Ministerie onderschat risico's bij beveiliging Elektronisch Patiënten Dossier

Op 26 maart 2010 maakte ik de conclusies van een onderzoek naar de beveiliging van het Elektronisch Patiënten Dossier (EPD) openbaar via een artikel in het NRC Handelsblad en het vrijgeven van het wetenschappelijke rapport. Reeds eerder waren minister Klink, Nictiz en de Eerste Kamer geïnformeerd over de bevindingen. Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) reageerde afgelopen week fel op de resultaten van mijn onderzoek. Met dit schrijven wil ik hierop reageren.

Mijn onderzoek naar het EPD beschrijft en analyseert het ontwerp, en hiermee de architectuur van het EPD. Een fout in de architectuur van een systeem heeft gevolgen voor het gehele systeem. De analyse baseert zich op een zorgvuldige studie van de ontwerpdocumenten van het EPD, aangevuld met gesprekken met het Nictiz. De hierop volgende aanbevelingen komen voort uit reeds lang bestaande, algemene ontwerpprincipes voor het ontwerpen van grootschalige systemen.

Het onderzoek gaat uit van de mogelijkheid van een inbraak in het Landelijk Schakelpunt (LSP) of in één van de op het EPD aangesloten zorginformatiesystemen. Uitgaande van de mogelijkheid van een inbraak, beredeneer ik de mogelijke consequenties hiervan. Bij een inbraak in het LSP is het mogelijk alle aangemelde gegevens van patiënten uit heel Nederland op te vragen bij verschillende zorginformatiesystemen. Bij een inbraak in een zorginformatiesysteem kan met een (gestolen) medewerkerspas op naam met PIN-code het mandateringsmechanisme worden misbruikt om patiëntgegevens op te vragen. Als gevolg hiervan kan het 'autorisatieprofiel' - waarmee patiënten bijvoorbeeld kunnen voorkomen dat hun buurman toegang krijgt tot hun EPD- worden omzeild. Een gerichte aanval kan, gezien de grote hoeveelheid transacties die plaatsvinden binnen het EPD, lange tijd onopgemerkt blijven. De gevolgen van het uitlekken of misbruiken van vertrouwelijke patiëntengegevens kunnen zeer ernstig zijn.

Het ministerie van VWS kwalificeerde het onderzoek als "niet onderbouwd". Er wordt als argument aangevoerd dat "aanvullende maatregelen" zijn getroffen bij het invoeren van het EPD. Er wordt daarmee gesteld dat de in het onderzoek veronderstelde inbraken in onderdelen van het systeem in de praktijk niet voor kunnen komen. Als argumentatie voert men o.a. aan dat uitgebreide testen door gespecialiseerde hackers zijn uitgevoerd die hebben aangetoond dat de beveiligingsmaatregelen adequaat zijn. Daarnaast vinden periodieke toetsingen plaats van de zorginformatiesystemen bij zorgverleners.

De kern van het verschil van mening wordt hier geraakt. Bovengenoemde toetsmethoden geven geen enkele *garantie* voor de veiligheid van het systeem. Als het EPD waterdicht zou zijn, zou dit het eerste systeem ter wereld zijn. Het punt is dat wanneer er een inbraak in het systeem plaatsvindt, de beveiligingsarchitectuur van het EPD de mogelijke schade moet kunnen beperken. Dit is in het huidige ontwerp niet het geval.

Het getuigt van onrealistische overmoed van VWS om ervan uit te gaan dat inbraken hen niet kunnen overkomen. Microsoft heeft duizenden zeer deskundige programmeurs in dienst. Toch worden ernstige fouten voortdurend ontdekt. Waarom zou het VWS dan wel lukken? Het Nederlandse EPD is erg groot, en ook nog eens afhankelijk van de beveiliging van een veelheid aan decentrale informatiesystemen. Deze hebben historisch gezien een zwakke reputatie op het gebied van informatiebeveiliging. Dit verandert niet van de ene op de andere dag.

