Noodzakelijke aanpassingen aan het Landelijk Elektronisch Patiëntendossier

De belangrijkste aanbevelingen, vragen, en opmerkingen naar aanleiding van het onderzoek naar de beveiliging van het Elektronisch Patiëntendossier (EPD).

Guido van 't Noordende, Universiteit van Amsterdam, 24 juni 2010.

De belangrijkste aanbevelingen op een rijtje.

1. Zorg voor 'end-to-end' authenticatie van berichten. Zo kan het informatiesysteem dat een verzoek ontvangt controleren of dit verzoek echt van een zorgverlener afkomstig is. End-to-end authenticatie helpt aanvallen vanuit het LSP voorkomen. Neem ook meer informatie op in de interne berichten (tokens).

2. Gebruik vooraf door de arts/verantwoordelijke ondertekende en centraal in het LSP controleerbare bewijzen van autorisatie. Stuur mandateringscertificaten mee naar de decentrale systemen voor end-to-end authenticatie (punt 1). Alleen met een bewijs van mandatering mag een medewerker toegang krijgen tot het EPD. Deze bewijzen moeten beperkt geldig zijn.

3. Behandelrelaties moeten expliciet vooraf door patiënten worden bevestigd. Zo kan betere preventie van misbruik plaatsvinden. Ook toezicht wordt eenvoudiger. Behandelrelaties moeten ook kunnen worden verbroken. Zonder expliciete, in het LSP controleerbare bevestiging van een behandelrelatie door een patiënt mag slechts een beperkte, specifiek omschreven en met expliciete toestemming van de patiënt gevulde set van (nood)gegevens worden bekeken. Gemandateerde medewerkers mogen geen nieuwe behandelrelaties kunnen claimen op het nivo van het LSP, of (nieuwe)gegevens registreren in het LSP. Dit mogen alleen artsen. In sommige gevallen mogen medewerkers bovendien nooit als gemandateerde toegang krijgen tot patiënten informatie, bijvoorbeeld bij psychische gegevens.

4. Voer een smartcard voor patiënten in die veilig inloggen op het klantenportaal mogelijk maakt. Het gebruik van één toegangsbeveiligingssysteem vereenvoudigt beheer en implementatie, en maakt end-to-end authenticatie mogelijk. Ook kan hiermee gevoelige (log)informatie en berichten in het LSP die zijn bedoeld voor de patiënt alleen worden beveiligd door versleuteling.

5. Minimaliseer de hoeveelheid loggegevens in het LSP. Maak verwijdering van gevoelige gegevens uit het EPD onvoorwaardelijk en volledig mogelijk. Verwijder erwijzingen en loggegevens uit het LSP die gerelateerd zijn aan patiënten, behandelrelaties, of verwijderde dossiers zo snel mogelijk en volledig.

6. Breid het informed consent model uit met een "nee tenzij" mogelijkheid voor patiënten. Hiermee kan 'onzichtbare' registratie van gegevens in het LSP op basis van "verondersteld consent" worden voorkomen. Zo ontstaat een mogelijkheid voor patiënten om invloed uit te oefenen op welke informatie wel en niet in het EPD wordt geregistreerd - als zij dat willen.

Opmerkingen:

Het is belangrijk na te denken over alternatieven voor landelijke, dossier-gebaseerde ("pull") communicatie, en te zorgen dat deze mogelijk blijven. Een dossiersysteem dat verwijzingen naar dossierstukken tot ver in het verleden bevat, en alleen in afscherming per gegevenscategorie voorziet, is inherent veel privacy-onvriendelijker dan bijvoorbeeld een postbussensysteem waarbij niet in een centraal 'geheugen' is voorzien. Een ander alternatief is bijvoorbeeld een systeem waarbij autorisatie is gebaseerd op verwijzingen. Een kritische houding ten aanzien van de vraag of het registreren van gegevens in het LSP wel écht noodzakelijk is, is erg belangrijk.

Indien de arts en de patiënt er (samen) voor kiezen om medische gegevens via een schakelpunt te ontsluiten ten behoeve van eventuele toekomstige inzage, wanneer de toestemming dus expliciet is, wordt automatisch voorzien in de eisen van WBP inzake minimaliteit, noodzakelijkheid, doelbinding, en informatieplicht. Dit is extra belangrijk in het EPD. Immers, het medisch beroepsgeheim wordt verbroken ten behoeve van het *potentieel* delen van informatie met andere zorgverleners via het schakelpunt. Dit moet een bewuste afweging zijn met inachtneming van de risico's.

Een kritische houding voorkomt dat het EPD gebruikt wordt (of zelfs gebruikt moet worden) in gevallen waar alternatieven, zoals eenvoudig elektronisch berichtenverkeer, uitstekend hadden volstaan. Een expliciete toestemming van de patiënt helpt om bewustzijn te creëren van de risico's van het delen van informatie ten opzichte van de eventuele noodzaak tot het delen van informatie. Uitzonderingen daargelaten ligt de keuze uiteindelijk bij de patiënt.

