

Privacy en het Elektronisch Patiënten Dossier **- belemmeringen bij de invoering -**

derdejaarsscriptie Informatiekunde

Stefan Koppejan

Titel:	Privacy en het Elektronisch Patiënten Dossier
Ondertitel:	belemmeringen bij de invoering
Auteur:	ing. S.A. Koppejan
Administratienummer:	S868136
E-mail:	s.a.koppejan@uvt.nl
Plaats:	Breda
Datum:	22 februari 2005
Begeleider:	dhr. M. Jeusfeld
Universiteit:	Universiteit van Tilburg
Opleiding:	Informatiekunde (verkort, vooropleiding: HIO)
Faculteit:	Faculteit Economie en Bedrijfswetenschappen

Voorwoord

Deze scriptie is geschreven in het kader van het vak “derdejaarsscriptie Informatiekunde” aan de Universiteit van Tilburg. Elke student dient gedurende zijn opleiding een scriptie te schrijven ter voorbereiding van de belangrijke afstudeerscriptie in het laatste jaar.

De oorsprong van mijn onderwerpkeuze ligt enkele jaren terug. Tijdens mijn afstuderen aan de HIO te 's-Hertogenbosch heb ik een afstudeeropdracht gedaan voor een aantal organisaties gelieerd aan Nederlandse ziekenhuizen en hoewel mijn opdracht niks te maken had met het Elektronisch Patiënten Dossier (EPD) was het in die periode dat het EPD voor het eerst mijn interesse wekte.

Ook tijdens mijn studie aan de UvT is het EPD verschillende malen voorbij gekomen in de colleges van e-commerce, e-business, informatiebeleid en business transformation & IT. Verder heb ik met twee andere personen voor het vak telematica een digitale scriptie gemaakt over telematica in de gezondheidszorg en ook daarin is het EPD de revue gepasseerd. Aangezien het voor mij tijd was om een derdejaarsscriptie te schrijven, en gezien de actualiteit van het onderwerp is mijn keuze dus gevallen op het EPD.

In eerste instantie wilde ik puur een scriptie over het EPD schrijven, maar na overleg met mijn begeleider, de Heer Jeusfeld, heb ik besloten om het privacyaspect erbij te betrekken omdat over het EPD alleen waarschijnlijk niet genoeg literatuur te vinden zou zijn.

Stefan Koppejan,
22 februari 2005

Inhoudsopgave

Samenvatting	5
1. Inleiding	6
2. Het Elektronisch Patiënten Dossier	7
3. Informatiestroom binnen een ziekenhuis	10
4. Privacy.....	12
5. EPD en Privacy	15
6. Conclusie.....	17
Referenties.....	18

Samenvatting

Deze scriptie gaat in op twee onderwerpen, het Elektronisch Patiënten Dossier (EPD) en het privacyaspect. Het EPD is een toepassing die ervoor zorgt dat alle medische gegevens van een patiënt uit verschillende disciplines centraal zijn opgeslagen en overal toegankelijk zijn, dit bevordert het hele medische proces. Gevolgen hiervan zijn kortere wachttijden en ligduur en lagere kosten. Ook zullen door het EPD bepaalde mogelijkheden voor medische toepassingen zoals digitale opslag en verwerking van röntgenbeelden goed benut kunnen worden.

Bij de behandeling van een patiënt zijn vele actoren betrokken. Het is belangrijk dat informatieoverdrachtmomenten goed worden vastgelegd, hiervoor is inzicht in en samenhang van medische processen nodig. Een adequate infrastructuur is nodig ter ondersteuning en om het berichtenverkeer zonder problemen te verwerken.

Met privacy wordt in deze scriptie digitale privacy bedoeld, er worden een aantal methoden besproken die privacy op het internet of op netwerken bevorderen. Aangezien dit niet genoeg is om alle klanten (in deze scriptie vooral patiënten) gerust te stellen is er wetgeving gecreëerd ter bescherming van de privacy van het individu.

Het EPD staat in Nederland nog aan het begin, in andere landen zoals de Verenigde Staten is men verder met de realisatie. Het privacyaspect is een van de grootste belemmeringen die de volledige realisatie van het EPD in de weg staat. Simpelweg omdat mensen bang zijn dat ze zullen worden aangetast in hun privacy door de komst van het EPD.

sleutelwoorden: *EPD, (digitale) privacy, informatiestroom, data, vertrouwen, wetgeving*

1. Inleiding

In de zomer van 2000 heeft het Universiteitsziekenhuis van Seattle bezoek gehad van een ongenodigde gast, het gaat om een Nederlandse hacker die zichzelf Kane noemt. Hij is binnengekomen via een niet voldoende beveiligde Linux server in de pathologieafdeling van het ziekenhuis. Hoge functionarissen van het medisch centrum van de Universiteit van Washington maakten bekend dat de hacker gebruikerswachtwoorden heeft gestolen en van ongeveer 5000 patiënten gegevensbestanden heeft gekopieerd.