Mijn onderzoek doet aanbevelingen die leiden tot een betere preventie van misbruik. Deze kunnen vrij eenvoudig en in het verlengde van het huidige EPD raamwerk worden uitgevoerd. Zij hebben geen, of slechts een geringe toename van de (organisatorische) complexiteit tot gevolg; in een bijlage ga ik hier op in. Daarnaast geven zij een betere bescherming van persoonsgegevens, en wordt de uiterst lastige taak van toezicht houden op het EPD flink verlicht.

De aanbevelingen die ik doe zijn o.a.:

- Zorg voor 'end-to-end' authenticatie van berichten, zodat het informatiesysteem dat een verzoek om een dossier ontvangt kan controleren of dit verzoek daadwerkelijk van een zorgverlener afkomstig is. Dit kan aanvallen vanuit het LSP voorkomen.

- Gebruik vooraf door de arts ondertekende -beperkt geldige- mandateringscertificaten als bewijs van autorisatie, voordat medewerkers toegang wordt verleend tot het EPD.

- Bevestig behandelrelaties expliciet, eventueel achteraf middels het klantenloket, ten behoeve van effectiever toezicht. Ook kan na bevestiging bepaalde privacygevoelige loginformatie uit het LSP worden verwijderd of versleuteld.

- Voer een smartcard voor patiënten in die veilig inloggen mogelijk maakt, en die ook het versleutelen van gevoelige patiëntgegevens in het LSP mogelijk maakt.

- Breid het “informed consent” model uit met een “nee tenzij” mogelijkheid voor patiënten. Dit is een eenvoudig te realiseren mogelijkheid waarmee patiënten die dat nodig achten invloed kunnen uitoefenen op welke informatie in het EPD wordt geregistreerd.

Nooit eerder was het mogelijk om via één enkele infrastructuur *alle* aangemelde gegevens van patiënten uit heel Nederland op te vragen. Het is daarom uitermate belangrijk om juist bij het EPD niet naïef te zijn ten aanzien van de beveiliging. Als er een hack mogelijk is, kun je ervan uitgaan dat deze gevonden en misbruikt gaat worden. Aanvullende maatregelen zoals toetsingen of monitoring van verkeersgegevens zijn niet geschikt om doelgerichte aanvallen op persoonsgegevens te voorkomen.

VWS neemt een groot risico, niet alleen voor zichzelf maar ook voor patiënten, door ervan uit te gaan dat inbraken kunnen worden voorkomen. Het gaat immers om een groot systeem dat zeer privacygevoelige informatie ontsluit van vrijwel alle burgers van Nederland, en dat voor zeer lange tijd gebruikt zal gaan worden. Het vormt daarmee een aantrekkelijk doelwit voor aanvallers. Naar mijn mening is het bagatelliseren van de risico's of het verkeerd aanpakken daarvan onverantwoord.

Een minder defensieve houding van VWS kan de beveiliging van het EPD ten goede komen.
Ik hoop dat de discussie kan verbreden tot een meer constructief en inhoudelijk debat over de afwegingen, keuzes, en de wenselijkheid van oplossingen, waarin alle bij het EPD betrokken partijen participeren.

Het volledige overzicht van alle onderzoekspunten en aanbevelingen is te vinden via http://www.science.uva.nl/~noordend/epd/

Bijlage - een reactie op de brief van het ministerie d.d. 30 maart 2010

1. Privacy en preventie van misbruik

Voor privacy is het *voorkomen* van misbruik essentieel. Het huidige EPD doet dit niet effectief. Het model leunt op controle (van onder meer logfiles) achteraf. Niet alleen is sluitend toezicht voor de toezichthouder achteraf en vrijwel onmogelijke taak door beperkte technische middelen - waaronder het ontbreken van valideerbare autorisatie informatie-, ook kan de vogel inmiddels gevlogen zijn - zeker als het een hacker en/of een corrupte medewerker betreft.

