

VN MediagidsHoofdpijndossier



Foto: Frank Muller/HH.

Hoofdpijndossier

De maatschappelijke onrust over het elektronisch patiëntendossier is volledig verstomd. Maar alle bezwaren staan nog steeds overeind. ‘We zijn er zelfs op achteruitgegaan.’

Door **Harry Lensink** / **Maurits Martijn**

De maatschappelijke onrust over het elektronisch patiëntendossier is volledig verstomd. Maar alle bezwaren staan nog steeds overeind. ‘We zijn er zelfs op achteruitgegaan.’

Door **Harry Lensink** / **Maurits Martijn**

Het klinkt zo vanzelfsprekend. Dat de arts op de spoedeisende hulp met een druk op de knop kan zien wat uw medische geschiedenis is.

Dat verpleegkundigen op de intensive care in een computerscherm lezen waar u allergisch voor bent. Dat u niet bij iedere doorverwijzing naar een specialist opnieuw moet uitleggen welke medicijnen u slikt. Wie kan daar nu tegen zijn? Dus dat systeem komt er. Vanaf 1 januari 2013 kunnen hulpverleners het elektronisch patiëntendossier (EPD) raadplegen van elke Nederlander die daarvoor toestemming heeft gegeven.

Eigenlijk bestaat het al. Sinds er in 2008 een begin werd gemaakt met het EPD zijn de gegevens van negen miljoen Nederlanders via een landelijk systeem te raadplegen. Zij hebben de afgelopen jaren stilzwijgend hun toestemming gegeven, door niet actief te protesteren tegen deelname aan het EPD. Een kleine half miljoen mensen heeft dat wél geweigerd. Dat deden ze via een zogenaamd *opt-out* regeling; ze hebben via een bezwaarformulier hun deelname uitgesloten.

Die *opt-out* was slechts één van de bezwaren waar de eerste versie van het EPD vorig jaar op strandde in de Eerste Kamer. De senatoren vonden dat het EPD via een *opt-in* zou moeten werken: je laat zelf weten of je meedoet, wie niets van zich laat horen wordt niet in het systeem opgenomen. De politici zagen meer beren op de weg. Het EPD zou niet alleen de privacy van patiënten schaden, ook de veiligheid van de gegevens leek niet gegarandeerd, bleek tijdens verschillende bijeenkomsten met IT-deskundigen. Duizenden zorgverleners zouden toegang krijgen tot een landelijke database gevuld met delicate privé-informatie. Daarnaast had het EPD niet voldoende technische waarborgen om misbruik uit te sluiten. Een landelijk systeem dat op zo'n grote schaal zou worden ingevoerd kon alleen maar voor problemen zorgen. Een motie van PvdA-senator Ing Yoe Tan werd Kamerbreed aangenomen en het EPD leek van de baan. De parlementariërs vroegen aan de verantwoordelijke minister Edith Schippers van Volksgezondheid om haar handen van het project af te trekken.

Het verlies van een pas met pincode is nog steeds 'potentieel een ramp'

Tot verdriet van veel organisaties in de zorg. Huisartsen, apothekers en zorgverzekeraars zien heil in de geautomatiseerde gegevensuitwisseling. Dus besloten ze Den Haag te passeren en zelf als private partij onder de naam Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ) verder te gaan, gefinancierd door de zorgverzekeraars. Dat leidde eind vorig jaar tot een doorstart van het EPD, onder de eufemistische titel 'Zorg-infrastructuur'. Om deels aan de wensen van de kritische politici tegemoet te komen, kozen ze voor *opt-in*: elke Nederlander die wil meedoen, moet dat zelf aangeven. Ook die negen miljoen die nu al staan geregistreerd. De campagne om patiënten over te halen 'ja' te zeggen gaat deze week van start.

Wie het niet vertrouwt, laat simpelweg niets van zich horen. Maar zijn daarmee de gevaren voor deelnemers – de miljoenen die ongetwijfeld opnieuw meedoen – ook weggenomen? Is de veiligheid nu wel gegarandeerd? Nee, zeggen deskundigen. Er is niets veranderd. 'Alle bezwaren die er eerder waren staan nog overeind,' stelt ICT-onderzoeker Guido van 't Noordende van de Universiteit van Amsterdam. 'Dat betekent dat je vanuit een willekeurige plek in Nederland, in ieder geval vanuit ziekenhuizen, gegevens kunt opvragen van patiënten die zich hebben aangemeld. En als ziekenhuizen dat kunnen, dan kan een hacker dat ook.'

Het 'nieuwe' EPD draait op dezelfde infrastructuur die eerder al is neergelegd door het ministerie van VWS. Een landelijk schakelpunt (LSP) verbindt via een beveiligd netwerk de computers van hulpverleners met elkaar. Wie straks gegevens wil raadplegen, heeft het burgerservicenummer van een patiënt nodig en een pas met een zogenaamde Unieke Zorg Identificatie (UZI), voorzien van een beveiligingscertificaat. Voorwaarde is verder dat de zorgverlener een 'behandelrelatie' met de patiënt heeft. Ook heeft niet iedere medische professional dezelfde privileges. Specialisten in een ziekenhuis kunnen 'slechts' lezen welke medicijnen een patiënt gebruikt. Datzelfde geldt voor apothekers. De basis vormen de dossiers die door de huisarts en de apotheker worden bijgehouden, met daarin alle relevante medische gegevens. De informatie wordt niet op een centraal punt opgeslagen; het landelijk schakelpunt zorgt ervoor dat zorgverleners de gegevens bij elkaar kunnen inzien.