Het medisch centrum had destijds al het vermoeden dat er iemand was geïnfilteerd in het netwerk en heeft toen stappen ondernomen om de hacker de toegang te ontnemen. Ze waren echter niet op de hoogte van het feit dat de er toen al bestanden waren gekopieerd. Daar kwamen ze pas achter nadat Kane de inbraak bekend had gemaakt bij Security-focus.com, een website uit San Mateo in Californië die zich richt op en bezig houdt met allerlei beveiligingsproblemen.

Kane ziet zichzelf duidelijk niet als een crimineel. Hij vindt dat hij meer een klokkenluider is en noemt zichzelf een ethische hacker die niks meer heeft gedaan dan het aantonen en bekend maken van de kwetsbaarheid van het systeem.

Wat Kane heeft gedaan is uiteraard – ondanks zijn misschien wel goede bedoelingen – niet goed te praten, maar het geeft wel in bepaalde mate aan waar deze scriptie over zal gaan. Deze situatie is simpelweg onaanvaardbaar aangezien er van een paar duizend patiënten zomaar strikt persoonlijke gegevens op straat zijn komen te liggen. De patiënten zijn aangetast in hun privacy omdat het betreffende ziekenhuis niet voldoende adequate beveiligingsmaatregelen heeft getroffen (Songini, 2000).

Ook in Nederland is men bezig met het ontwikkelen van een systeem waarin patiëntgegevens worden bijgehouden, het zogenaamde Elektronisch Patiënten Dossier (EPD). Maar de invoering hiervan gaat lang niet zo snel als van tevoren was gewenst. Dit heeft te maken met een aantal zaken zoals de hoge kosten, het vele werk en de organisatorische perikelen die komen kijken bij het aansluiten en ontwikkelen van de systemen en – zoals het voorbeeld hierboven al aangaf – het privacyaspect.

Deze scriptie gaat over het EPD met de nadruk op het privacyaspect. In het tweede hoofdstuk zal eerst het EPD wat nader worden bekeken. Daarna zal in het derde hoofdstuk worden ingegaan op de informatiestroom binnen een ziekenhuis. In hoofdstuk vier komt privacy aan de orde. In het vijfde hoofdstuk zullen het EPD en het privacyaspect samengenomen worden en wordt gekeken naar de hoofdvraag: *In hoeverre vormt het privacyaspect een belemmering voor de invoering van het EPD?* Als laatste volgt daarna de conclusie.

2. Het Elektronisch Patiënten Dossier

In Nederland bevindt het EPD zich nog in de beginfase, wel zijn er in ons land vele systemen die medische gegevens van patiënten hebben opgeslagen voor verschillende doeleinden. Enkele voorbeelden hiervan zijn het patiëntensysteem van de huisarts en van artsen en specialisten in het ziekenhuis. En ook de gegevens van fysiotherapeuten, tandartsen, psychologen, plastisch chirurgen, apothekers en zelfs de verzekeringsmaatschappij voor ziektekostenverzekering.

Het doel van het EPD is dat al deze systemen aan elkaar gekoppeld zijn en dat zorgverleners tegelijkertijd op elk tijdstip en ongeacht waar ze zich bevinden die informatie kunnen inzien die ze nodig hebben.

Volgens de sector Health Sciences van Ernst & Young (2002) ontwikkeld het EPD zich volgens een bepaald groeimodel. Het EPD wordt niet in één stap gerealiseerd maar volgt een aantal stadia, te weten een informatief, registratief en multidisciplinair stadium. Elke overgang naar een volgend stadium brengt uitbreiding van de functionaliteit of gebruikersgroep met zich mee. Binnen een informatief EPD is alleen inzage van patiëntgegevens mogelijk. Een registratief EPD biedt daarnaast ook registratiemogelijkheden van patiëntgegevens. Het volgende stadium van het groeimodel is een multidisciplinair geheel, waarbij vooral de zorgprocessen op elkaar worden afgestemd. In iedere fase treedt een verbetering van het zorgproces op, kwaliteit en inzicht verbeteren door verdere integratie in het zorgproces.

De sector Health Sciences van Ernst & Young heeft in 2002 een onderzoek uitgevoerd naar de status van de invoering van EPD's in Nederlandse ziekenhuizen¹. Hieruit kwam naar voren dat ziekenhuizen zelf vinden dat ze goed op weg zijn. 85% van de respondenten heeft invoering van EPD's opgenomen in het ICT-beleid. Bij 75% is men bezig met een pilot of andere testsituaties betreffende een informatief EPD. Van deze 75% heeft 35% van de respondenten het informatieve EPD reeds ziekenhuisbreed uitgerold. Ongeveer 10% van de respondenten heeft (beperkte) gegevensinvoer gerealiseerd. De meeste ziekenhuizen bevinden zich nog in de pilotfase, slechts eenderde van de ziekenhuizen is op dit moment bezig met daadwerkelijke ziekenhuisbrede implementatie van het EPD.