Controle achteraf is simpelweg het verkeerde model voor de bescherming van privacygevoelige informatie. In tegenstelling tot bijvoorbeeld financiële delicten, is het verlies van privacy gevoelige gegevens immers niet herstelbaar of compenseerbaar. Misbruik van het persoonlijke gegevens kan tot onherstelbare schade leiden voor individuele patiënten, en mogelijk zelfs de maatschappij. Een eenzijdige of eenvoudige risico-inschatting volstaat dan ook niet.

2. Test en audit resultaten zijn niet openbaar

VWS beroept zich op audits en (indringers)testen om aan te tonen dat de onderdelen van het EPD goed beveiligd zijn. Echter, de resultaten van deze audits zijn niet volledig openbaar gemaakt en dus niet onafhankelijk te evalueren. Pas als software (onder een "open source" beleid) een aantal jaren lang publiek getest en geëvalueerd is, met een beloning voor het vinden van fouten, is er wellicht iets zinnigs over de beveiliging te zeggen. Meer openheid is een aanbeveling die ik graag doe. Capabele kwaadwillende hackers vinden fouten toch wel; het kan zeer waardevol zijn wanneer een grote groep onafhankelijke deskundigen de code kan analyseren.

Graag zou ik zien dat alle relevante informatie (met uitzondering wellicht van nog onopgeloste problemen), waaronder niet alleen de resultaten op hoofdlijnen maar ook de vraagstelling, aannames, en eventuele randvoorwaarden en contractuele disclaimers van de testers, openbaar worden gemaakt ten behoeve van een onafhankelijke evaluatie.

3. End-to-end authenticatie en toename van complexiteit

Het ministerie stelt in haar reactie op mijn voorstel tot end-to-end authenticatie dat doorvoeren van de aanbevelingen zal leiden tot een "significante toename van de complexiteit van de implementatie GBZen met mogelijke nieuwe implementatie-, beheer- en beveiligingsrisico's."

Dit is een enorme overdrijving. De voorgestelde oplossing is om de bestaande authenticatie tokens (waar overigens nog wat informatie aan toegevoegd moet worden, dit is een ander punt van kritiek waar VWS niet op in is gegaan) door te sturen naar de decentrale systemen. De verificatie van de corresponderende velden in het token en het bericht, en het controleren van de digitale handtekening op basis van het meegestuurde certificaat van de verzender is triviaal.

Het enige wat nodig is is een eenmalige investering om de verificatie software te schrijven, die overigens analoog is aan software die al in het LSP gebruikt wordt. De verificatie kan eventueel zelfs worden uitgevoerd door middel van een los systeem dat voor het zorginformatiesysteem wordt neergezet. Overigens is end-to-end authenticatie ook nodig om end-to-end versleuteling voor de geheimhouding van berichten mogelijk te maken. Dit kan op een later moment eenvoudig op basis van end-to-end authenticatie worden ingevoerd.

4. Loggegevens en 'UZI' smartcard voor patiënten

Aangaande de gerapporteerde kwetsbaarheid van (lange termijn) opslag van log- en reconstructiegegevens in het LSP, gaat het ministerie niet in op de voorgestelde oplossing. Dit probleem kan, in ieder geval voor lange termijn opslag van gegevens, worden opgelost door versleuteling met een patiëntspecifieke sleutel. Dit kan wanneer patiënten de beschikking hebben over een "sterk" authenticatiemiddel, zoals een smartcard. Uiteraard impliceert een versleuteling van gegevens dat analyse van (oude) historische gegevens niet direct zonder hulp van de patiënt kan plaatsvinden; dit is echter een noodzakelijke en logische stap gezien de privacy van patiënten. Een alternatief is om log-informatie te verwijderen zodra dit mogelijk is, bijvoorbeeld na de bevestiging van een behandelrelatie (of bevestiging van transacties door een bepaalde zorgverlener) door de patiënt.

Het voordeel van het gebruik van een smartcard (UZI pas) voor patiënten, is dat er slechts één enkele techniek voor authenticatie hoeft te worden ondersteund in het systeem; dit voorkomt 'bridging' van authenticatiemechanismen, wat risico's met zich meebrengt. Bovendien is dit eenvoudiger te onderhouden en implementeren dan wanneer verschillende systemen worden gebruikt; uiteindelijk zal dit weer besparingen opleveren. Het systeem is ingewikkeld genoeg zoals het is; ondersteunen van een extra functionaliteit (EPD-DigiD gebaseerde toegang tot het klantenloket) maakt het systeem onnodig ingewikkelder.