'Ik kan er vrij gemakkelijk een usb-stick insteken met wat narigheid erop'

Dat klinkt robuust, maar eerder wezen critici er op dat zorgverleners niet getraind zijn in informatiebeveiliging, zoals het omgaan met logins, toegangspassen en wachtwoorden. In het geval van het EPD is het verlies van één enkele pas met bijbehorende pincode 'potentieel een nationale ramp', zei een deskundige in 2009 tegen de Eerste Kamer. Dat is met het nieuwe EPD niet anders. 'Het is nog steeds een kwetsbaar systeem,' zegt ook Mark Koek, expert van het ICT-beveiligingsbedrijf Fox-IT. 'Er zijn veel gebruikers in een lastig te beveiligen omgeving. Uit de tests die wij hebben gedaan, blijkt dat ziekenhuizen vaak eenvoudig te compromitteren zijn. En van apothekers en huisartsen kun je al helemaal niet verwachten dat ze een database van deze waarde kunnen beveiligen.' Koek geeft een voorbeeld. 'Bij mijn apotheek staan pc's op de balie. Daar kan ik vrij gemakkelijk een usb-stick insteken met wat narigheid erop om zo de computer over te nemen om het systeem binnen te dringen. Bijvoorbeeld om te achterhalen wie er allemaal aidsremmers slikt, om die mensen vervolgens te chanteren.' Zijn bedrijf adviseert deelnemers dan ook om apart voor het EPD een pc te kopen, die los staat van andere computers en het internet. Daarnaast kunnen kwaadwillenden zorgverleners onder druk zetten, zegt Koek. 'Je kunt een arts omkopen of bedreigen, als je informatie echt graag wil hebben.'

De VZVZ geeft toe geen 'honderd procent garantie' te kunnen bieden tegen misbruik, maar stelt dat het systeem voldoende checks vooraf en achteraf heeft, om veilig te kunnen worden gebruikt. Zo wordt op voorhand vastgesteld of

een gebruiker inderdaad een ‘behandelrelatie’ met de patiënt heeft. Daarnaast is er slimme software die in de gaten houdt of er vreemde dingen gebeuren op het netwerk, bijvoorbeeld of er midden in de nacht vanuit Noord-Oost-Groningen honderden dossiers van patiënten uit Zeeland worden geraadpleegd.

Maar dan is het kwaad al geschied. Wie preventief te werk wil gaan, moet volgens Mark Koek continu het netwerk blijven monitoren. ‘Bij British Telecom houdt een heel team in de gaten wie de data opvraagt van bijvoorbeeld David Beckham. Als iemand vanuit een BT-kantoor op het platteland dat dossier opent, dan is er iets aan de hand en kunnen ze meteen ingrijpen.’ Daarnaast is het nog maar de vraag of misbruik van gegevens altijd de aandacht zal trekken. ‘Een slimme hacker valt juist heel gericht aan,’ zegt Guido van ’t Noordende van de UvA. ‘Het valt niet op als iemand vanuit Friesland opeens in één Limburgs dossier kijkt, want dat is nu juist het hele idee van het systeem.’

Degene die als beste weet wie er legitiem naar zijn of haar dossier kijkt, is de patiënt zelf. Via de website VZVZ kunnen deelnemers een inzageformulier invullen, waarna ze een overzicht krijgen thuisgestuurd van zorgverleners die hun gegevens hebben ingezien en zo kunnen controleren of er misbruik plaats heeft gevonden. Maar wie gaat zo iets regelmatig doen? Het klinkt toch vooral als een halfslachtige poging om de patiënt medeverantwoordelijk te maken voor de veiligheid van het systeem.

‘Wie moet je nu op misbruik aanspreken? Het toezicht ligt bij private partijen’

Terwijl de patiënt juist meer zeggenschap over zijn gegevens zou moeten hebben, zegt Guido van ’t Noordende. ‘Je moet het omdraaien. Patiënten moeten een pasje krijgen waarmee ze artsen toestemming verlenen om in hun dossier te komen.’ Dat vindt ook Mark Koek van Fox-IT. ‘Alleen op de afdeling Spoedeisende Hulp geef je de medewerkers de bevoegdheid om de gegevens in te zien zonder de patiëntenpas. Dat is veel beheersbaarder.’