Bij zeer grote systemen zoals het EPD is het extra belangrijk om de hoeveelheid informatie die via dit systeem gedeeld wordt te minimaliseren, om de risico's van privacyschade bij een inbraak of kwetsbaarheid in het centrale systeem te minimaliseren.

Aanvullende notities bij de aanbevelingen:

Ad 2:
Mandateringscertificaten kunnen tevens helpen om decentrale logging sluitend te maken, wanneer ze worden meegestuurd bij end-to-end authenticatie (punt 1). Door decentrale logging kan de hoeveelheid en de aard van de centraal opgeslagen historische (log)informatie in het LSP worden geminimaliseerd.

De decentrale zorginformatiesystemen (GBZ systemen) dragen de verantwoordelijkheid voor toegangscontrole tot hun dossiers de-facto over naar het LSP. Het is de vraag wat voor consequenties dit heeft voor de (formele) aansprakelijkheid en verantwoordelijkheid voor deze dossiers, die op dit moment bij de zorgverleners ligt. Het LSP is immers niet alleen verantwoordelijk voor de verkeersstromen, maar voor de volledige toegangscontrole tot de decentraal opgeslagen medische informatie. Hoe rijmt zich dit met de verantwoordelijkheid van zorgverleners voor de medische dossiers van patiënten en de eventuele ontsluiting daarvan, zoals gedefinieerd in WGBO?

Gemandateerde medewerkers mogen alleen gebruik maken van het LSP/EPD met een UZI pas op naam. UZI passen met wel een functiecodering maar niet op naam (zoals vermeld in de brief die ik van het ministerie ontving, p. 3 regel 5), zijn niet herleidbaar, voldoen niet aan PKI-overheid, en zijn uit den boze.

In bepaalde gevallen zal mandatering overigens helemaal niet mogen worden toegestaan. Bijvoorbeeld wanneer de patiënt aangeeft dat dit niet mag, of bij psychiatrische gegevens.

Merk op dat een strakke regulering van mandatering extra relevant is in een groot systeem zoals het EPD vanwege het niet-inzichtelijk zijn van behandelteams voor patiënten, het LSP, en de aangesloten GBZ bronsystemen.

Ad 3:
Expliciete bevestiging van behandelrelaties door patiënten zou altijd verplicht moeten zijn, behalve voor een beperkte set van (nood)gegevens. Dit in tegenstelling tot het huidige model waarin expliciete bevestiging van de behandelrelatie door de patiënt zelf nooit afgedwongen wordt door het LSP, zelfs niet achteraf. Het decentrale 'pop-up' scherm waarmee de arts in zijn eigen systeem moet bevestigen dat een behandelrelatie bestaat beschermt niet tegen kwaadwilligen. Het helpt de toezichthouder ook niet bij de lastige taak van het analyseren van de (centrale) logfiles.

In Duitsland moeten patiënten tegelijkertijd met de arts een pas in een kaartlezer steken, anders krijgt de arts geen toegang krijgt tot het dossier. In het Nederlandse EPD moet het minimaal mogelijk zijn om het klantenportaal te gebruiken voor de bevestiging van behandelrelaties voordat toegang wordt verleend, liefst met behulp van een sterk authenticatiemiddel (zie ook punt 4).

Ad 4:
Een sterk authenticatiemiddel -een smartcard analoog aan de UZI pas- is nodig voor identificatie van patiënten, en voor end-to-end authenticatie van berichten op dezelfde wijze als punt 1. Ook kan hiermee informatie worden versleuteld zodat alleen de patiënt deze informatie kan zien, bijv. loginformatie of brieven van artsen. Ook kunnen behandelrelaties hiermee eenvoudig worden bevestigd, met een door de smartcard ondertekend bericht.

Ten aanzien van het klantenportaal kan het verder van belang zijn om het inzien van volledige medische informatie alleen mogelijk te maken vanaf goed beveiligde werkstations bij zorgverleners. Dit niet alleen om het risico van aanvallen op het inlogsysteem door bijvoorbeeld virussen die bij

patiënten thuis op de PC te verminderen, maar tevens om patiënten te kunnen begeleiden bij het inloggen en het gebruiken van het klantenloket, en eventueel bij het interpreteren van de in het EPD geregistreerde informatie.

Een veilige inlogplek is ook essentieel om te voorkomen dat patiënten door bijvoorbeeld verzekeraars of bedrijfartsen onder druk worden gezet om via hun klantenloket toegang te verschaffen tot hun medische gegevens. Eventueel kan op andere plekken (zoals thuis) wel toegang worden verschaft tot niet-inhoudelijke informatie. Bijvoorbeeld, verzoeken om (vooraf) behandelrelaties te bevestigen, of de toegangslogs.

