“L-EPD moet samenstelsel van techniek worden”

Dit opiniestuk verscheen voor het eerst op Qure (http://www.qure.nl), en is op uitnodiging van qure geschreven. Reproductie met toestemming.

08-apr-2011 EPD-wet weg. Wat nu?

Guido van ’t Noordende lanceert alternatief

Een landelijk EPD is best mogelijk, maar dan met een samenspel van technieken, én meer kleinschalig.

Dat zegt Guido van ’t Noordende, die sinds begin 2010 gaten schoot in de beveiliging van het landelijke EPD. Hier is zijn bijdrage.

Het doek is gevallen voor het landelijke EPD. Ik speelde hier een niet-onaanzienlijke rol in, door mijn kritiek op de architectuur en het Landelijk SchakelPunt (LSP), en op het EPD-wetsvoorstel zelf.

De stopzetting van het LSP was voor mij geen vooringenomen doel of uitkomst. Maar gaandeweg werd voor mij, zoals kennelijk ook voor de Eerste Kamer, de conclusie onontkoombaar dat op deze weg niet doorgegaan kon worden. De grootschaligheid en de hoge mate van centralisatie zie ik als de grootste problemen.

Het is belangrijk om dit moment te gebruiken om met een andere bril naar ICT-systemen in de gezondheidszorg te kijken. Vooral de schaal daarvan is een belangrijk punt. Bij grootschaligheid blijken de risico's -op velerlei vlak- te groot en fundamenteel. Er is een minder uniforme en grootschalige manier nodig om ons zorgICT-landschap in te vullen.

Als belangrijke uitspraak van de Eerste Kamer zie ik dat de regie van de patiënt over de ontsluiting van gegevens essentieel is. Dat ligt zowel in de toestemmingseisen, als in de toegang tot gegevens via een (regionale) infrastructuur.

Juist bij pull-systemen zoals het L-EPD (zowel landelijk als regionaal) is de mogelijke opvrager niet bij voorbaat bekend. Je moet er dan maar op vertrouwen dat alles goed gaat. Ervaringen met andere systemen wijzen uit dat teveel vertrouwen niet verstandig is.

Vooral bij grootschalige *pull*-gebaseerde systemen zijn er flinke risico's van ongeoorloofde toegang,

zeker als de patiënt niet betrokken is bij de autorisatie van zorgverleners. Als er daarnaast weinig controle door de patiënt vooraf is (over wat in het systeem mag worden gezet) kan het resultaat geleidelijk onbeheersbaar worden. Dat geldt nog sterker als gegevens heel lang in het systeem blijven -en als steeds nieuwe EPD-functies worden toegevoegd.

Mogelijk zijn zulke systemen goed voor de zorg. Maar ze bieden geen goede basis voor privacybescherming van burgers op de lange termijn. Dat is essentieel is voor het vertrouwen van burger en zorgverleners in de gebruikte systemen.

Er zijn alternatieven. Pull-systemen kunnen wel degelijk nuttig zijn bij kleinschalig gebruik, zoals tussen direct samenwerkende zorgverleners. Maar dan liefst niet voor teveel zorgverleners en niet teveel verschillende functies via één enkel systeem. Teveel concentratie van informatie of toegang is altijd risicovol. Het is dus belangrijk deze systemen klein te houden.

Naast kleinschalige regionale systemen kan worden gecommuniceerd met *push* berichtenverkeer (beveiligd, natuurlijk). Dat heeft een wettelijke basis, omdat het gaat om gerichte communicatie in het kader van de behandeling van een patiënt.

Zulk berichtenverkeer kan prima in combinatie met de UZI-pas, de smartcard voor artsen. Die pas is geschikt voor inloggen op systemen binnen zorginstellingen én voor authenticatie binnen regionale EPD’s, maar ook in ketenzorg- en andere systemen.

De UZI-pas maakt het mogelijk om "aan de bron" te controleren en vastleggen wie toegang tot een dossier heeft gevraagd. Dit maakt systemen veiliger.

De UZI-pas wordt een nóg sterker middel, als er goede normen en mechanismen zijn om medewerkers te mandateren (scherper dan in de laatste EPD-versie). Dit zou ook lokaal binnen zorginstellingen gebruikt moeten worden.

