EPD Opinie

Bart Jacobs, Hoogleraar Computerbeveiliging
Institute for Computing and Information Sciences,
Radboud Universiteit Nijmegen

(Geschreven op uitnodiging van Eerste Kamer Commissie VWS/JG)

Versie van: 28 oktober 2009

Het onderwerp 'Elektronische Patiëntendossier' (EDP) is veelomvattend en ingewikkeld. Ik heb niet de pretentie het geheel te overzien, en geef mijn opinie allereerst vanuit mijn achtergrond op het gebied van de informatiebeveiliging, maar daarnaast ook enigszins vanuit mijn positie als zorgconsument. Een eenduidige opinie kan ik helaas niet bieden. Enerzijds vind ik het doodeng om zo gevoelige informatie zo gemakkelijk voor zo veel mensen toegankelijk te maken. Anderzijds zie ik dat eenvoudige alomtegenwoordige toegang (ook) tot medische gegevens een zekere onvermijdbaarheid heeft en nu al door medische professionals op allerlei manieren eigenstandig vanuit behoefte "van onderop" gerealiseerd wordt. In dat licht is het beter deze zaken systematisch, uniform, transparant en met eisen en waarborgen omkleed "van bovenaf" te reguleren.

In het onderstaande zullen een aantal zaken puntsgewijs nader worden uitgewerkt. De term 'EPD' zal daarin generiek gebruikt worden, voor een landelijk patiëntendossier dat toegankelijk is via het beoogde landelijke schakelpunt (LSP), via het burgerservicenummer (BSN) van de patiënt. Het EPD zelf is hierbij gefragementeerd aanwezig bij de verschillende hulpverleners die te maken hebben (gehad) met de patiënt. De precieze invulling en omvang van het EPD (bijv. WDH, EMD, of meer) is daarbij ondergeschikt. De zorgvuldigheid gebiedt mij toe te voegen dat ik vanuit een "helicopterview" schrijf, zonder gedetailleerd zicht op de implementatiepraktijk (van bijv. het LSP of de verschillende computersystemen die gebruikt worden bij zorgaanbieders).

Regulering van toegang tot the EPD

1. Erg veel zorgverleners krijgen een UZI-pas, namelijke alle zogenaamde "artikel 3" en "artikel 34" beroepen in de wet BIG; er zijn aantallen van 200 tot 300 duizend genoemd, maar ook van meer dan een half miljoen mensen.

2. Er is geen technisch afgedwongen beperking tot "behandelrelatie": iedere UZI-pas geeft in principe — bijv. in handen van een kwaadwillende —

toegang tot alle landelijke dossiers. Wel is er beperking van "rollen" (arts, verpleger, etc.). Verlies van één enkele pas met bijbehorende PIN-code is potentieel een nationale ramp.

3. Zorgverleners zijn getraind om zorg te verlenen en om daarbij zorgvuldig om te gaan met patiëntgegevens. Ze zijn echter niet getraind in informatiebeveiliging: zorgvuldig omgaan met logins, wachtwoorden, UZI-passen, authenticatie van patiënten, etc. Zie bijv. het schokkende NOVA item van 12 nov. 2008 (zoek op YouTube onder "NOVA EPD ziekenhuis"). Iedereen in de sector herkent dit gedrag.

4. De betrouwbaarheid van het EPD is mede afhankelijk van de betrouwbaarheid van het BSN en van de controle daarvan. Dit punt wordt in de praktijk echter nog nauwelijks ingezien: "ik ben toch geen politieagent" verzucht menig zorgverlener.

5. Indien iemand anders — bijvoorbeeld een onverzekerde — zich ongemerkt als mij voor kan doen kunnen er verkeerde gegevens in mijn dossier terecht komen. Door landelijke koppelingen zullen zulke fouten niet slechts locaal aanwezig zijn, maar zich propageren waardoor de kans groot is dat ik er daadwerkelijk (nadelig) mee geconfronteerd zal worden. Het zal nog moeten blijken in welke mate ik (of een nabestaande) een nalatig controlerende zorgverlener aansprakelijk kan stellen voor de schade door vervuiling van mijn dossier.

6. Gemakkelijke (online) toegang voor de patiënt tot de loggegevens van het eigen EDP is een cruciaal controlemiddel. Zorgverleners zullen er dan ook rekening mee moeten houden dat ongepast gluurgedrag eerder opgemerkt zal kunnen worden, en tot klachten zal leiden. Belangrijk is ook dat patiënten in principe ook toegang tot hun dossier selectief, voor bepaalde zorgverleners af kunnen sluiten.

7. Toegang van patiënten tot hun eigen EPD zal mogelijk een grotere invloed hebben op de communicatie tussen zorgverlener en patiënt dan op de communicatie tussen zorgverleners onderling (zoals beoogd). Het is van belang de infrastructuur flexibel op te zetten zodat ook voor patiënten nuttige toevoegingen in de toekomst mogelijk zijn (doorgave van eigen metingen, online consult, etc.).