Het helpt ook in dit verband (mogelijk misbruik van het klantenportaal door pressie op patiënten) wanneer de hoeveelheid gegevens die in het EPD worden opgeslagen wordt geminimaliseerd tot het hoogst noodzakelijke. Ook helpt het wanneer volledige en tijdige verwijdering van gegevens mogelijk is.

Het is belangrijk dat patiënten zelf een afweging kunnen maken tussen de baten en de risico's van het ontsluiten van informatie, door expliciete toestemming van de patiënt te vragen voordat informatie wordt aangemeld in de verwijsindex. Op deze wijze kan de patiënt -in samenspraak met de arts- mede bepalen welke informatie wel en welke informatie niet via in het EPD ontsloten wordt.

Het moet tenminste mogelijk worden voor de patiënt om aan te geven dat hem of haar toestemming moet worden gevraagd voordat nieuwe informatie in het EPD kan worden aangemeld **(punt 6).**

Ad 5:
Centrale opslag van loggegevens moet zoveel mogelijk worden voorkomen. Waarschijnlijk hoeven logging- of reconstructiegegevens die op de patiënt of op specifieke dossiers herleidbaar zijn helemaal niet centraal opgeslagen te worden. Decentrale opslag van (deel)informatie is waarschijnlijk ook mogelijk, met uitzondering van eventuele loggegevens die inzichtelijk moeten zijn voor inzage door de patiënt (punt 4). Deze zouden echter versleuteld kunnen worden. Centraal hoeft waarschijnlijk alleen niet op patiënten of specifieke dossiers herleidbare verkeersinformatie te worden opgeslagen.

Het realiseren van een minimale en veilige (eventueel deels versleutelde) opslag van loggegevens is niet eenvoudig. De gekozen oplossing moet daarom openbaar worden gemaakt ten behoeve van een publieke evaluatie voordat deze wordt ingevoerd.

NB:
De ontwerpspecificatie en het programma van eisen voor het LSP (PvE-LSP) zijn niet openbaar. Ook gegevens omtrent de hackerstesten, audits, en toetsingen van het LSP en de decentrale systemen zijn niet publiek gemaakt.

Deze en andere relevante gegevens zouden volledig openbaar moeten worden gemaakt, inclusief (contractuele) randvoorwaarden en andere informatie die voor een onafhankelijke evaluatie nodig is. Er kan eventueel een korte uitzonderingstermijn worden gehanteerd voor nog niet opgeloste problemen, maar deze termijn dient kort te zijn. Dit is des te belangrijker zolang de gerapporteerde kwetsbaarheden in de protocollen en het architecturele ontwerp van het EPD niet zijn opgelost.

Recente voorstellen van de Minister:

In een recente brief aan de Eerste Kamer, waarin de minister uitstel van de behandeling van de kaderwet verzoekt (kamerstuk 31466 H, 6 mei 2010), gaat minister Klink van VWS niet in op de verbeterpunten zoals in dit overzicht vermeld.

De minister vermeldt wel dat hij een onderzoek wil laten verrichten naar een aantal andere aspecten van de architectuur. Hij noemt onder meer een regionale partitionering en een mogelijkheid voor SMS notificatie. SMS notificatie houdt in dat patiënten een SMS krijgen op het moment dat iemand toegang krijgt tot een dossier van hun EPD. Het gebruiken van regionale communicatie in plaats van landelijke communicatie lijkt mij een zinvol alternatief voor landelijke communicatie, maar het is dan wel van belang dat die communicatie ook echt op zo beperkt mogelijke schaal plaatsvindt - dus regionaal via een regionaal schakelpunt en niet via het Landelijk schakelpunt zoals door sommigen

is gesuggereerd. Het landelijke schakelpunt zou wel voor landelijke berichtencommunicatie ("push verkeer") gebruikt kunnen worden.

SMS notificatie kan een redelijk idee zijn, maar roept wel veel nieuwe vragen op. Bijvoorbeeld, welke informatie wordt er in een SMS opgenomen? In een recente NEN bijeenkomst over logging in het LSP werd gesproken over het beschermen van de privacy van medewerkers. Betekent dit dat informatie over gemandateerde medewerkers die namens een arts toegang krijgen tot een dossier niet zichtbaar is voor patiënten?

Bovendien, leidt SMS notificatie niet tot nodeloze ongerustheid bij burgers, en op termijn juist tot een verminderde waakzaamheid? Deze oplossing schuift bovendien mogelijk de verantwoordelijkheid voor een adequate beveiliging van en toezicht op het EPD (ten onrechte) nog duidelijker af op de burger dan al het geval was. En hoe snel wordt actie ondernomen als een patiënt een melding doet van ongeautoriseerde toegang tot het dossier? Komt er een mobiel team dat meteen een inspectie doet, zodat een inbreker ook daadwerkelijk gepakt kan worden? En wat als een patiënt net op op het strand in Spanje ligt?

