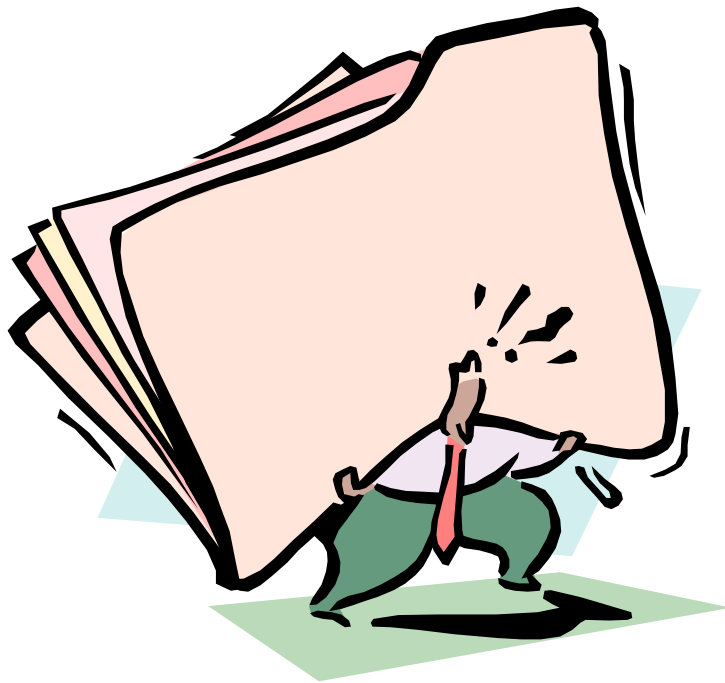


HET EPD



Begeleidster: Mw. Mr. T.A.M. te Braake
Module: 4
Datum: 18-03-2005
Auteurs: Khalid Bohoudi [0467073]
Mark de Groot [0455253]

INHOUDSOPGAVE

<u>SAMENVATTING</u>	<u>3</u>
<u>HOOFDSTUK 1: Inleiding</u>	<u>4</u>
<u>HOOFDSTUK 2: Wat is het EPD?</u>	<u>5</u>
<u>HOOFDSTUK 3: De patiënt en zijn rechten</u>	<u>6</u>
§ 3.1: Rechten van de patiënt	6
§ 3.2: Wensen van de patiënt in verband met het EPD	8
§ 3.3: Privacy	9
<u>HOOFDSTUK 4: De beveiliging van het EPD</u>	<u>9</u>
<u>HOOFDSTUK 5: Conclusies en discussie</u>	<u>12</u>
§ 5.1: Conclusies	12
§ 5.2: Discussie	13
<u>BIJLAGEN</u>	<u>14</u>
<u>BIJLAGE A: Beveiliging van het EPD (beveiligingseisen)</u>	<u>14</u>
<u>BIJLAGE B: Een interview met huisarts E.C. Kanter</u>	<u>16</u>

SAMENVATTING

Een echt landelijke Elektronische Patiënten Dossier (EPD) is er nog niet helemaal. Er zijn wel al veel kleinere EPD's, maar dat kan je niet echt een EPD noemen, denk hierbij aan het HIS van de huisartsen. Het EPD zou vele voordelen met zich mee brengen. Maar Om het EPD te realiseren moet men vele obstakels overwinnen. In het bijzonder gaat het om de rechten van de patiënt te handhaven. Dat zou betekenen dat je een acceptabele beveiliging moet hebben voor het EPD en zo als er al reeds bekend is bied er geen enkele beveiliging 100% veiligheid. Het EPD moet minstens dezelfde functies kunnen vervullen als het papieren dossier en het HIS van de huisarts. In de huidige situatie wordt de privacy van de patiënt m.b.t. het papieren dossier vrij goed gewaarborgd.

Zowel de patiënt als de zorgverlener hebben rechten en plichten. Als beide partijen zich hieraan houden kan er een uitstekende zorgvoorziening bewerkstelligd worden. De rechten en plichten van beiden partijen zijn opgenomen in het Burgerlijk Wetboek. Hierin zijn diverse artikelen opgenomen die hierop slaan. Maar de patiënt heeft wel meer wensen dan alleen wat er in de Wet Boek is opgenomen. Moet het EPD ook hieraan tegemoetkomen? Deze vraag moet worden beantwoord voordat er überhaupt het EPD ingevoerd kan worden. Een andere vraag is natuurlijk wie bepaalt er welke informatie uit het EPD beschikbaar wordt gesteld voor buitenstaanders¹. Moet de patiënt dat zelf bepalen? Heeft de patiënt wel voldoende kennis om de beslissingen zelf te nemen of is het toch beter als hij wordt bij gestaan door een medicus?

De inhoud en het uiterlijk van het EPD spelen beiden een even grote rol. Het is in beiden gevallen duidelijk aan welke eisen deze moeten voldoen. Het staat vrijwel allemaal in het BW. De enige echte probleem is de beveiliging en de gebruikers en hun bevoegdheden duidelijk in kaart te brengen en zo veilig mogelijk te maken zodat deze geen negatieve invloed kunnen hebben op het EPD.