In de Verenigde Staten zijn ze verder met de invoering van verschillende EPD's maar dat zal geen verrassing zijn aangezien ze daar sowieso vooruitlopen wat betreft ICT voorzieningen. Er zijn reeds complete EPD's gerealiseerd die al in gebruik zijn genomen. Ze hebben in de VS meerdere systemen omdat het een enorm land is, niet te vergelijken met enig Europees land. De Amerikaanse benaming voor het EPD is *Electronic Patient Records* (EPR). Er volgen nu enkele definities van een EPR:

Electronic Patient Records electronically maintain information about the lifetime health status and healthcare of individuals. Reaching beyond the mere automation of paper-based records, EPRs encompass the entire scope of health information in all media forms, and facilitate retrieval of medical history, current medications, laboratory test results, and X-ray images (Lorence, Richards & Spink, 2002).

¹ Ernst & Young interviewde voor het onderzoek 48 ziekenhuizen, circa 50% van alle ziekenhuizen in Nederland.

EPR is a means to manage and integrate all types of clinical data. The information is collected, archived and distributed, introducing automated methods for traditional medical evidence recording. Above all, EPR represents the core element to accomplish new healthcare services with improved quality and efficiency (Costa, Gama, Oliveira & Silva, 2003).

The electronic medical record contains medically-related information of a patient for a specific enterprise such as a hospital, whereas the electronic patient record contains all the health-care-related information on one person. The latter thus combines several enterprise-based electronic medical records concerning one patient (Eloff & Smith, 1999).

Zoals in de definities is terug te vinden houdt het EPD alle informatie bij over de medische geschiedenis van een persoon. Het archiveert en integreert de gegevens van verschillende afdelingen zodat alles snel en compleet terug te vinden is. Het EPD heeft veel meer mogelijkheden dan de oude papieren versie, bijvoorbeeld het opslaan van röntgenfoto's en hartfilmpjes.

Het werken met een centraal dossier is efficiënter dan het bijhouden van verschillende afzonderlijke dossiers. Het centraal opslaan van gegevens ondersteunt en optimaliseert het proces van de patiëntenzorg als geheel. De verschillende functies die het zorgproces ondersteunen worden met elkaar geïntegreerd. Hierdoor wordt de afstemming tussen de verschillende disciplines van de zorg verbeterd. Ook werkt het EPD kwaliteitsverhogend, onder andere doordat de instructies en rapportages beter te lezen zijn. Verder zullen op de langere termijn de kosten aanzienlijk afnemen omdat er minder personeel nodig is en er minder fouten zullen optreden, ook kunnen er meer patiënten in een bepaalde periode geholpen worden.

In Anderson (2000) wordt aangegeven dat zowel in Europa als de VS de vraag naar EPD's stijgt. Medische gegevens zijn niet alleen nodig om patiënten te helpen maar zijn ook belangrijk voor ondersteuning van onafhankelijke onderzoeken en het handhaven van de volksgezondheid. Verder valt in toenemende mate – bij reeds geïmplementeerde EPD's – te zien dat patiënten steeds vaker via een EPD op zoek gaan naar medische informatie, of dat ze toegang hebben tot hun eigen medische gegevens. Ook is het mogelijk om te communiceren met hulpverleners en kan het EPD hulp bieden bij het leven met een chronische ziekte.

Het is de bedoeling dat er in Nederland over een paar jaar één groot transmuraal systeem is. Dit is ook bij de meeste andere Europese landen het doel. Je ziet nu al dat er een behoorlijk aantal ziekenhuizen zijn die al EPD's in het klein in huis hebben. Het gaat dan vaak om enkele afdelingen binnen een ziekenhuis waar veel patiëntendoorloop is. Ook huisartsen zijn steeds vaker aan een ziekenhuis verbonden, het gaat dan meestal om een ziekenhuis in de regio (Ellingsen & Monteiro, 2003).

Op basis van het eerder genoemde onderzoek van Ernst & Young valt te concluderen dat ziekenhuizen in Nederland op dit moment niet klaar zijn om de verwachtingen die in de samenleving heersen op het gebied van het opzetten van transmurale EPD's waar te maken. De grootste problemen zijn dat er te weinig ervaring is met de interne EPD's, de onderliggende infrastructuur niet voldoende is en het koppelen van de EPD's van diverse zorgverleners nog veel werk behelst.

Volgens Costa et al. (2003) is het momenteel een groot probleem om alle heterogene en autonome systemen die ook nog eens vaak gedistribueerd zijn probleemloos samen te laten werken. Het ligt daarom in de verwachting dat in de nabije toekomst de gezondheidszorg in rap tempo gebruik zal gaan maken van de grote mogelijkheden van webtechnologie en het internet om zo snel, goedkoop en op grote schaal medische data te delen.

Voor de patiënt wordt er veel verbeterd, twee grote ergernissen worden volgens Breed & Teeuw (1995) met de invoering van het EPD opgelost. Ten eerste vindt een patiënt het vervelend om aan elke specialist zijn of haar verhaal opnieuw te moeten vertellen. Deze ergernis is het gevolg van de organisatiestructuur van de zorgsector. De bestaande structuur zit fragmentarisch in elkaar en zodoende zullen de gegevens van de huisarts niet bekend zijn bij anderen in de zorgsector. Het komt ook wel eens voor dat bepaalde onderzoeken opnieuw worden uitgevoerd omdat onbekend is dat het onderzoek al elders is uitgevoerd. Een ander opmerkelijk feit is dat dezelfde informatie meerdere keren opgeslagen kan zijn in verschillende dossiers. Deze dossiers kunnen hierdoor verouderde informatie bevatten waardoor er inconsistenties ontstaan, dit kan veel verwarring veroorzaken.

