NH 26-03-10 katern 1 pagina 02

**Patiëntendossier** Informaticus waarschuwt voor privacygevaren van landelijke databank met medische gegevens

# Het EPD is lek omwille van de bruikbaarheid

Het elektronisch patiëntendossier is niet goed beveiligd. „De deuren staan wagenwijd open voor corrupte medewerkers van artsen."

**Door onze redacteur**
**ANTOINETTE REERINK**

DEN HAAG, 26 MAART. De senaat heeft nog grote bedenkingen bij het Elektronisch Patiëntendossier (EPD), maar de voorbereidingen voor de landelijke uitwisseling van medische gegevens van patiënten zijn al in volle gang. En dat terwijl de beveiliging nog niet op orde is.

Uit de eerste brede wetenschappelijke studie naar de beveiliging van het EPD blijkt dat het systeem gaten bevat. Volgens informaticus Guido van 't Noordende, onderzoeker aan de Universiteit van Amsterdam, ontbreken „basale veiligheidskleppen".

Van 't Noordende deed maandag mee aan een *expertmeeting* over het EPD in de senaat, die het wetsvoorstel van minister Klink (Volksgezondheid, CDA) hierover nog moet goedkeuren. Hij preludeerde toen op zijn binnenkort te publiceren studie.

De onderzoeker kroop in de huid van een kwaadwillende die misbruik wil maken van het EPD. Hij bestudeerde het raamwerk voor de landelijke uitwisseling van medische gegevens. Eén centrale vraag had hij: wat zijn de consequenties als iemand inbreekt in het EPD; ofwel in het Landelijk Schakelpunt (LSP) waarlangs straks alle informatie geleid wordt óf in de lokale systemen waar zorgverleners de patiëntgegevens bewaren.

Het Landelijk Schakelpunt controleert alle binnenkomende toegangsverzoeken, van wie ze afkomstig zijn en of ze digitaal zijn ondertekend. Op zich een goed idee, vindt Van 't Noordende, maar de informatie over de verzoeker wordt niet doorgestuurd naar het lokale systeem waar het dossier wordt bewaard. Als een kwaadwillende in het LSP weet te komen, kan hij alle informatie uit de decentraal opgeslagen dossiers opvragen zonder digitale handtekening. „Dit is een heel gekke fout."

Veel ernstiger vindt hij dat de autorisatie, de beslissing of een zorgverlener een medisch dossier mag inzien, centraal wordt genomen maar alleen decentraal te controleren is. Het gaat om de controle of er wel een behandelrelatie is tussen patiënt en arts, en om het delegeren van bevoegdheden van artsen aan medewerkers. Artsen moeten aangeven dat zij een behandelrelatie hebben met hun patiënt en als dat niet zo is, valt dat pas achteraf vast te stellen. „Dat vind ik niet zo gek", zegt Van 't Noordende. „Een arts is niet zomaar iemand. Als hij misbruik maakt van zijn positie, kan hij zijn beroep verliezen. Dit vertrouwen vind ik gerechtvaardigd."

Maar dat geldt wat hem betreft niet voor de autorisatie die een arts aan een medewerker geeft. Een medewerker kan gewoon in het systeem als hij bij zijn aanvraag van een dossier een veld invult met de naam van de mandaterende arts. Er hoeft geen bewijs bij te zitten dat de arts hem daadwerkelijk toestemming heeft gegeven. Van 't

> 'De deur staat wijd open voor corruptie'
> **Informaticus Van 't Noordende**

Noordende: „De medewerker heeft weliswaar een pas op naam nodig om dossiers te bekijken, maar uit de praktijk weten we dat ziekenhuizen slordig omgaan met passen." Ze kunnen ook gestolen worden. Een corrupte medewerker of iemand van buiten die zo'n pas bemachtigt, kan namens een arts dezelfde toegang krijgen tot patiëntendossiers als de arts. „Dit risico moet je niet lopen. Een corrupte medewerker of hacker is moeilijk te traceren en te straffen. Dit is veel te slecht afgedicht. Daar gaan kwaadwillenden gebruik van maken. Zorg dat je het risico vermindert door de arts een expliciet bewijs voor mandatering aan zijn medewerker te laten geven."

Van 't Noordende: „Een medewerker zal zich makkelijker laten omkopen door een criminele organisatie. En als iemand veinst dat hij voor een arts werkt, kan hij bij het Landelijk Schakelpunt claimen dat hij ook een behandelrelatie met de patiënt heeft. Die combinatie van factoren zet de deur wagenwijd open voor corrupte mensen. Tot dit opgelost is, zou ik zeggen: mandateer niemand."

Van 't Noordende: „Voor deze mandatering moet echt een oplossing komen, anders is het EPD gewoon lek." De meeste aandacht bij het ontwerp van het EPD gaat uit naar de bruikbaarheid voor de zorgverlening, vindt de informaticus. „Daarbij delft de privacybescherming weleens het onderspit. Ik zou voor de extra beveiliging gaan. Je belast zorgverlening iets meer, maar het toezicht op het EPD vereenvoudig je enorm. De toezichthouder, het College Bescherming Persoonsgegevens, moet nu toezien op een systeem dat niet waterdicht is. Dat is heel lastig." Van 't Noordende begrijpt niet waarom de EPD-architecten dit niet hebben ingebouwd. „Het is gewoon basaal."

De onderzoeker is ook niet gerust op de inzage van patiënten in hun eigen dossier. Hij vindt dat burgers daarvoor een soort smartcard moeten krijgen. Evenzeer zou bij hen de zeggenschap moeten liggen welke informatie zorgverleners in hun dossier opnemen. Burgers kunnen weliswaar bezwaar maken tegen opname van hun gegevens in het EPD, maar moeten zelf actie nemen om opslag van privacygevoelige informatie tegen te houden. „Gegevens die eenmaal op het Landelijk Schakelpunt staan, zijn er nooit meer helemaal uit te verwijderen. Ik wil dat de patiënt daarom toestemming verleent aan de zorgverlener voordat deze gegevens van hem opslaat. Al is het maar een schermpje dat oplicht bij de arts met de waarschuwing dat hij nog even de goedkeuring van de patiënt moet vragen."

Nictiz dat voor Volksgezondheid het EPD invoert, overweegt sommige aanbevelingen over te nemen. Maar vooralsnog is Nictiz tot een andere afweging gekomen bij het streven naar een optimale veiligheid. „Niet ieder theoretisch concept levert in de praktijk een optimaal resultaat op", aldus Nictiz-directeur Gert-Jan van Boven.

Van 't Noordende vindt het geen irreële scenario's dat kwaadwillenden op zoek gaan naar privacygevoelige informatie. „Je kunt iemand chanteren, bijvoorbeeld een politicus. Als je vreemd bent gegaan, ben je omkoopbaar. Maar je staat ook zwakker in het leven als bekend is dat je een psychose hebt gehad. Privacy is een grondrecht. Het is heel fundamenteel."

Achtergronden over het patiëntendossier op nrc.nl/epd