Overigens zijn een aantal zwakke punten ten aanzien van de beveiliging van het EPD met het EPD-DigiD gebaseerde inlogsysteem voor patiënten reeds vermeld in een rapport uitgevoerd door onder meer PriceWaterhouseCoopers, in opdracht van het ministerie. Hierin bleef de mogelijkheid van een smartcard voor patiënten op basis van UZI technologie opvallend onbelicht. De invoering van de elektronische Nationale Identiteits Kaart (eNIK) zal volgens de minister nog wel even op zich laten wachten. Gegeven de genoemde overwegingen, stel ik voor om niet af te wachten maar direct over te gaan op een sterk, (UZI) smartcard-gebaseerd patiënten identificatie (authenticatie) middel. Eventueel kan later relatief eenvoudig overgegaan worden op de eNIK, die in technisch opzicht veel lijkt op de voorgestelde smartcard.

5. Mandatering en behandelrelaties – foute conclusies

Het ministerie gaat niet in op de suggestie om mandatering en eventueel behandelrelaties expliciet en controleerbaar te maken op het nivo van het LSP. Bij behandelrelaties gaf ik eerder aan dat ik me kan voorstellen dat een bevestiging vooraf door de patiënt vooraf niet in alle gevallen mogelijk, en soms ook te verantwoorden is. Dat geldt echter niet voor mandatering.

Gemandateerde medewerkers mogen op dit moment alles wat de mandaterende arts mag. Dit is te veel. Medewerkers zouden zelf geen gegevens moeten kunnen opvragen of registreren wanneer dit een nieuwe behandelrelatie impliceert. Ook denk ik dat voor bepaalde gegevens, zoals psychiatrische dossiers, mandatering wellicht helemaal niet moet worden toegestaan. Bovendien is het denkbaar dat in dit geval expliciete bevestiging van de behandelrelatie door de patiënt vooraf moet worden geëist.

In tegenstelling tot wat VWS stelt, is het voor een aanvaller wel degelijk mogelijk om de controles -die decentraal worden uitgevoerd om een behandelrelatie te controleren of vast te leggen- te omzeilen; het LSP heeft namelijk geen mogelijkheid om vast te stellen of deze controles plaats hebben gevonden. Een hacker kan daarom eenvoudig een ondertekend bericht met de juiste inhoud naar het LSP versturen om operaties namens een arts uit te voeren. Om die reden stel ik voor om autorisaties (mandatering) expliciet te maken ten tijde van het opvragen van gegevens. In het geval van behandelrelaties kan dit in de regel achteraf door middel van het elektronische klantenloket; dit helpt toezichthoudende taken te vereenvoudigen. In sommige gevallen, zoals bij toegang tot psychiatrische gegevens, zou bevestiging van een behandelrelatie vooraf, mogelijk ter plekke, kunnen plaatsvinden met behulp van de smartcard van de patiënt.

Als oplossing pleit ik overigens niet voor een "centrale registratie" van mandateringsrelaties, zoals VWS het in haar brief fout samenvat. Integendeel, ik neem als uitgangspunt de reeds voor het EPD voorziene *decentrale mandateringstabellen* om, gecombineerd met bijvoorbeeld agenda's, mandateringscertificaten te creëren met een beperkte geldigheid, die door de mandaterende arts moeten worden ondertekend. Deze moeten dan als bewijs mee worden gestuurd met de berichten van medewerkers die naar het LSP worden gestuurd. Dit kan ingewikkeld lijken, maar het voordeel is dat op een uniforme en gestructureerde manier omgegaan moet worden met mandateringsgegevens; de resulterende verbetering van de beveiliging en de verlichting van toezichthoudende taken achteraf, wegen mijns inziens sterk op tegen de benodigde investering.