¹ Buitenstaanders, hiermee worden bedoeld: Specialisten, huisartsen, dokterassistenten en overige niet-medici. Alle personen die niet direct betrokken zijn bij de behandeling

HOOFDSTUK 1: Inleiding

In het Elektronisch Patiënten Dossier (EPD) zal alle relevante (voor het zorgproces) informatie van de patiënt worden opgeslagen. Deze gegevens zijn nodig om de patiënt goed te kunnen behandelen. In hoofdstuk 2 komt aan bod wat het EPD is en wat er in het EPD moet staan. Het doel van het EPD komt ook in dit hoofdstuk aan bod.

Het is van belang dat de privacy van de patiënt gerespecteerd wordt, want de gegevens van het EPD mogen niet in de handen vallen van onbevoegden. Het is wel duidelijk dat geen beveiliging 100% bescherming biedt.

Een EPD gaat over een patiënt. De patiënt heeft recht op zeggenschap over zijn/haar EPD. De ene patiënt wil waarschijnlijk ook meer invloed op zijn/haar dossier uitoefenen dan een andere patiënt, met andere woorden de ene patiënt is de andere patiënt niet. Er kunnen vraagstukken naar voren komen omtrent de zeggenschap van de patiënt in zijn/haar dossier.

Aan het EPD en de rechten van de patiënt zitten heel wat haken en ogen. De rechten van de patiënt in verband met zijn/haar EPD staat centraal. Daarbij gaat het in het bijzonder over de zeggenschap van de patiënt zelf. Daarnaast speelt de manier van opslag van de gegevens in het dossier een rol, maar ook de beveiliging van deze gegevens ter verkoming van kennisneming door onbevoegden.

De rechten van de patiënt, privacy en kennisneming door onbevoegden komen in hoofdstuk 3 aan bod. Om de privacy te kunnen waarborgen moet het EPD beveiligd worden. Dit komt in hoofdstuk 4 aan bod.

Welke eisen moeten worden gesteld aan het EPD, gelet op de rechten van de patiënt met betrekking tot zijn medische gegevens?

Deze onderzoeksvraag zullen wij gaan beantwoorden. Dit gaan we doen door literatuuronderzoek uit te voeren. Tijdens onze stageweek zijn we van plan om zorgverleners en patiënten van het gezondheidscentrum te interviewen om zo hun ideeën te inventariseren over het EPD. We moeten echter rekening houden dat dit moeilijk te realiseren is. Het is ons niet gelukt om patiënten te interviewen.

HOOFDSTUK 2: Wat is het EPD?

Het elektronisch patiëntendossier (epd) is een virtueel concept. In de nota positionering algemene ziekenhuizen wordt het epd geschetst als een modulair opgebouwd geheel van een hoeveelheid relevant geachte data in diverse bestanden op diverse fysieke locaties. De door respectieve zorgverleners over een patiënt in het kader van een geneeskundige behandelingsovereenkomst verzamelde en decentraal vastgelegde medische informatie kan met behulp van elektronische communicatiemiddelen los van tijd en plaats in onderling verband worden gebracht, de zogenaamde gegevensverwerking. In die situatie spreekt men van een epd, vormgegeven door opslag aan de bron, met mogelijkheid van koppeling van de afzonderlijke bronnen aan elkaar mits daartoe aan bepaalde voorwaarden is voldaan.²

Het EPD is de digitale vorm van het papieren patiëntendossier. Het bevat onder andere medische gegevens, bijvoorbeeld ziekten die een patiënt heeft of welke behandelingen hij/zij al ondergaan heeft. Labuitslagen of röntgenfoto's kunnen ook in het EPD worden opgenomen. Helaas zijn (bijna) alle programma's die nu nog draaien nog niet zo flexibel (foto's kunnen bijna nog niet worden opgenomen in een dossier).

Het EPD bevat (voor een groot deel medische) gegevens over de patiënt. Deze gegevens zijn nodig om de goede zorg van de patiënt te waarborgen, bijvoorbeeld gegevens over allergieën of overgevoeligheid voor medicatie. *'Verantwoorde zorg' is zorg van inhoudelijk goed niveau die in ieder geval doeltreffend, doelmatig en patiëntgericht wordt verleend en die voldoet aan de behoefte van de patiënt.*³

Om dit te kunnen bereiken heeft iedere zorgverlener de plicht om een medisch dossier bij te houden. De gegevens die worden opgeslagen zijn van belang bij de goede zorgverlening aan de patiënt. Het is de bedoeling dat het EPD moet op ieder moment op iedere plaats op te vragen is, om zo het zorgproces nog meer te verbeteren. Het doel van het EPD is het verbeteren van de zorg en daarnaast ook het verbeteren van het zorgproces.

Het EPD heeft de voorkeur van veel mensen, dat blijkt uit een onderzoek van de NICTIZ⁴, de gegevens zijn sneller beschikbaar bij calamiteiten en ook beter bereikbaar en toegankelijk. Daarnaast is de leesbaarheid ook verbeterd en is er een beter overzicht (natuurlijk als het EPD volledig goed geïmplementeerd is).