De Eerste Kamer stuurt ook aan op een “zorgpas”. Dit juich ik erg toe. Een zorgpas, op moderne leest geschoeid, is een erg elegante methode om de patiënt voldoende regie te geven. Zo’n zorgpas kan opslag en authenticatiemechanismen (via sleutels) bevatten, om regionale systemen beter te beveiligen. Als de patiënt hier voor kiest, biedt het betere beveiliging.

Eén aspect dat het afgeblazen L-EPD onveilig van maakte, was dat de patiënt niet betrokken was bij de autorisatie van zorgverleners -zelfs niet voor gevoelige soorten informatie.

Een “zorgpas” zou een smartcard moeten zijn waarop opslag van gegevens mogelijk is, én waar cryptografische sleutels op staan. Opslag van data is belangrijk, voor o.a. SOS- en noodgegevens (die ook direct in ambulance of buitenland uitleesbaar zijn) en voor vastlegging van gegevens bij patiënten die helemaal geen vertrouwen hebben in elektronische uitwisselsystemen. Er kan tegenwoordig heel veel informatie op één kaartje.

De cryptografische sleutels op de pas zijn bruikbaar voor het autoriseren van artsen in (regionale) EPD's, maar ook voor veilig inloggen in bijvoorbeeld zorgportalen en *Personal Health Records* (PHR's, zorgportalen) door de patiënt zelf.

Voor spoedgevallen zou je toegang zonder toestemming door de patiënt kunnen toestaan, voor een beperkte set van noodgegevens. Maar een expliciete autorisatie van artsen (via de zorgpas) is nodig voor andere gegevens. Autorisatie kan bijvoorbeeld met certificaten met beperkte geldigheid, waardoor een arts (of diens medewerkers) nog enige tijd een dossier kunnen raadplegen, ook als de patiënt er niet bij is.

Ook hierbij blijft de kleinschaligheid van de techniek belangrijk, vanwege de gevoeligheid van centrale verwijsindices, logbestanden, etc. Dus geen grote schakelpunten. Wellicht moet de patiënt zelf zeggenschap, een keuze, houden over op welke schaal gegevens uitgewisseld mogen worden.

Een zorgpas kan *push* berichtenverkeer trouwens niet vervangen. Dat werkt altijd, ook als de patiënt zijn pasje niet bij zich heeft, of geen toestemming heeft gegeven voor gebruik van een schakelpunt. Een landelijk postbussensysteem (decentraal, bij de zorgverlener) is dus hoe dan ook essentieel.

Hoe bovenstaande systemen en technieken effectief kunnen samenwerken, bijvoorbeeld met behulp van push communicatie en zorgpassen, vergt nog wat denkwerk en technische uitwerking. Maar ik ben ervan overtuigd dat een EPD-inrichting langs deze lijnen uitvoerbaar is én recht doet aan de wens en het grondrecht van patiënten op regie over de eigen medische gegevens.

Een aanpak zoals hierboven geschetst, is veilig en niet overmatig ingewikkeld. Ook sluit die aanpak aan bij wat elke burger en arts gewend is: pasjes meenemen, bellen en mailen met collega's, dossiers delen met collega's die we goed kennen, etc. De techniek is overzichtelijk en niet te complex, en blijft daardoor beheersbaar.

Het lijkt me wel belangrijk dat VWS en Nictiz doorgaan met de ontwikkeling van standaarden voor registratie en uitwisseling van patiëntgegevens. Dit moeten open, flexibele, breed gedragen en liefst eenvoudige standaarden zijn. Deze standaarden moeten simpel en bruikbaar zijn voor datatransport via zorgpassen, voor kopiëren van medische gegevens naar een zorgportaal of een USB-stick, etc.

De markt kan de rest doen. Zo nodig is een centrale noodgegevens-database denkbaar, die gevuld wordt na toestemming van de patiënt. Maar die gegevens kunnen ook gewoon op de zorgpas, als een briefje in de portemonnee niet volstaat.

Het is nu tijd voor een heroriëntatie op de gebruikte technieken voor uitwisseling van medische gegevens, en op de inrichting van het systeem als geheel. Het is mijn hoop dat Nederland nu het moment pakt om de nodige technieken te ontwikkelen voor een bruikbare, veilige en privacy-vriendelijke uitwisseling van gegevens.

Dan kunnen we op termijn écht vooruit lopen met EPD-ontwikkelingen - ook op de rest van de wereld.

Guido van 't Noordende

Onderzoeker Universiteit van Amsterdam