Een tweede ergernis zijn de eindeloze wachttijden. Men staat voor een bepaalde medische handeling vaak weken – of zelfs langer – op de wachtlijst. Voordat men aan de beurt is, kan een behandeling al niet meer nodig zijn. Bovendien als blijkt dat zorgverlener of patiënt niet de goede voorbereiding heeft getroffen voor de medische handeling, of indien er een bepaalde handeling verkeerd wordt uitgevoerd of zelfs vergeten, dit mogelijk resulteert in een nieuwe plaatsing op de wachtlijst. Ook stelt de individuele zorgverlener bij het plannen van zijn patiënten zijn eigen agenda te veel voorop, de patiënt moet zich aanpassen aan de zorgverlener.

In Tabel 1 wordt ter afsluiting van dit hoofdstuk een overzicht gepresenteerd van de voor- en nadelen van een EPD. Enkele nadelen zijn hiervoor nog niet besproken en zullen terugkomen in de volgende hoofdstukken.

Tabel 1: voor- en nadelen van een EPD

<i>voordelen</i>
<ul style="list-style-type: none"> ▪ toegang onafhankelijk van plaats en tijd ▪ integratie functies zorgproces ▪ verbeterde leesbaarheid/duidelijkheid ▪ lagere kosten (op lange termijn) ▪ er zullen minder fouten optreden ▪ capaciteit voor meer patiënten ▪ nieuwe mogelijkheden op het gebied van informatie en communicatie ▪ mogelijkheden tot uitwisselen en delen van medische data
<i>nadelen</i>
<ul style="list-style-type: none"> ▪ realisatie duurt lang ▪ realisatie is kostbaar ▪ verlies/inconsistentie/corruptie van data ▪ eventuele veiligheidsperikelen ▪ waarborging van privacy

Meer informatie over de in dit hoofdstuk beschreven onderwerpen is te vinden in Elberg (2001) en Safran & Goldberg (2000).

3. Informatiestroom binnen een ziekenhuis

Bij de medisch-farmaceutische verzorging van een patiënt zijn vele actoren betrokken. Dit gegeven resulteert in vele informatieoverdrachtsmomenten. Om optimale zorg te waarborgen dient deze informatieoverdracht tijdig plaats te vinden en dient de informatie volledig, transparant en relevant te zijn (Bemmel, 1997). In de huidige situatie met lokale schriftelijke dossiers en geschreven informatieoverdracht kan niet aan deze eisen worden voldaan. In het perspectief van de beschikbare informatietechnologie is het creëren van een EPD volgens de TRANSFORM groep (2003) de passende oplossing.

Inzicht en samenhang in processen gebaseerd op medisch-farmaceutische informatie benodigd in de zorgketen ontbreekt. Hierdoor wordt een zinvolle inrichting van het EPD belemmerd. Een oplossing hiervoor wordt gezocht in het project TRANSFORM [1]. Het doel van dit project is het verbeteren van de beschikbaarheid en toegankelijkheid van de medicatiegegevens van de patiënt zodat continuïteit en kwaliteit van de medische en farmaceutische zorgverlening aan de patiënt gewaarborgd kan worden.

Het volgende gedeelte van dit hoofdstuk gaat over het doorlopen van de zorgketen door een patiënt zoals dit op de website van TRANSFORM is beschreven.

Vanaf het moment van ervaren van een klacht ondergaat een patiënt vele activiteiten bij de behandeling hiervan (het doorlopen van de zorgketen). In eerste instantie wordt een bepaald verschijnsel niet als klacht ervaren. Wellicht zal door de patiënt eerst getracht worden zelf de klacht te verhelpen. Vervolgens wordt de huisarts geraadpleegd. Deze kan verwijzen naar een specialist en deze kan vervolgens weer doorverwijzen naar andere deskundigen alvorens een goede diagnose en een behandelplan opgesteld kan worden. Dit kan eventueel leiden tot een ziekenhuisopname en een operatie. Na behandeling volgt herstel en ontslag uit het ziekenhuis.

In Tabel 2 worden de (mogelijke) stadia in het doorlopen van de zorgketen van begin tot eind nog eens overzichtelijk weergegeven.

Tabel 2: stadia zorgketen

<i>stadium</i>	<i>activiteit</i>
1	klacht
2	zelf verhelpen
3	huisarts
4	specialist 1
5	specialist N (*)
6	opname
7	operatie
8	herstel/verpleging
9	ontslag

(*) = meerdere mogelijk

Een belangrijk punt bij het verlenen van zorg door vele behandelaars en verzorgenden binnen de zorgketen is het beschikken over de juiste informatie op het juiste moment. Door ieder van de behandelaars en verzorgenden wordt medische informatie vastgelegd. Indien anderen bij de behandeling worden betrokken dient deze informatie overgedragen te worden aan, en toegankelijk te zijn voor de andere behandelaar. Deze overdrachtmomenten zijn derhalve van cruciaal belang voor het verlenen van kwalitatief goede zorg.