² Mw. Prof. Mr. Henriette D.C. Roscam Abbing, Medische informatie, patiënt en epd. NTMA, 2000; 102: 57 - 63

³ Kwaliteitswet Zorginstellingen (KWZ), Staatsblad 1996, 80

⁴ drs. G. Hoeks en drs. A. Nijhuis, Kort eindverslag behorend bij project autorisatie EPD en patiëntenperspectief. Rapport 2004-59/K&T/05.02.05/GH/tk. Opdrachtgever NICTIZ uitvoerder NPCF, 2004; 21 - 62

HOOFDSTUK 3: De patiënt en zijn rechten

Als we praten over de rechten van de patiënt met betrekking tot zijn medische gegevens dan hebben we vooral te maken met de WBP (Wet Bescherming Persoonsgegevens) en de WGBO (Wet op de Geneeskundige Behandelingsovereenkomst). De WBP bevat artikelen die in het algemeen gaan over persoonsgegevens; de WGBO is toegespitst op de gezondheidszorg, of beter gezegd; de behandelingsovereenkomst.

§ 3.1: Rechten van de patiënt^{5,6,7}

De wet (7:BW)

In het 7: BW zijn artikelen opgenomen m.b.t. de rechten van de patiënt en de hulp-, zorgverlener.

Recht op inzage

Naast de zorgverlener (heeft toestemming van de patiënt, impliciet dan wel expliciet verkregen van de patiënt) die de patiënt behandelt, mag alleen de patiënt het EPD inzien (7:456 BW). In artikel 7:457 BW staat beschreven dat de zorgverlener zich hier aan moet houden; het beroepsgeheim (zwijgplicht).

De patiënt heeft recht op informatie

De informatie van de patiënt wordt opgeslagen in het EPD, (een deel) deze informatie zal een zorgverlener gebruiken voor de behandeling van de patiënt. Een zorgverlener moet de patiënt duidelijk uitleggen wat er precies gaande is. De behandelmethodes moet goed uitgelegd worden evenals de alternatieve behandelmogelijkheden. Daarnaast moet het de patiënt ook duidelijk zijn wat de gevolgen zijn en welke risico's er aan gebonden zijn (7:448 BW). De zorgverlener moet het zorgproces van de patiënt goed, duidelijk en begrijpelijk overbrengen op de patiënt. De zorgverlener is verplicht de patiënt genoeg informatie te verschaffen om zo mee te kunnen beslissen in de behandeling, ondersteund door de patiënt inzage in zijn/haar EPD te verlenen (7:456 BW).

De patiënt mag alleen informatie onthouden worden als het volgens de zorgverlener ernstig nadelig zou zijn voor de patiënt. Om te bepalen of deze informatie ernstig nadeel kan geven voor de patiënt, moet de zorgverlener dit overleggen met een andere zorgverlener (lid 3 7:448 BW).

De patiënt mag de zorgverlener ook te kennen geven dat hij/zij de desbetreffende informatie niet wil ontvangen. De zorgverlener moet dit verzoek respecteren, maar mag het verzoek negeren wanneer het informatie betreft die ernstig nadeel voor de patiënt dan wel de omgeving kan opleveren (7:449 BW).

⁵ Wet Geneeskundige Behandelingsovereenkomst (WGBO), Staatsblad 1994, 838

⁶ Wet Bescherming Persoonsgegevens (WBP), Staatsblad 2000, 302

⁷ Mr. J.K.M. Gevers en Mr. H.D.C. Roscam Abbing, Het EPD en de positie van de patiënt bij raadpleging patiëntengegevens. ICZ, oktober 2002; 9 - 25

Bevoegdheid tot inzage van de gegevens

Het moge duidelijk zijn dat de behandelend artsen (en zorgverleners die betrokken zijn bij de behandelingen van de patiënt) ook inzage hebben in deze gegevens (7:459 BW).

Als de patiënt om zorg vraagt dan wordt verondersteld dat deze patiënt dus ook toestemming geeft tot inzage van zijn EPD door de behandelend arts dan wel specialist (wordt gedeeltelijk beschreven in artikel 23 van de WBP). *...bij raadpleging door andere zorgverleners van medische gegevens (dient) altijd van enige vorm van betrokkenheid van de patiënt sprake moeten zijn.*⁸

De directe omgeving van de patiënt (familie) heeft alleen bevoegdheid tot het inzien van de gegevens als ze op een bepaalde manier betrokken zijn bij de behandeling of als de patiënt toestemming heeft gegevens tot inzage van zijn/haar gegevens (7:457 BW).

Bevoegdheid tot gegevensverwerking

Volgens artikel 16 van de WBP is niemand bevoegd om persoonsgegevens te verwerken betreffende iemand zijn/haar gezondheid. Er is een uitzondering zoals genoemd wordt in artikel 21. Daarin staat wie er bevoegd zijn om met de persoonsgegevens betreffende de patiënt zijn gezondheid te verwerken. Het betreft vooral personen die direct betrokken zijn bij de gezondheid van de patiënt, zoals de zorgverleners (bijvoorbeeld behandelend arts en huisarts).

*Om geen verandering teweeg te brengen in de onder de WGBO als gangbaar geaccepteerde praktijk is in art. 21 WBP aangegeven welke personen en instanties voor welke doelen gezondheidsgegevens mogen verwerken.*⁹

Vernietiging van gegevens/dossierstukken

De bewaartermijn is vastgesteld op 10 jaar (er zijn uitzonderingen, bijvoorbeeld allergie gegevens en gegevens over erfelijke aandoeningen zijn blijvend belangrijk). De patiënt heeft ook het recht om gegevens te laten vernietigen (lid 1 7:455 BW), maar de zorgverlener mag daar tegen ingaan als de desbetreffende gegevens echt noodzakelijk zijn voor de behandeling (goede zorg) van de patiënt (lid 2 7:455 BW).