Meer algemeen, ook met betrekking tot het klantenloket, is het de vraag of patiënten nu en in de toekomst eigenlijk wel voldoende zicht hebben op behandelteams om te kunnen bepalen wie wel of niet legitiem medische informatie heeft bekeken. Dit compliceert het toezicht, maar ook de waarde van oplossingen zoals SMS notificatie. En hoe dan ook, dit is opnieuw een vorm van toezicht achteraf, in plaats van een (benodigde) preventieve maatregel.

De minister gaat niet in op het feit dat er simpelweg teveel informatie in het LSP wordt opgeslagen, op het feit dat autorisaties niet voor het LSP controleerbaar zijn, en dat het bij een inbraak in het systeem mogelijk is om onrechtmatig toegang tot medische informatie te krijgen. Bijvoorbeeld door misbruik van het mandateringsmechanisme, of van binnenuit het LSP.

Kortom, de voorstellen die de minister doet bieden geen oplossing voor de fundamentele ontwerpkwesties die zijn gecontstateerd.

In het algemeen:

Het EPD gaat uit van een dossier systeem. Dit is –in het algemeen, maar zeker als uitgevoerd op grote schaal- een inherent risicovolle aanpak, vanwege het simpele feit dat een dossier een geheugen heeft. Het voor langere tijd bewaren of toegankelijk maken van informatie is immers het doel van een dossier. Bovendien biedt de voorgestelde wet de mogelijkheid om –middels aanvullende maatregelen van bestuur- steeds meer (typen) informatie in het EPD op te slaan.

Het EPD komt met een "informed consent" model waarbij binnen de gegeven informatietypen informatie kan worden geregistreerd zonder vooraf overleg met de patient – een "verondersteld consent" model. Gezien het feit dat een grootschalig EPD niet én eenvoudig bruikbaar én absoluut veilig te krijgen is, creëert het EPD hiermee reële risico's voor de privacy van patiënten.

Het lijkt erop dat alternatieven minder risicovol zijn. Het dient daarom aanbeveling om serieus studie te maken van alternatieven die uitgaan van bijvoorbeeld kleine, beheersbare dossiers bij zorgverleners –waarbinnen de dossiers alleen toegankelijk zijn voor leden van kleine behandelteams of ten hoogste kleine groepen van concreet samenwerkende zorgverleners. In aanvulling daarop kan worden gedacht aan specialistische systemen voor specifieke groepen patiënten of voor complexe zorg. Voor deze systemen is het overigens ook denkbaar dat andere (niet rol-gebaseerde) mechanismes voor toegangscontrole wenselijk zijn dan die geboden worden door het LSP of vergelijkbare schakelpunten.

In aanvulling op (kleinschalige) systemen, kan door middel van een beveiligd postbussensysteem (dus *zonder* geheugen!) informatie gericht en alleen wanneer dat nodig is tussen zorgverleners worden uitgewisseld. Dit wordt ook wel "push" berichtenverkeer genoemd. Een andere mogelijkheid om de beveiliging te verberen is verder om automatisch na een beperkte periode (bijvoorbeeld na een jaar, of na afloop van een behandeling), verwijzingen automatisch uit het LSP te verwijderen.

Een minimale vereiste voor het gebruik van het Landelijk EPD voor het uitwisselen van medische gegevens, is dat het toestemmingsmodel in overeenstemming is met het risico van misbruik van het

systeem. Kortom, punt 6 van mijn aanbevelingen is een minimale voorwaarde voor een afdoende bescherming van de privacy in het EPD.

Ten slotte

Ondanks de aanmerkingen en aanbevelingen die ik beschrijf ten aanzien van het Landelijke EPD, heeft de ontwikkeling hiervan wel degelijk ook goede gevolgen gehad. Bijvoorbeeld, het gebruik van UZI passen voor zorgverlener identificatie is een zeer waardevolle ontwikkeling. Ook het stellen van hoge(re) eisen aan de beveiliging van GBZ systemen is een goede ontwikkeling, als althans het toezicht hierop voldoende streng is en de beveiliging van andere systemen hier niet van afhankelijk is. Echter, geen van deze ontwikkelingen maakt een landelijk EPD systeem noodzakelijk. Wel is het belangrijk om deze ontwikkelingen, op zichzelfstaand, te blijven gebruiken in toekomstige systemen. En wanneer in de toekomst regionale of kleinschalige schakelpunten ontwikkeld worden, dient ook hierbij kennis genomen te worden van de voor het LSP gerapporteerde beveiligingsrisico's.

Meer informatie: http://www.science.uva.nl/~noordend/epd/