De zorg wordt steeds procesmatiger aangepakt, samen met de nieuwe technologische ontwikkelingen leidt dit tot complexe ICT-structuren. Binnen één instelling is tegenwoordig vaak sprake van vele platforms, netwerken, applicaties en koppelingen, die onderling gegevens moeten uitwisselen. Het zorgproces is daarvan voor een groot deel afhankelijk. Een visie op de totale informatiestroom is daarom noodzakelijk. Technisch gezien moet er een infrastructuur zijn die het berichtenverkeer adequaat af kan handelen zonder het zorgproces te verstoren [2].

Meer informatie over de in dit hoofdstuk beschreven onderwerpen is te vinden in De Meyer et al. (1998) en Toussaint & Lodder (1998).

4. Privacy

In het woordenboek staat privacy omschreven als “privé-leven”. Iedereen heeft recht op en behoefte aan privacy. Een aantal bekende voorbeelden die duidelijk met privacy te maken hebben zijn: het niet openen van post voor een ander, het bouwen van een schutting om je tuin omdat anders iedereen naar binnen kijkt en het geheim houden van je telefoonnummer en financiële zaken.

Een andere vorm van privacy is digitale privacy, het gaat hier om privacy op netwerken en internetten. Het is deze vorm van privacy die in deze scriptie naar voren komt. Gebruikers hechten veel belang aan hun privacy. Ze maken zich vooral zorgen over welke persoonlijke informatie door wie kan worden gezien, of ze berichten kunnen uitwisselen zonder dat iemand anders meekijkt en of het mogelijk is anoniem berichten te versturen en hoe dat moet [3].

Het is een feit dat de wereld de laatste tijd een minder betrouwbare plaats is geworden wat betreft het doen van zaken. Recente ontwikkelingen hebben het wereldwijde economische en competitieve landschap veranderd. Topmanagers opereren in een klimaat met ongekende mogelijkheden, onzekerheden en een gebrek aan vertrouwen (Consumer Products Ernst & Young 2002).

Volgens de sector Consumer Products van Ernst & Young (2002) is de manier om de klant te winnen het aanbieden van producten die meer waarde hebben voor de klant. Maar om er achter te komen wat voor producten meer waarde hebben voor consumenten moet je de klant kennen. Daarvoor is het verkrijgen van persoonlijke informatie zeer belangrijk. Juist het uitwisselen van persoonlijke informatie wordt door klanten vaak geweigerd op grond van hun recht op privacy.

Uit een gezamenlijk online onderzoek² van Ernst & Young, Privacy & American Business en het Amerikaanse Instituut van Gecertificeerde Publieke Accountants (AICPA) gedurende 2001 en 2002 is gebleken wat de grootste angsten van consumenten met betrekking tot privacy zijn. De drie meest genoemde angsten zijn:

- dat vertrouwelijke gegevens zonder toestemming worden doorgesluisd aan derden
- dat transacties onveilig zijn
- dat hackers persoonlijke gegevens stelen

De meeste webgebruikers willen er zeker van zijn dat de persoonlijke informatie die ze gebruiken bij niemand anders terecht komt zonder uitdrukkelijke toestemming. Een jaarlijks onderzoek uitgevoerd door het Graphics, Visualisation and Usability Center van het Technologisch Instituut in Georgia (VS) geeft aan dat 70% van de webgebruikers zichzelf niet registreert op websites vanwege zorgen over privacy. Het grootste gedeelte van deze mensen geeft ook aan dat wanneer privacy gegarandeerd zou worden ze dit wel zouden doen.

In een open netwerk zoals het internet is het noodzakelijk privéboodschappen, vooral e-commerce transacties, te versleutelen, dit wordt encryptie genoemd. Ook e-mails kunnen worden versleuteld zodat alleen een ontvanger met een juiste sleutel het bericht kan lezen.

² Voor het gezamenlijke (online) onderzoek zijn 1529 volwassenen geïnterviewd.

Verder is er ook nog de mogelijkheid van het meesturen van een digitale handtekening die ervoor zorgt dat niemand ongemerkt gegevens kan wijzigen terwijl een bericht op weg is naar de ontvanger. Soms kan het ook nodig zijn om een anonieme boodschap te versturen, bijvoorbeeld wanneer je een misdaad wilt aangeven. Dit wordt vaak opgelost door gebruik te maken van een site die een boodschap verstuurt vanaf zijn eigen adres. Dit wordt ook wel een remailer genoemd. Helaas wordt deze methode tegenwoordig vaak misbruikt door verzenders van spam³.