Als een patiënt een verzoek doet van vernietiging, dan laat een zorgverlener zich ook leiden door zijn deskundigheid (7:453 BW). Hij moet zijn beweegredenen wel goed verwoorden en duidelijk overbrengen aan de patiënt.

Toestemming

Voor iedere behandeling (of welke andere verrichting dan ook) is toestemming van de patiënt nodig, deze toestemming kan (in de meeste gevallen) expliciet dan wel impliciet verkregen worden. De patiënt beslist of hij/zij behandeld wordt en niet de zorgverlener. De patiënt heeft het recht om zijn/haar eerder gegeven toestemming weer in te trekken.

⁸ Mr. J.K.M. Gevers en Mr. H.D.C. Roscam Abbing, Het EPD en de positie van de patiënt bij raadpleging patiëntengegevens. ICZ, oktober 2002; 31 - voor het zinsverband is 'dient' tussen haken toegevoegd

⁹ Mr. J.K.M. Gevers en Mr. H.D.C. Roscam Abbing, Het EPD en de positie van de patiënt bij raadpleging patiëntengegevens. ICZ, oktober 2002; 26

Soms wordt er vanuit gegaan dat de patiënt stilzwijgend toestemming geeft (als een patiënt bij de EHBO van het ziekenhuis komt is het zeer waarschijnlijk dat de patiënt toestemming geeft om hem/haar te behandelen). De patiënt kan te allen tijde verlangen en vragen om de toestemming voor een medische verrichting te noteren in zijn/haar EPD (7:451 BW).

Het (beoogde) beleid van het ministerie van VWS:

De kamerleden hebben gedebatteerd over het landelijk EPD. De minister van Volksgezondheid, Welzijn en Sport mocht namens de regering antwoord geven op de vragen. Eén vraag is interessant in de context van onze paper, deze vraag werd gesteld door het lid Schippers (VVD)¹⁰. De vraag was: *Welke waarde hecht u aan patiëntparticipatie in het zorgproces, zoals bijvoorbeeld het inzage hebben in het eigen dossier, het geven van toestemming aan zorgverleners om het dossier te mogen raadplegen en het registreren van zelfzorgmedicatie?*

Het antwoord van de minister van VWS op deze vraag was: *Patiëntparticipatie is een speerpunt van mijn beleid waarbij verantwoordelijkheid voor de eigen gezondheid en het eigen zorgproces centraal staan. Het recht op inzage in het eigen dossier verandert niet bij een elektronische versie. Dat geldt ook voor de toestemming die artsen nodig hebben voordat zij een dossier raadplegen. Ook heeft de patiënt het recht om gegevens aan zijn dossier te laten toevoegen.*

In de toekomst zal de patiënt ook thuis elektronisch zijn eigen dossier willen inzien en/of gegevens daaraan willen toevoegen. Ik ben daar voorstander van en er loopt een aantal projecten die daarmee experimenteren. Belangrijke voorwaarde hierbij is echter dat voorzien wordt in elektronische identificatie en authenticatie van patiënten.

De minister is een voorstander van participatie van patiënten in het EPD. Daarnaast is de minister van mening dat er geen verschil mag zijn met de papieren versie met betrekking tot rechten van de patiënt. Daarnaast heeft de KNMG¹¹ ook richtlijnen opgesteld voor het omgaan met medische gegevens.

§ 3.2: Wensen van de patiënt in verband met het EPD

In de WBP en WGBO staat beschreven welke rechten de patiënten precies hebben (in de WBP staat hoe gegevens beschermd dienen te worden). Hebben patiënten aanvullende wensen? Waar hecht de patiënt de waarde aan? Het onderzoek van de NICTIZ¹² geeft hierover meer duidelijkheid.

Wijziging gegevens

Je kan de patient niet alle gegeven laten wijzigen omdat hij/zij simpel weg niet over de juiste kennis beschikt. Je kan wel de wijziging van adresgegevens en verzekeringsgegevens laten wijzigen. Het zou nog beter zijn als deze gegeven geïntegreerd zouden zijn met de gegevens van verzekeringsmaatschappijen.

¹⁰ Kamerstuk: Antwoorden op kamervragen van Schippers over het landelijk EPD. KVR22078 2040505550. Sdu Uitgevers, 2005

¹¹ Mr. D.Y.A. van Meersbergen, KNMG Richtlijnen inzake het omgaan met medische gegevens. 9 december 2003; 9-15

¹² Drs. G. Hoeks en drs. A. Nijhuis, Kort eindverslag behorend bij project autorisatie EPD en patiëntenperspectief. Rapport 2004-59/K&T/05.02.05/GH/tk. Opdrachtgever NICTIZ uitvoerder NPCF, 2004; 21 - 62

Controlebehoefte

Uit het onderzoek is gebleken dat patiënten een grote behoefte hebben aan controle. Ze willen graag weten wat er gebeurt met hun persoonlijke EPD. Alleen in noodgevallen mogen de gegevens ingezien worden door zorgverleners, een onafhankelijke instantie zou moeten toezien dat het allemaal volgens de regels dan wel de richtlijnen gaat.