Opvallend is dat de grote maatschappelijke onrust over het EPD volledig verstomd lijkt. Lange tijd was het elektronisch patiëntendossier samen met de OV-chipkaart hét voorbeeld van een megalomaan ICT-project met dramatische gevolgen voor de privacy van de burger. Alle bezwaren van toen staan nog steeds overeind. ‘We zijn er zelfs op achteruitgegaan,’ beweert hoogleraar computerbeveiliging Bart Jacobs van de Radboud Universiteit Nijmegen. Hij was een van de experts die drie jaar geleden hun zorgen uitten in de Eerste Kamer. Juist vanwege de risico’s die een zo groot en kwetsbaar systeem met zich meebracht, pleitte Jacobs uiteindelijk vóór het EPD. Dan was het wettelijk verankerd dat de verantwoordelijkheid bij het ministerie van VWS lag. Jacobs vindt het daarom jammer dat de Eerste Kamer de plannen voor het landelijk EPD heeft getorpedeerd. En gevaarlijk dat de verantwoordelijkheid nu bij belanghebbenden uit het veld ligt. ‘Wie moet je nu op misbruik aanspreken? Het toezicht ligt bij de private partijen, terwijl het gaat om een infrastructuur met een hoog publiek gehalte. Het is alsof je taxichauffeurs zelf de wegen aan laat leggen. En als het misgaat, diezelfde taxichauffeurs de klacht laat afhandelen.’

Helemaal zonder onafhankelijke controle is het systeem niet. Mocht het écht misgaan, dan krijgt de VZVZ een tik op de vingers van het College bescherming persoonsgegevens (CBP). ‘De bescherming van medische gegevens in het algemeen en het landelijk EPD in het bijzonder staan heel hoog op onze agenda,’ laat een CBP-woordvoerder weten. ‘Medische gegevens zijn gevoelige persoonsgegevens en vallen onder een strikter beschermingsregime. Daarnaast is het landelijk EPD een grootschalige gegevensverwerking die grote groepen mensen raakt.’

Kortom, het CBP zit er bovenop. Maar deelt de privacywaakhond de zorgen van IT-experts? Daar wil het College nu niet op reageren. ‘In het doorstartmodel zagen we op dit punt geen bijzondere risico’s, maar dit zegt niets over de praktijk,’ klinkt het formeel. ‘Eventueel onderzoek naar de praktijk van het landelijk EPD en eventuele handhaving zal in ieder geval niet eerder dan 1 januari 2013 starten.’ En het Nationaal Cyber Security Centrum (NCSC)? Dat waakt immers over de digitale veiligheid van de Nederlandse burger? De woordvoerder: ‘Het EPD? Fris mijn geheugen even op.’ Dan, minuten later: ‘Private partijen zijn zelf verantwoordelijk voor hun digitale veiligheid. Pas als er een aanval van buitenaf komt, kunnen wij helpen.’

08-11-2012

Vind ik leuk  6  Tweeten  11

3

1 comment

0 Stars



Leave a message...

Discussion ▾

Community

▾

**Ron** • 10 days ago

De oplossing is simpel, de beheerder van de database is verantwoordelijk voor alle directe-, indirecte- en vervolgschade.

Dit kan oplopen tot verhuizing, ander werk, naam verandering en elke combinatie hiervan.

Eens kijken of ze dan leren omgaan met ICT !

0 △ ▾ ▾ • Reply • Share ›

ALSO ON VRIJ NEDERLAND

What's this? ✕

VN MediagidsStemmingmakerij over regeerakkoord

33 comments • 10 days ago



maxim renders — Een trefzekere constatering Kees. dank daarvoor. Het wordt vaak gezegd: er is weer niks op tv. Maar ...

Veelverdieners ongewenst - Vrij Nederland

31 comments • a month ago



Peter Klein — zeggen dat ' de arbeiders de partij hebben verlaten',- en daar ben je dan tientallen jaren lid voor ...

Israël-hater - Vrij Nederland

1 comment • a day ago



VT — De term Sovjetkabinet verraadt anders ook weinig affiniteit met bronnen.

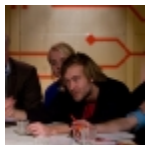
VN MediagidsHet Midden-Oosten wacht gedonder

1 comment • 2 days ago



shuri — Je ziet nu dat Israel slechts een heel klein deel van het probleem is. Het echte probleem is de kuns...

Over Maurits Martijn



Maurits Martijn (1981) is sinds oktober 2007 redacteur van Vrij Nederland. Daarvoor coördineerde hij de succesvolle debatreeks 'Vrij Nederland in debat'.

Meer van Harry Lensink, Maurits Martijn

- [Hoofdpijndossier](#)
- [EHBO-les voor stekers](#)
- [Veelverdieners ongewenst](#)

- [Donald G. eerder genoemd als moordopdrachtgever](#)
- [Beloning voor de klikkende boef](#)

Meest gelezen artikelen

- [Malware op VN.nl: opgelost](#)
- ['Israël-hater'](#)
- [Het Midden-Oosten wacht gedonder](#)
- [Vrij Nederland IDFA dagen 2012](#)
- [Stemmingmakerij over regeerakkoord](#)

Volg ons



[Volg VN op Twitter](#)



[Volg VN op Facebook](#)



[Updates via RSS](#)



[Nieuwsbrief](#)

[vn.nl Hoofdpijndossier](#)



[Probeer VN
nu](#)

12 Weken voor 15 Euro



[Bestel nu!](#)

VN-IDFA dag 2012



[Nu geopend](#)

VN Wijnwinkel