Deze genoemde methoden werken prima, net zoals legio niet genoemde methoden die nog beschikbaar zijn. Het probleem met deze methoden is dat niet iedereen ze gebruikt en je er dus niet zomaar vanuit kunt gaan dat als je iets bestelt of een bericht verstuurt alles veilig gaat. Dit is geen goede zaak voor internetondernemers en andere bedrijven die online zaken doen, of voor instanties die met gegevens werken die via internet worden verkregen en verstuurd. Op initiatief van deze ondernemingen en instanties is er lijst opgesteld met de wensen van klanten (gebruikers die online betalen of ergens persoonlijke data online hebben staan) met betrekking tot privacy. Deze lijst ziet er als volgt uit:

- duidelijkheid over het soort informatie dat wordt verzameld, waar het voor gebruikt gaat worden en of het wordt doorgespeeld naar derden
- controle over het feit dat hun informatie hergebruikt mag worden, en door wie
- de mogelijkheid tot het bekijken en veranderen van bestanden met persoonlijke informatie

Het bovenstaande lijstje vormt de basis voor de meeste wetgeving op het gebied van privacy over de hele wereld. In Europa is men eind negentiger jaren met wetgeving gekomen, gebaseerd op de *Data Protection Directive* van de Europese Unie (EU). De nieuwe regels gaan door het leven met de naam: *Directive on privacy and electronic communications*. Het Europese Parlement omschrijft deze nieuwe set regels als volgt:

Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (European Parliament, 2002).

Bij deze Europese benadering is het de bedoeling alle persoonlijke informatie te beschermen, op andere plaatsen en met name in de VS is de benadering meer specifiek gericht op een bepaalde commerciële sector. Eén van deze sectoren is de gezondheidszorg. De Amerikaanse versie van de *Directive on privacy and electronic communications* toegepast op de gezondheidszorg heet: *HIPAA*, de omschrijving luidt als volgt:

The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (HHS, 2003).

Het valt te verwachten dat er heel wat inhoudelijke verschillen bestaan tussen deze twee varianten – in ogenschouw nemende dat het puur over zaken gaat die betrekking hebben op de gezondheidszorg. De strekking van beide is echter hetzelfde: het voorzien in wetgeving die de privacy van het individu beschermt (Robertson & Sarathy, 2003; Hinde, 2003).

³ Mail die in grote hoeveelheden (bulk) en ongevraagd (unsolicited) wordt verstuurd [4].

Volgens Deloitte & Touche (2003) bestaat er een tegenstelling tussen de begrippen privacy en beveiliging, maar ook een overlapping, dit kan leiden tot een beveiliging-privacy paradox. Het in stand houden van de voorschriften of wensen van het ene aspect kan serieuze schade toebrengen aan het andere aspect. Dit houdt in dat wanneer rekening wordt gehouden met privacy dit ten koste kan gaan van de beveiliging, en andersom.

In Nederland is eind 2001 de nieuwe Wet bescherming persoonsgegevens (WBP) in werking getreden die de privacy van persoonsgegevens moet waarborgen. De WBP verving de tot dan toe geldende Wet persoonsregistratie (WPR). De WBP geeft, net als de WPR, algemene wettelijke bescherming van de privacy van personen. Een belangrijk verschil tussen beide wetten is dat de WPR eisen stelde ten aanzien van persoonsregistraties, terwijl de WBP eisen stelt aan de manier waarop de persoonsgegevens worden verwerkt – van het verzamelen tot aan het vernietigen van persoonsgegevens (Huizing, 2003).

Meer informatie over de in dit hoofdstuk beschreven onderwerpen is te vinden in Allaert et al. (2004), Crichard (2003), Sadan (2001) en Seničar et al. (2003).

5. EPD en Privacy

De laatste jaren is men pas echt gaan inzien wat het belang is van het verzamelen, elektronisch opslaan en gebruiken van informatie in de gezondheidszorg. De informatie kan gebruikt worden door patiënten en artsen om goed geïnformeerde keuzes te maken, door specialisten om de juiste medische zorg te kunnen verlenen en door verzekeringsmaatschappijen, fondsen en de overheid om kosten te beheersen en kwaliteit te monitoren (Anderson, 2000).

Het verzamelen, opslaan en gebruiken van deze grote hoeveelheden persoonlijke informatie brengt wel een probleem met zich mee. Rindfleisch (1997) vraagt zich af of het mogelijk is te voorzien in de informatie die is benodigd door de nieuwe vormen van medische zorg en tegelijkertijd de privacy te beschermen.

Recente debatten over wetgeving voor privacy van persoonlijke informatie in de gezondheidszorg, software voorschriften en telematica in de gezondheidszorg hebben aangegeven dat een oplossing niet snel gevonden zal worden. Het probleem is systematisch en komt voort uit routinematig handelen. Ook de informatiestromen zitten diep in de organisaties en de medische sector als geheel geslepen.

De digitaal opgeslagen informatie wordt gebruikt door geautoriseerde gebruikers, maar toch wordt de informatie niet alleen gebruikt voor patiëntenzorg en financiële doeleinden. De informatie wordt ook gebruikt door secundaire gebruikers zoals het medisch onderwijs, verschillende onderzoeks- en ontwikkelingsinstituten, instanties rondom de volksgezondheid en commerciële doeleinden zoals het ontwikkelen van nieuwe producten (medicijnen en apparatuur) en het vinden van nieuwe marketingtechnieken (Gostin, 2001). En hoewel er vele gevaren schuil gaan achter het internet komt de grootste bedreiging van de privacy vanuit de zorgverlenende instellingen en de instellingen die toegang hebben tot de informatie vanwege de eerder genoemde secundaire doeleinden.