Toegang van derden tot het EPD

Uit het onderzoek blijkt dat er redelijk wat zorgen bestaan als de overheid of verzekeraars toegang krijgen tot het EPD, daarnaast vind 85%¹³ dat er expliciet toestemming gevraagd moet worden om de gegevens van het EPD in te zien. Het gaat hierbij om derden die niet direct betrokken zijn bij het behandelproces.

Toegang tot het eigen EPD

De meeste patiënten zouden het makkelijk vinden als ze hun eigen EPD in kunnen zien via het internet. Wat opviel in het onderzoek was dat de 65-plussers nauwelijks vertegenwoordigd waren. Naast het idee om via het internet het eigen EPD in te zien, hadden anderen de voorkeur om het EPD in te zien bij de huisarts of bibliotheek. Eén tiende zou graag via een informatiezuil bij de huisarts (of een andere zorgverlener) het eigen EPD willen inzien. Eén vijfde zou inzage willen krijgen via een papierenafdruk van het EPD.

§ 3.3: Privacy^{14,15}

Met bevoegdheid hangt de privacy nauw samen. De zorgverlener dient de privacy van de patiënt te beschermen dan wel te bewaren. Alle gegevens dienen vertrouwelijk te worden behandeld. De privacy is al ten dele gewaarborgd doordat het EPD in eerste instantie alleen in te zien is door de patiënt en de behandelende zorgverleners. De patiënt moet nadrukkelijk toestemming geven voordat de zorgverlener informatie mag verstrekken aan derden (7:457 BW en 7:459 BW), daar behoort de familie ook toe.

Toegang tot gegevens voor wetenschappelijk onderzoek is aan strenge regels gebonden (7:458 BW). Het wetenschappelijk onderzoek moet het algemeen belang dienen en het onderzoek is niet uit te voeren zonder de desbetreffende gegevens (enkele medische gegevens uit het EPD van de patiënt). Daarnaast heeft de patiënt tegen de verstrekking geen uitdrukkelijk bewaar gemaakt. Als gegevens worden vrijgegeven voor onderzoek, dan moet er een aantekening gemaakt worden in het EPD (lid 3 7:358 BW).

Als de patiënt overleden is, mag de privacy niet geschonden worden. Derden hebben dan geen recht tot inzage van het EPD (privacybescherming), tenzij de zorgverlener er van overtuigd is dat de patiënt er geen bezwaar tegen gehad zou hebben.

¹³ Drs. G. Hoeks en drs. A. Nijhuis, Kort eindverslag behorend bij project autorisatie EPD en patiëntenperspectief. Rapport 2004-59/K&T/05.02.05/GH/tk. Opdrachtgever NICTIZ uitvoerder NPCF, 2004; 50

¹⁴ Wet Geneeskundige Behandelingsovereenkomst (WGBO), Staatsblad 1994, 838

¹⁵ Wet Bescherming Persoonsgegevens (WBP), Staatsblad 2000, 302

HOOFDSTUK 4: De beveiliging van het EPD¹⁶

Om de privacy te kunnen waarborgen is het van belang om het EPD van de patiënt te beveiligen. Als het EPD beveiligd wordt dan is het voor onbevoegden nagenoeg onmogelijk om het EPD in te zien. De Registratiekamer hanteert 4 risicoklassen (O, I, II, III; O is publiek niveau¹⁷, III is hoog risico). De EPD's vallen onder risicoklasse II, er bestaat een verhoogd risico voor deze gegevens. Onder verhoogd risico wordt verstaan dat er extra negatieve gevolgen zijn voor de patiënt wanneer deze gegevens openbaar worden.

Voor risicoklasse II gelden speciale beveiligingsregels; de gegevens dienen versleuteld te zijn, de identificatie en verificatie moeten adequaat geregeld zijn en er dient sprake te zijn van strikte autorisatie. Alleen de direct betrokkenen mogen in het EPD kijken. Door de toegang (via een computer) tot het EPD te beveiligen is er de autorisatie te waarborgen. Degenen die via de wet (toestemming patiënt) toestemming hebben om in het EPD te kijken moeten toegang krijgen met een login-code¹⁸.

Voor de beveiliging van informatiesystemen bestaat een norm, NVN-ENV 12924. In deze norm zijn beveiligingseisen opgenomen die onder te verdelen zijn in 4 soorten: [1] systeemeisen, [2] administratieve en operationele eisen, [3] personele eisen en [4] fysieke en omgevingseisen. Voor alle 4 genoemde eisen gelden bepaalde regels die genoemd zijn in de NVN-ENV 12924, (zie Bijlage A: Beveiliging van het EPD (beveiligingseisen) pagina 14).

Naast de concrete invulling van beveiligingsnormen moet er ook nagedacht worden over de technische maatregelen ter beveiliging van het EPD, deze maatregelen worden ook besproken in een rapport van de ICZ¹⁹. Enkele manieren van beveiliging zullen in dit hoofdstuk besproken worden. Het is niet mogelijk om alle methoden te bespreken.