Het belangrijkste verschil met het huidige model is dat in plaats van controle van mandaterings-tabellen achteraf, de gegevens uit de mandateringstabellen nu gebruikt worden om misbruik van mandatering te voorkomen - *preventief* dus. Dit is een belangrijk voordeel. Preventie van misbruik essentieel voor de bescherming van privacy.

Overigens maakt deze methode meteen ook de verantwoordelijkheid van de mandaterende arts zichtbaar, bijvoorbeeld voor juridische aansprakelijkheid. Ook verlicht het de taak van de toezichthouder aanzienlijk.

In het ergste geval zal bij het ontbreken van een mandatering vooraf, een arts zo nu en dan zelf het EPD moeten benaderen om gegevens op te halen. Dit lijkt mij gezien de extra geboden veiligheid geen onoverkomelijk probleem. Overigens kan een niet-gemandateerde medewerker, bij gebrek aan een mandateringscertificaat, altijd nog opvraagberichten klaarzetten ten behoeve van de arts zodat tijd bespaard kan worden. Dit is een reeds bestaande EPD-techniek. De arts hoeft deze berichten dan alleen nog zelf te ondertekenen.

Het lijkt al met al dat met de voorstellen ten aanzien van mandatering geen onaanvaardbare druk op de "werkbare praktijksituatie" hoeft te ontstaan.

6. Informed consent – "nee tenzij" niet haalbaar vanwege doelstellingen?

Ik stel voor om het "informed consent" model aan te passen, door naast de bestaande mogelijkheid van (volledig) bezwaar, een *"nee tenzij"* optie voor patiënten instelbaar te maken. Hierdoor kunnen patiënten die dit willen meer directe zeggenschap krijgen over welke informatie wel en welke informatie niet via het EPD kan worden uitgewisseld, in overleg met de arts of deels geautomatiseerd. Technisch is dit eenvoudig realiseerbaar.

De reactie in de brief van VWS is als volgt. *"Er is voor het huidige informed consent model gekozen om te borgen dat binnen een afzienbare tijd medische gegevens van een groot deel van de zorgconsumenten in Nederland kunnen worden uitgewisseld tussen zorgverleners. Dit is noodzakelijk om de doelstellingen en daarmee de beoogde toegevoegde waarde van het landelijk EPD te kunnen realiseren."*

Het halen van een doelstelling lijkt geen goede reden om de privacy bescherming af te zwakken door patiënten zeggenschap over wat in het EPD wordt geplaatst te ontzeggen.

Het is verder opmerkelijk dat VWS stelt dat de toegevoegde waarde van het EPD wordt bepaald door het *aantal* medische gegevens dat wordt geregistreerd. Het lijkt mij persoonlijk dat de *aard van de gegevens en de noodzakelijkheid voor het landelijk uitwisselen van deze gegevens* bepalend moeten zijn voor de vraag of het landelijk EPD toegevoegde waarde heeft.

Dit aspect raakt aan de discussie tijdens de expertmeeting in de Eerste Kamer op 22 maart 2010. Het lijkt me zinvol om deze discussie verder te voeren.

Patiënten zullen overigens in overleg met de arts uiteraard gewoon akkoord gaan met registratie van gegevens in het EPD als dit noodzakelijk is. Het belangrijkste aspect van het voorstel is dat niet *ongemerkt*, op basis van “veronderstelde toestemming”, gegevens in het EPD kunnen worden geregistreerd, zoals nu wel gebeurt.

Merk op dat een 'nee tenzij' model een *democratisering* teweeg kan brengen ten aanzien van wat er wel en niet in het landelijk EPD wordt geregistreerd. En dit is goed. Ultimo immers, is de zeggenschap over wat er met persoonlijke gegevens gebeurt – allereerst vanuit WGBO, maar ook vanuit onder meer de (Nederlandse en Europese) regelgeving voor databescherming - een grondrecht dat burgers hebben, en horen te behouden. De invoering van een van overheidswege ontworpen systeem dat dit grondrecht aantast staat hiermee op gespannen voet.