De invoering in Nederland loopt veel trager dan verwacht, alle ziekenhuizen zijn wel gestart met het automatiseren van het primaire zorgproces maar bij slechts een kwart is concrete vooruitgang te constateren aldus de sectorgroep Health Sciences van Ernst & Young [5]. De tijdschema's voor de invoering van het EPD van ziekenhuizen komen niet overeen met de verwachtingen van het Ministerie van Volksgezondheid en het Nationaal ICT Instituut in de Zorg.

Er blijkt verder dat vrijwel alle gegevensinvoer nog steeds via de traditionele manier gebeurt, al bestaan er zoals al eerder opgemerkt wel verschillen tussen afdelingen binnen ziekenhuizen. Een opmerkelijk resultaat van het onderzoek is dat de meeste ziekenhuizen geen leveranciersselectie uitvoeren, maar het EPD uitbesteden aan de leverancier van wie zij hun bestaande informatiesystemen hebben. Ook heeft een meerderheid van de ondervraagde ziekenhuizen (55%) geen pakket van wensen en eisen voor het EPD opgesteld. Naar de mening van Ernst & Young is dat niet verstandig, omdat het ontbreken van een dergelijk pakket in het vervolgtraject kan leiden tot problemen.

Het ligt dus in de verwachting dat de invoering van het (transmurale) EPD nog op zich laat wachten. Eerst zullen alle problemen wat betreft handhaving van privacy moeten worden overwonnen, pas dan zal de angst van de mensen verdwijnen. De Nederlandse overheid kan helpen door veel te investeren in ICT en voorlichting te verzorgen over de voordelen van het EPD. Op deze manier kan mogelijk een kentering teweeg worden gebracht in de houding van de bevolking jegens het digitaal opslaan en gebruiken van persoonlijke gegevens [6].

6. Conclusie

Het EPD is op papier de wens van elke zorgverlenende instantie. Het EPD is een koppeling van alle verschillende zorgondersteunende en medische systemen en zorgt ervoor dat zorgverleners tegelijkertijd op elk tijdstip en ongeacht waar ze zich bevinden die informatie kunnen inzien die ze nodig hebben. In Tabel 1 (Hoofdstuk 2) worden de voor- en nadelen van een EPD weergegeven.

In dit paper is een aantal obstakels dat de invoering van het EPD in de weg staat voorbij gekomen. Hier volgt een opsomming:

- veel verschillende pilots, weinig ziekenhuisbrede implementaties
- achterstand in ontwikkeling ICT (t.o.v. andere landen)
- te weinig ervaring met interne EPD's
- onderliggende infrastructuur is onvoldoende
- koppeling van verschillende systemen behelst enorm veel werk
- realisatie is tijdrovend en kostbaar
- inzicht en samenhang in processen in de zorgketen ontbreekt
- steeds meer complexe ICT-structuren

Een laatste – zeer belangrijk – obstakel is het privacyaspect. In dit paper is onderzocht in hoeverre het privacyaspect een belemmering vormt voor de invoering van het EPD. Uit het onderzoek is gebleken dat de volgende aan privacy gerelateerde aspecten de invoering van het EPD belemmeren:

- veranderende wereld
→ *ongekende mogelijkheden leiden tot onzekerheden en gebrek aan vertrouwen*
- gebrek aan vertrouwen
→ *nieuwe mogelijkheden, weinig affiniteit met ICT*
- gebrekkige beveiliging
→ *duidelijkheid, controle, toegangsrechten, beveiliging-privacy paradox*
- angst van consumenten
→ *informatie naar derden, gegevensdiefstal hackers, onveilige transacties*
- gebrekkige wetgeving
→ *net nieuw, verschillen tussen landen*
- gevaar van secundaire gebruikers
→ *secundaire gebruikers zijn groter gevaar dan internet*

Met de grote hoeveelheid persoonlijke informatie die elektronisch zal worden verzameld, opgeslagen en gebruikt, wordt het moeilijk de privacy van mensen te garanderen. Dit zorgt voor grote weerstand bij alles wat met elektronische gegevens te maken heeft, daarom heeft men wetgeving gecreëerd gebaseerd op de wensen van klanten. Deze staat echter nog maar aan het begin en zal constant moeten worden verbeterd.

Als er eenmaal een oplossing is voor de genoemde obstakels – en vooral het privacyaspect – zal de lancering van één nationaal transmuraal EPD over een aantal jaren een feit zijn. De gezondheidszorg zal zich daarom in de toekomst zorgen moeten gaan maken over andere zaken, want het probleem van de wachttijden en (te) lange ligduur zal met de invoering van het EPD opgelost zijn.