Biometrie

Mensen hebben unieke eigenschappen, welke niet na te bootsen zijn door anderen. Deze eigenschappen zijn uitermate geschikt ter beveiliging tegen onbevoegden. Bij biometrische beveiliging moet er gedacht worden aan een irisscan, een vingerafdruk, een handpalmscan, een stemherkenning-scan of een combinatie van de genoemde mogelijkheden.

Cryptografie en encryptie

Een andere manier van het beveiligen (coderen en decoderen) van gegevens is het versleutelen door middel van algoritmen en sleutels. Er zijn grofweg twee manieren om dit uit te voeren; symmetrische

¹⁶ Mr. Sjaak Nouwt, Beveiliging van het EPD. ICZ, oktober 2002; 24 - 28

¹⁷ Publiek niveau wil zeggen dat het over openbare persoonsgegevens gaat, bijvoorbeeld gegevens in het telefoonboek.

¹⁸ Het is bijvoorbeeld niet mogelijk om van buiten het AMC op de interne website te komen, alleen als je van binnenuit werkt is het mogelijk om via een wachtwoord in te loggen en de website te bezoeken (autorisatie). Zonder geldig wachtwoord is dat niet mogelijk.

¹⁹ Mr. Sjaak Nouwt, Beveiliging van het EPD. ICZ, oktober 2002; 31 - 47

encryptie en asymmetrische encryptie. Bij symmetrische encryptie wordt gebruik gemaakt van één sleutel (deze sleutel is zo moeilijk mogelijk). Voorbeelden van deze methode zijn de Caesar-encryptie²⁰ en de Vigenère-encryptie²¹. Asymmetrische encryptie is een meer geavanceerde methode en bestaat uit meerdere stappen:

Stap 1: Er worden 2 sleutelparen gemaakt door A en B. De publieke sleutel wordt vrijgegeven en de privé sleutel blijft strikt geheim.

Stap 2: Coderen van het bericht. Als B naar A een gecodeerd (versleuteld) bericht wil sturen, dan gebeurt dit met de ontvangen publieke sleutel van A.

Stap 3: Het bericht wordt verzonden en bevat nu het met behulp van A's publieke sleutel gecodeerde bericht.

Stap 4: Met behulp van A's corresponderende privé-sleutel zal het bericht voor A leesbaar worden gemaakt.²²

Beveiligingsprotocollen

Voor het verzenden van informatie over het internet bestaan verschillende beveiligingsprotocollen die moeten voorkomen dat gevoelige informatie bij derden terecht komt. Enkele voorbeelden van beveiligingsprotocollen zijn: SSL – Secure Socket Layer (biedt privacy en integriteit, webpagina's worden versleuteld en verzonden naar de browser en weer versleuteld teruggestuurd naar de informatieaanbieder. Daarnaast kan SSL ook van digitale certificaten gebruik maken, zodat een instelling zich kan identificeren) en S/MIME (voor de beveiliging van e-mail, biedt ook privacy en integriteit). Er zijn nog meer beveiligingsprotocollen, maar deze twee zijn de meest bekende.

Digitale handtekening

Een digitale handtekening kan gebruikt worden om gegevens te beveiligen en als er wijzigingen worden aangebracht in een EPD is bekend wie deze wijzigingen doorvoert, immers er staat een digitale handtekening. Digitale handtekeningen kunnen gestalte krijgen in de vorm van een certificaat of een uniek identificatienummer.

ICPC²³ Codering

De ICPC codering wordt gebruikt bij het coderen van ziekten of aandoeningen. Bijvoorbeeld K geeft aan dat het over de bloedsomloop gaat K01 geeft aan dat de pijn toegeschreven kan worden aan het hart. Als er gefilterd wordt op ICPC codes kan alleen de informatie zichtbaar worden voor de desbetreffende zorgverlener wat voor hem/haar van belang is.

²⁰ Het verplaatsen van het alfabet, bijvoorbeeld met de sleutel 3. De A wordt dan een D, B een E ..., Z een C.

²¹ Hetzelfde idee als Caesar, maar dan met een woord. Bijvoorbeeld de sleutel is KOM. Bij de eerste letter wordt er gebruik gemaakt van de K (waarbij de K een A wordt, L een B, enz) bij de tweede letter een O (waarbij de O een A wordt, P een B, enz) en bij de derde letter een M (waarbij de M een A wordt, N een B, enz). Wanneer de boodschap langer is dan het sleutelwoord, dan wordt het woord hergebruikt. De vierde letter wordt versleuteld zoals het bij de K van KOM gebeurt.

²² Voor meer informatie over asymmetrische encryptie: Mr. Sjaak Nouwt, Beveiliging van het EPD. ICZ, oktober 2002; 36 - 37

²³ International Classification of Primary Care, een idee van huisarts E.C. Kanter om zo te filteren

HOOFDSTUK 5: DISCUSSIE EN CONCLUSIES

§ 5.1: Discussie

Geen beveiliging is waterdicht, maar het kan hackers altijd zo moeilijk mogelijk gemaakt worden om bij de informatie te komen (login, stemherkenningscan en digitale handtekening), de drie genoemde beveiligingsmogelijkheden lijken ons het gemakkelijkst realiseerbaar en ook het financiële plaatje is aantrekkelijker dan bij een handpalmscan of een irisscan. Wat naar onze mening ook heel belangrijk is dat er een goede logfunctie in het systeem wordt ingebouwd, zodat te zien is wie wat wanneer heeft veranderd of heeft toegevoegd. Filtering op ICPC-codes kan voorkomen dat informatie bij onbevoegden terecht komt, dit is een goede methode, mits de zorgverlener de ICPC-codes gebruikt. De verantwoordelijke voor deze persoonsgegevens is natuurlijk degene die het opslaat. Bij het EPD is dat een moeilijk verhaal, want er zijn meerdere personen die wat op kunnen slaan. Hierover moeten goede afspraken gemaakt worden en het aantrekkelijkst zal zijn als deze afspraken in protocollen worden vastgelegd.