Beveiligingsrisico's

1. Het grootste risico zit op dit moment waarschijnlijk niet in de ICT-infrastructuur (LSP) maar in de slordige houding van de medische sector mbt. informatiebeveiliging.

2. Indien die landelijke infrastructuur door kwaadwillenden (insiders of outsiders) gecompromiteerd raakt is dat een nationale ramp.

3. Vertrouwelijkheidsschendingen kunnen zeer kwalijk zijn, door reputatieschade, of misbruik door anderen (verzekeraars, werkgevers, financiële instellingen, e.d.); zulke schendingen zijn niet repareerbaar. Inzage in loggegevens zal in enige mate een rem zetten op dergelijke schendingen.

4. Integriteitsschendingen (aantasting van juistheid van gegevens) bijv. door invoer- of communicatie-fouten of door hacking kunnen levensgevaarlijk zijn, maar kunnen, mits tijdig ontdekt, hersteld worden. Speciale software kan integriteit deels bewaken.

5. Beschikbaarheid van het EDP voor zorgverleners wordt cruciaal. Aantasting daarvan maakt niet-locale informatietoegang in de zorg onmogelijk. Hieraan worden terecht hoge eisen gesteld. Betrouwbare toegang tot locale systemen is echter nog belangrijker want falen daarvan legt de zorg plat.

6. Toegang tot het eigen dossier vereist een extra "face-2-face" controle binnen het huidige DigiD. Zulke toegang brengt ook nieuwe risico's, en mogelijke spanningen of conflicten met zich mee: oneigenlijke toegang onder druk van een werkgever, of misbruik van medische gegevens bij een scheiding of erfenis. Dit zal ongetwijfeld tot incidenten leiden. Mensen hebben de afgelopen jaren echter ook geleerd met een zekere zorgvuldigheid online om te gaan met hun bankgegevens.

7. Het EPD geeft patiënten de mogelijkheid om toegang tot hun dossier te beperken, of zelfs helemaal af te sluiten. Het valt te verwachten dat mensen dat in grotere aantallen gaan doen bij het optreden van serieuze beveiligingsincidenten. Deze "feedbackloop" houdt de verantwoordelijken voor het systeem onder gezonde druk.

8. Naast het beoogde doel van verbetering en optimalisering van medische zorg zal het EPD ook nieuwe kwetsbaarheden en risico's met zich meebrengen, met name op het gebied van beveiliging, identiteitsfraude, en propagatie van foutieve gegevens.

Eisen

1. Nictiz stelt "GBZ" eisen (voor: goed-beheerd zorgsysteem) aan systemen van zorgverleners die aangesloten worden op het LSP en "ZSP" eisen (voor: zorgserviceprovider) aan leveranciers voor dataverbindingen tussen zorgverleners en het LSP.

2. In het algemeen kan er een spanningsveld ontstaan tussen het vasthouden aan eisen en druk om voortgang te maken.

3. Regionale initiatieven tot koppeling van medische gegevens zijn echter niet of nauwelijks onderworpen aan strenge eisen, met name met betrekking tot

beveiliging. Het (landelijke) EPD moet daar een eind aan maken, via een nationaal gereguleerde infrastructuur, die zorgverleners en patiënten uniforme en herkenbare toegang moet bieden. Het opschonen van deze (goedbedoelde) locale houtje-touwtje initiatieven — bekritiseerd door het College Bescherming Persoonsgegevens en de Inspectie voor de Gezondheidszorg — is een positieve bijkomstigheid van het landelijk EPD. Misschien is het uiteindelijk wel het sterkste argument om het EPD überhaupt in te voeren.

Aandachtspunten

1. Toegang met UZI-passen moet technisch beperkt worden tot "behandelrelatie" of "noodknop" (met gegarandeerde audit).

2. EPD-beveiliging is nooit "af" en vergt een continu proces van monitoring, rapportage en verbetering. Dit moet expliciet ingericht worden, met nadrukkelijke aandacht voor o.a. LSP, gebruik van UZI-passen, patiëntentoegang via DigiD, locale systemen.

3. Het EPD vereist nieuwe zorvuldigheid in het gedrag van medisch personeel en nieuwe beveiligingseisen aan locale computersystemen. Gezien de notoire eigenzinnigheid en fragmentatie van de medische sector is dit een niet te onderschatten aspect van het EPD dat niet zomaar gerealiseerd is.

4. Daadwerkelijk gebruik van het landelijk EPD kan sterk gestimuleerd worden door het gebruik van de huidige regionale systemen — met al hun zwakheden/overtredingen mbt. beveiliging/privacy — gewoonweg te verbieden.

5. De medische sector zal door het EPD gedwongen transparanter moeten werken. Het is onduidelijk hoe nieuw geconstateerde misdragingen (gluren, verlies van pas & code, falende identiteitscontrole) afgehandeld worden: in de tuchtsfeer, of ook via het civiele recht.

6. Het EPD zal een nieuwe dynamiek met zich meebrengen waarin de patiënt een cruciale rol speelt.