Referenties

- Allaert, F.A., Teuffel, G., Quantin, C., Barber, B. (2004). The legal acknowledgement of the electronic signature: a key for a secure direct access of patients to their computerised medical record. *International Journal of Medical Informatics* 73 239-242 (2004).
- Anderson, J.G. (2000). Security of the distributed electronic patient record: a case-based approach to identifying policy issues. *International Journal of Medical Informatics* 60 111-118 (2000).
- Bemmel, V. (1997). Handbook of Medical Informatics. M. A. Musen Editors. Springer (1997).
- Breed, N.F., Teeuw, W.B. (1995). Telematica in de gezondheidszorg. Twee visies op de toekomst. *TRC Report Series RS/95004* (2003).
- Costa, C., Gama, V., Oliveira, J.L., Silva, A. (2003). An integrated access interface to multimedia EPR. *International Congress Series* 1256 880-886 (2003).
- Crichard, M. (2003). Telecoms privacy directive – UK implementation. Privacy and electronic communications. *Computer Law & Security Report Vol. 19, No. 4, 2003*.
- Deloitte & Touche. (2003). The Security-Privacy Paradox. Issues, Misconceptions, and Strategies. (2003).
- Elberg, P.B. (2001). Electronic patient records and innovation in health care services. *International Journal of Medical Informatics* 64 201-205 (2001).
- Ellingsen, G., Monteiro, E. (2003). A Patchwork Planet: Integration and Cooperation in Hospitals. *Computer Supported Cooperative Work* 12: 71-95 (2003).
- Eloff, J.H.P., Smith, E. (1998). Security in health-care information systems – current trends. *International Journal of Medical Informatics* 54 39-54 (1999).
- European Parliament (2002). Directive 2002/58/EC. <http://europa.eu.int>, geraadpleegd 1 mei 2004.
- Gostin, L.O. (2001). Health Information: Reconciling Personal Privacy with the Public Good of Human Health. *Health Care Analysis* 9: 321-335 (2001).
- Hinde, S. (2003). Privacy legislation: a comparison of the US and European approaches. *IS Audit* 0167-4048/03.
- Huizing, N. (2003). Bescherming persoonsgegevens. *Health Sciences Digest No .1, februari 2003*.
- Lorence, D.P., Richards, M.C., Spink, A. (2002). EPR Adoption and Dual Record Maintenance in the U.S.: Assessing Variation in Medical Systems Infrastructure. *Journal of Medical Systems, Vol. 26, No. 5, oktober 2002*.
- Meyer de, F., Lundgren, P., Moor de, G., Fiers, T. (1998). Determination of user requirements for the secure communication of electronic medical record information. *International Journal of Medical Informatics* 49 39-54 (1998).
- Rindfleisch, T.C. (1997). Privacy, information technology, and health care. *Association for Computing Machinery. Communications of the ACM* 40, 8: ABI/INFORM Global pg. 92 (1997).
- Robertson, C.J., Sarathy, R. (2003). Strategic and Ethical Considerations in Managing Digital Privacy. *Journal of Business Ethics* 46: 111-126 (2003).
- Sadan, B. Patient data confidentiality and patient rights. *International Journal of Medical Informatics* 62 41-49 (2001).

Safran, C., Goldberg, H. (2000). Electronic patient records and the impact of the Internet. *International Journal of Medical Informatics* 60 77-83 (2000).

Sector Consumer Products Ernst & Young. (2002). Privacy: What Consumers Want. *The Survey Says...More Assurance Leads to More Business* (2002).

Sector Health Sciences Ernst & Young. (2003). Elektronische patiëntendossiers in Nederlandse ziekenhuizen. *EDP Audit* (2001).

Seničar, V., Jerman-Blažič, B., Klobučar, T. (2003). Privacy-Enhancing Technologies – approaches and development. *Computer Standards & Interfaces* 25 147-158 (2003).

Songini, M.L. (2000). Hospital confirms hacker stole 5,000 patient files: Supposed 'ethical' hacker infiltrated system last summer. *Computerworld*; Dec 18, 2000; 34, 51; *ABI/INFORM Global* pg. 7

Toussaint, P.J., Lodder, H. (1998). Component-based development for supporting workflows in hospitals. *International Journal of Medical Informatics* 52 53-60 (1998).

United States Department of Health & Human Services (2003). Summary of the HIPAA Privacy Rule. <http://www.hhs.gov/ocr/hipaa>, geraadpleegd 1 mei 2004.

URL

- [1] <http://home.planet.nl/~groul003/trwpinh.html>, geraadpleegd op 25 januari 2005.
- [2] http://www.getronics.com/nl/nl-nl/industries/healthcare/trends_en_ontwikkelingen/trends_ontwikkelingen_health.htm, geraadpleegd op 27 januari 2005.
- [3] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212829,00.html, geraadpleegd op 30 april 2004.
- [4] <http://www.spamvrij.nl/faqomat/fom.php?page=faq-001&pagemode=qa#qa-001>, geraadpleegd op 12 december 2004.
- [5] <http://www.nvma.nl/nl/actueel/item.php?ID=514>, geraadpleegd op 1 mei 2004.
- [6] http://www.minfin.nl/DEFAULT.ASP?CMS_ITEM=MFCR2C007DC9556BC11D5BFDC00104B3FB E32, geraadpleegd op 28 januari 2005.