Het is ook duidelijk dat patiënten niet alles kunnen eisen, bijvoorbeeld sommige gegevens mogen niet vernietigd worden anders zou de behandeling niet (goed) uitgevoerd kunnen worden. De zorgverlener moet alleen gegevens opnemen die van belang zijn bij het zorgproces. De patiënt moet ook zeker (via patiëntenorganisaties) invloed kunnen uitoefenen op de ontwikkeling van het EPD.

Er kunnen nog steeds problemen ontstaan waarbij een conflict is tussen verschillende artikelen in de wet²⁴. Deze problemen grenzen (of overschrijden) aan het ethische vlak. Door overleg met de patiënt en de zorgverlener kunnen sommige problemen al opgelost worden, maar in sommige gevallen zou de zorgverlener een (ethische) beslissing moeten nemen. Hier gaan wij verder niet op in; dit gedeelte valt buiten de context van deze paper, maar met deze problemen dient wel rekening gehouden te worden. Deze laatste problemen kunnen nog wel eens discussies opleveren tussen patiënt en zorgverlener of tussen zorgverleners onderling.

²⁴ De hulpverlener moet dan nagaan wat het beste is voor de patiënt; welke optie de patiënt waarschijnlijk het meest bij gebaat is. Waarbij de hulpverlener bij zijn werkzaamheden de zorg van een goed hulpverlener in acht neemt en handelt daarbij in overeenstemming met de op hem rustende verantwoordelijkheid, (...). Artikel 453 van de WGBO.

§ 5.2: Conclusies

Gelet op het voorgaande kunnen wij concluderen dat de beveiliging de grootste rol speelt gelet op de rechten van de patiënt m.b.t. zijn (medische) gegevens in het EPD. Het is belangrijk dat de patiënt steeds toestemming moet blijven geven om informatie te verstrekken aan derden, zo blijft de patiënt betrokken bij zijn eigen EPD. Handpalmscan en irisscan zijn moeilijk realiseerbaar; immers het EPD moet landelijk beschikbaar zijn en overal op te vragen zijn. Als je deze methoden van beveiliging gebruikt moet iedereen een handpalmscan en irisscan thuis hebben wat een hele investering is. De beste oplossing is om deze gegevens d.m.v. asymmetrische encryptie te versleutelen.

Bij het EPD moet ook een logboek aanwezig zijn waarin gegevens worden opgenomen wie, wanneer, hoelang en welke gegevens heeft bekeken van het EPD. Daarnaast moet ook aangegeven worden welke wijzigingen zijn doorgevoerd.

Het is van belang, met betrekking tot gegevensverwerking, dat de beveiligingsnormen (bijvoorbeeld NVN-ENV 12924) gerespecteerd worden (bijlage A).

BIJLAGEN

De lay-out van alle bijlagen is aangepast. Aan de inhoud is niks veranderd.

BIJLAGE A: Beveiliging van het EPD (beveiligingseisen)

Bron: Mr. Sjaak Nouwt, Beveiliging van het EPD. ICZ, oktober 2002; 26 - 28

(...) De beveiligingseisen die in de Nederlandse-Europese voornorm zijn opgenomen, zijn te verdelen in vier soorten: (1) systeemeisen, (2) administratieve en operationele eisen, (3) personele eisen en (4) fysieke en omgevingseisen. Deze eisen houden het volgende in:

♦ Systeemeisen

- identificatie en authenticatie (ten minste gebruikersnaam, wachtwoord, automatische log-out)
- toegangscontrole en autorisatie (autorisatie van toegangsbevoegdheid: raadplegen, muteren en/of verwijderen van gegevens)
- aansprakelijkheid en toezicht (aanmaken logbestanden)
- juistheid (softwarematige controle op format, getallenreeks, versie laatste back-up, handmatige procedures)
- betrouwbaarheid (regelmatige back-ups maken, file-dumps, automatische herstel procedures, back-up op brandveilige plaats, etc.)
- gegevensuitwisseling en netwerken (onderhoud netwerk door bewerker, netwerkbeveiliging, voorkomen van modem-koppelingen, fysieke beveiliging tegen aftappen)

