arjen Kamphuis: *Baas over eigen bits? ICT in de Nederlandse zorg*, niet gepubliceerd.
93. CBS persbericht: 'Helft bedrijven lijdt schade door computervirussen', 20 juni 2005, <http://www.cbs.nl/nl/publicaties/artikelen/algemeen/webmagazine/artikelen/2005/1729k.htm>.
94. McAfee persbericht, 'McAfee AVERT Reports That Top Threats for Q2 2005 Include Money Making Schemes and a Rise in BOTS and Spyware', 11 juli 2005, <http://www.mcafeesecurity.com/us/about/press/mcafee_enterprise/2005/20050711_182503.htm>.
95. 'NI health trusts hit by computer virus', *BBC News* 1, november 2001, <news.bbc.co.uk/1/hi/northern_ireland/1633119.stm>.
96. 'Got paper? Beth Israel Deaconess copes with a massive computer crash', *Boston Globe*, 26 november 2002, <www.bnug.org/drhal.htm>.
97. 'Computer viruses afflict hospitals, which learn to cope', *Health-ITWorld* 2003, <www.health-itworld.com/enewsarchive/e_article000183662.cfm>.
98. SUN's Healthcare Community,

<www.sun.com/br/healthcare_1014/feature_virus.html>.

99. 'Computer virus affects VUMC', *The Reporter*, 31 januari 2003, <www.mc.vanderbilt.edu/reporter/?ID=2499>.
100. 'Toronto public health computer accidentally erases records', *RISKS Digest*, 10 maart 2003, <catless.ncl.ac.uk/Risks/22.62.html>.
101. 'Virus hits hospital systems', *BBC News*, 22 augustus 2003, <news.bbc.co.uk/2/hi/uk_news/scotland/3174173.stm>
102. Sasser Worm Impacted Businesses Around the World', *TechWeb*, 7 mei 2004, <www.techweb.com/wire/26804909>.
103. 'Computer Virus Sasser Spreads Worldwide', *Arirang News*, 4 mei 2004.
104. Zie de beschrijving van SirCam in de McAfee virusbibliotheek, <vil.nai.com/vil/content/v_99141.htm>.
105. Michel Bouquet in een telefonisch interview, 17 maart 2005.
106. 'Een piepende en krakende PC', *Huisarts Vandaag*, 3 juli 2004, <www.huisartsvandaag.nl/content/view/3957/>.
107. '$100K Reward for Stolen ID Data', *Wired News*, 2 januari 2003, <wired-vig.wired.com/news/privacy/0,1848,57045,00.html>;'Security breach', *Palo Alto Weekly, 25* juni 2003, <www.paloaltoonline.com/weekly/morgue/2003/2003_06_25.wire25.html>; 'A tough lesson on medical privacy', *SFGate.com*, 22 okrober 2003, <www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G1.DTL>; 'Drug histories exposed', *RISKS Digest*, 26 januari 2005, <catless.ncl.ac.uk/Risks/23.68.html>.
108. Jelle Wijkstra, 'Dwing overheid tot herbezinning', *Automatisering Gids* 27 mei 2005.

Literatuur

- Marc Berg e.a., *Bytes op recept? Medicatiesystemen in de specialistische zorg*, Rotterdam 2002, p. 5.
- Ernst & Young: *eMedicatiedossier. Resultaten van het onderzoek naar de status en voortgang van de invoering van het eMedicatiedossier in Nederland*, juni 2005.
- JBF Hutten et al., *De zorgpas in Eemland. Ervaringen en meningen van betrokkenen omtrent de elektronische overdracht van gegevens via het zorg informatie netwerk tijdens de proef in de regio Eemland*, NIVEL, Utrecht 2002.
- IGZ: *ICT in ziekenhuizen. Beveiliging van informatie nog onvoldoende voor een betrouwbare papierloze patiëntenzorg. Een inventariserend onderzoek bij twintig ziekenhuizen, uitgevoerd najaar 2003*, Den Haag, augustus 2004.
- IGZ: *Jaarrapport 2001*, Den Haag, mei 2002.
- IGZ: *Jaarrapport 2002*, Den Haag, juni 2003.
- IGZ: *Jaarrapport 2003*, Den Haag, juni 2004.
- IGZ: *Staat van de Gezondheidszorg 2004. Patiëntveiligheid: de toepassing van geneesmiddelen en medische hulpmiddelen in zorginstellingen en thuis*, Den Haag, december 2004.
- Rathenau Instituur: *De nacht schreef rood. Informatisering van zorgpraktijken*, Rathenau, Den Haag 1998.
- RVZ: *Informatietechnologie in de zorg*, Zoetermeer 1996. *Deel 1: Advies* en *Deel 2: Achtergronden.*
- RVZ: *Internetgebruiker en de veranderingen in de zorg*, Rijswijk 2005.
- RVZ: *Standaardisering Elektronisch Patiënten Dossier*, Zoetermeer, 17 februari 2005.
- Symposiumverslag *Huisarts, specialist en het Elektronisch Medisch Dossier: EMD2002*, Instituut Medische Informatica Erasmus Universiteit, Rotterdam 2003.
- VWS: *ICT in de zorg. Implementatieplan EMD/WHD*, nota minister Hoogervorst van 3 juni 2005 (in de wandeling: het 'eerste spoorboekje'); Kamerstukken 2004-2005 II, 27529 nr. 15.
- VWS: *Informatie- en Communicatietechnologie (ICT) in de Zorg*, nota minister Borst , 28 november 2000, Kamerstukken II 2000-2001, 27 529, nr 1.
- VWS: *Informatievoorziening in de zorg*, nota minister Borst, 4 november 1997, Kamerstukken II 1997-1998, 25 669, nr 2.
- vws: *Van Elektronisch Medicatie Dossier naar Elektronisch Patiënten Dossier. Plan van aanpak* . nota minister Hoogervorst, 2 maart 2005.

Afkorting	*Betekenis*
AIS	apotheek informatiesysteem
BIG	wet Beroepen in de Individuele Gezondheidszorg
BSN	burger service nummer
DBC	diagnose-behandelcombinatie
DigiD	digitaal identiteitsbewijs
EMD	elektronisch medicatiedossier
eNIK	elektronische identiteitskaart
EPD	elektronisch patiëntendossier
EVS	elektronisch voorschrijfsysteem (voor medicatie)
GBA	gemeentelijke basisadministratie
HL7	health level 7, een internationale standaard voor uitwisseling van elektronische medische berichten
HL7 V3 RIM	HL7 versie 3 Reference Information Model, medisch gegevensmodel
HIS	huisartsen informatiesysteem
ICT	informatie- en communicatietechnologie
IGZ	Inspectie voor de Gezondheidszorg
LSP	landelijk schakelpunt (centrale verwijsindex patiëntengegevens)
NPCF	Nederlandse Patiënten Consumenten Federatie
NICTIZ	Nationaal ICT instituut in de zorg
RFID	radio frequency identification (herkenningschip)
RVZ	Raad voor de Volksgezondheid en Zorg
SOFI	sociaal en fiscaal nummer
UMLS	Unified Medical Language System
UPID	EPD-pilot Nieuwegein (Universele Patiënten Identificatie Database)
UZI	unieke zorgverleneridentificatie
WDH	elektronisch waarneemdossier voor huisartsen
ZAIS	ziekenhuisapotheek informatiesysteem
ZIN	zorg identificatienummer
ZIS	ziekenhuis informatiesysteem