♦ Administratieve en operationele eisen

- beveiligingsmanagement (bevorderen veilige praktijken en attitudes)
- beveiligingsmanager (verantwoordelijke individu)
- IT beveiligingsbeleid (onder verantwoordelijkheid van de beveiligingsmanager, algemeen advies over verdeling verantwoordelijkheden)
- terugkoppeling van incidenten (procedure voor snelle terugkoppeling van incidenten, kwetsbare toegangscontroles direct tijdelijk vervangen door noodprocedures, uiteindelijk vervangen door veiliger procedures)
- continuïteitswaarborgen (behoud van gegevens bij calamiteiten, gedetailleerde rampenplannen, recovery-procedures jaarlijks testen)
- virusprotectie (anti-virus beleid ter preventie, opsporing, bestrijding, verwijdering en herstel, dagelijkse controles van PC's en servers)
- systeembeheer (onderhoudscontracten, procedure voor remote-access door onderhoudsmedewerkers, geheimhoudingsplicht in contract)
- media- en documentatiebeheer (bewaren in afsluitbare ruimten, toegang en verwijdering wordt gedocumenteerd, unieke identificatie van media, ontvangen media checken op aparte machines op compatibiliteit met hard- en software)

- systeemonderhoud (onderhoud van originele software en updates, alle software uitvoerig testen voor invoering)

♦ **Personele eisen**

- werving (referenties nagaan)
- personeelsmanagement (geen toegang personeel tot programmeeromgeving; procedures beschikbaar voor geautoriseerde toegang: overzicht mogelijkheden, wat te doen bij problemen, etc.)
- beveiligingsbewustzijn (training, cursussen, meldingsplicht incidenten)
- einde arbeidsovereenkomst (direct afsluiten toegang, overheveling toegang naar andere medewerkers, verwijderen uit gevoelige gebieden, inleveren pasjes, sleutels, handboeken, etc.)
- privacy personeel (beveiligingsmaatregelen, zoals monitoren en loggen, mogen geen onbehoorlijke inbreuk maken op de privacy van het personeel)

♦ **Fysieke en omgevingseisen**

- fysieke toegangscontrole (centrale computers in afgesloten ruimtes)
- beveiliging tegen diefstal (markeren apparatuur, registratie bruikleenapparatuur)
- bescherming fysieke omgeving (air conditioning, vuur, water)

(...)

BIJLAGE B: Een interview met huisarts E.C. Kanters

Interview gehouden met huisarts E.C. Kanters ten tijde van de stage. Dit interview in stappen afgenomen vanwege de werkzaamheden die tussendoor kwamen.

♦ Wat vindt u van het EPD?

Goed idee, maar we zijn er nog lang niet. Eén van de belangrijkste punten is het respect hebben voor de patiënt. Het betreft immers zijn/haar gegevens. Als er goede regels en protocollen zijn dan is er een grote kans van slagen van het EPD.

♦ Wat zou u de voorkeur geven als u kunt kiezen tussen een EPD en een papieren dossier en waarom zou u daarvoor kiezen?

Vanaf 1989 werk ik met het papieren dossier deed toen al wel wat met computers. Vanaf 1991 zijn we overgegaan op MicroHIS (en is daar nu een expert in volgens huisarts mevr. G.A. IJff). Ik heb een enorme voorkeur voor het EPD; ik ben dus een voorstander van het EPD. Voor (bijna) alles gebruik ik nu MicroHIS. Het is een uitstekende informatiebron voor mijzelf en daarnaast ideaal voor jaarverslagen en rapporten. De leesbaarheid is beter en door de controle van het systeem worden er al fouten gefilterd (bijv. bij de medicatie). Natuurlijk bestaat het EPD uit meer gegevens dan het MicroHIS, maar als het EPD goed gestructureerd wordt dan heeft het een kans van slagen.

♦ Hoe denkt u over de veiligheid van het EPD en over de beveiliging?

SABA is een programma waarmee ik werk op het AMC. Alles wat ik invoer kan ik alleen inzien. Ze zijn er nog mee bezig dat ook anderen deze informatie kan inzien. Patiënten moeten wel expliciet of impliciet toestemming geven voor inzage van de gegevens. We moeten vertrouwen dat artsen zich aan het beroepsgeheim houden en geen gegevens doorspelen aan derden. De huisarts mag alle gegevens over zijn patiënt inzien, de specialist moet er echt toestemming voor krijgen.

Door middel van autorisatie is het mogelijk om bepaalde delen voor bepaalde artsen onzichtbaar te maken, om dit te bereiken moeten de gegevens gefilterd worden; als iedereen bijvoorbeeld de ICPC codes gebruikt kan er op die codes gefilterd worden en zo alleen de gegevens weergeven die voor de desbetreffende arts van belang zijn.

♦ Patiënten zijn erg bang dat hun privacy geschaad wordt, hoe denkt u daarover en is er een verschil volgens u tussen het EPD en het papieren dossier?

Na mijn idee wordt de privacy niet geschaad. Artsen moeten immers hun beroepsgeheim handhaven. Door middel van filtering kan bepaalde informatie onzichtbaar worden voor artsen die de desbetreffende gegevens niet nodig hebben. Daarnaast zijn de werkgegevens van een arts niet beschikbaar voor een patiënt.

Het papieren dossier is misschien wat minder vatbaar voor privacyverlies, maar die kan je ook ergens laten liggen waardoor onbevoegden de gegevens tot zich kunnen nemen.

♦ In hoeverre moet de patiënt zeggenschap t.a.v. zijn/haar eigen EPD krijgen volgens u?

De patiënt moet niet de volledige zeggenschap krijgen over zijn/haar EPD. Er zouden regels opgesteld moeten worden of protocollen, zodat iedereen wat er gebeuren moet. Het zou misschien handig zijn als het in de wet duidelijk wordt vastgelegd.