FACULTY OF SCIENCE

Bart Jacobs

EPD, privacy & security

Radboud University Nijmegen

Actualiteit

(© Kidsweek, 6 feb. 2009)

Inhoud

I. Achtergrond

Wie is die man eigenlijk?

- Hoogleraar computerbeveiliging, in Nijmegen & Eindhoven (studie: wiskunde + filosofie)
- Betrokken oa. bij ***e-paspoort***, ***OV-chip***, ***rekeningrijden***, ***elektronisch stemmen*** (lid cie. Korthals Altes over herinrichting stemmen)
- O.a. geïnteresseerd in “identiteitsmanagment”
- Auteur van online boek *De Menselijke Maat in ICT*, zie `www.cs.ru.nl/B.Jacobs/MM`

Betrokkenheid bij EPD

- Geen centraal onderzoeksonderwerp
- Geen betrokkenheid bij LSP infrastructuur (met gekoppelde zgn. *Goed Beheerde Zorgsystemen*)
- Wel advies voor ministerie VWS over toegang tot eigen EPD (dec.’08)
- Kleine rol in maatschappelijk debat (oa. interviews in kranten/SynthesHis, okt’08)

Grote maatschappelijke vragen & zorgen

Computerbeveiliging

- Regulering van toegang tot gevoelige digitale gegevens, zoals:
  - militaire of industriële gegevens
  - privacy-gevoelige gegevens, bijv. over gezondheid (EPD), communicatie, financiën
- Vereist juiste mix van technologische, organisatorische & juridische maatregelen
- Focus niet op functionaliteit van ICT, op maar mogelijk misbruik (vak heeft hoge kwajongensmentaliteit)

Privacy I

- Mensen hebben vele rollen/sferen (werk, sportclub, kerk, thuis, patiënt, etc)
- Essentieel aan privacy is om zelf informatie tot een rol te kunnen beperken
- Sterk gelieerd aan persoonlijke autonomie
- Keuze belangrijk; groot verschil tussen:
  (1). vrijwillig in je blootje lopen
  (2). gedwongen worden om in je blootje te lopen

(Als velen (1) doen is dat geen reden om (2) op te leggen)

Privacy II

- Velen bereid persoonlijke info te delen, tbv.
  - terrorismebestrijding
  - zelfexpressie/communicatie (Hyves etc)
- Echter reserves mbt. medische gegevens
  - (naief) vertrouwen in zorgvuldigheid van zorgverleners
  - maar bijv. niet in verzekeringsmaatschappijen
  - Brede opvatting: medische gegevens moeten in medische/vertrouwelijke sfeer blijven!

II. EPD architectuur

Drie mogelijke architecturen

I. ***Centraal:*** alle dossiers van iedereen in één grote databank

II. ***Decentraal:*** iedere patiënt heeft eigen dossier in bezit (en neemt dat steeds mee)

III. ***Pointer:*** zorgverlener beheert dossiers van eigen patiënten, maar maakt ze centraal toegankelijk, via verwijzingen

Ad I: centrale opslag

- Ogenschijnlijk simpele, naieve aanpak, maar met grote problemen:
- Concentratie van gevoelige gegevens risicovol:
  - privacy (denk aan omvallen databank)
  - beveiliging (denk aan aanslag)
- Centrale database is ook *performance bottleneck*.

Geen goed idee!

Ad II: decentrale opslag

- Geef patiënten hun dossier in eigen beheer
- Niet ongebruikelijk (Fr, It, . . .)
- Verschaf bijbehorende infrastructuur: online datakluis,
  - (cryptografische) sleutels in handen van burger
  - standaardinstellingen, met variatie
  - kan ook gedeeltelijk met smart card (D)
- Vereist vertrouwen in burgers!

Aansprekend idee, maar niet gekozen in NL

Ad III: pointer structuur

- In NL as: *Landelijk Schakelpunt* (LSP)
- Mijn medisch dossier is gefragmenteerd:
  - opslag bij zorgverleners (in principe)
  - centraal in LSP staan verwijzingen daarnaar
  - gebruik door anderen via deze verwijzingen, met BSN
- Patiënt heeft online inzage, maar zelf geen gegevens; anderen beslissen over toegang

Blik terug

- ***Traditioneel:*** huisarts heeft mijn dossiermap in afgesloten praktijk-kast; redelijk vertrouwd
- ***PC van arts:*** langzaamaan ingevoerd
  - overgang zichtbaar/begrijpelijk voor patiënt
  - arts wil beheer/beveiliging niet zelf doen
  - maar is (en voelt zich) wel verantwoordelijk
- ***HIS:*** "stiekem" ingevoerd
  - onduidelijk waar mijn gegevens staan
  - mij (patiënt) is niks verteld/gevraagd
  - misschien neem ik dossier liever mee naar huis

III. Kanttekeningen

Waarom eigenlijk EPD?

- Verbetering zorg . . .
- door betere onderlinge communicatie zorgverleners
- en daardoor minder fouten
- en daardoor minder lijden en minder kosten
- meer (statistische) informatie

Schatting: jaarlijks ± 1000 doden door onjuiste behandeling door onjuiste/onvolledige gegevens

Twijfels van een niet-medicus

- Onderbouwing lijkt overtuigend, maar:
  - Verplegers blijken niet te kunnen rekenen; hoeveel doden door foute doseringen?
  - Ambulancepraktijk hoeft geen EPD: snel behandelen staat voorop, daarna pas opzoeken
  - Artsen hebben eigen stijl/terminologie/handigheid; hoeveel aanklik/invulfouten & misinterpretaties?
  - Propageren van fouten door landelijke koppeling (onverzekerde misbruikt mijn BSN, krijgt zorg op mijn naam, en voegt verkeerde bloedgroep in mijn dossier)

EPD introduceert ook nieuwe risico's

Kanttekeningen, vanuit beveiliging

- ***Confidentialiteit:*** onbevoegden kunnen dossiers inzien
  - onjuiste toegang / lekken / hacken
  - herstel confidentialiteit niet mogelijk
- ***Integriteit:*** gegevens kloppen niet
  - bijv. onjuiste invoer / persoon
  - erg schadelijk, maar herstel in principe mogelijk
- ***Beschikbaarheid:*** gegevens niet toegankelijk
  - wordt essentieel voor medische praktijk

Focus hier

- Niet op infrastructuur (LSP, GBZ) met bijbehorende risico's
- Maar op regulering van toegang
  - voor zorgverleners via "Uzi-pas"
  - voor zorgconsumenten via DigiD
- Drie basis vragen:
  - ***Identificatie:*** wie ben je?
  - ***Authenticatie:*** hoe bewijs je dat?
  - ***Autorisatie:*** wat mag je?
- Grote zorg: *identiteitsfraude*

Met Karel van de computer . . .

Filmpje!

Karel Ornstein belt 'n afdeling van 'n ziekenhuis
(NOVA, 12 nov. 2008)

UZI-pas I

- UZI = Unieke Zorgverlener Identificatie
- UZI-pas = chipkaart voor zorgverleners voor EPD-toegang (identificatie, authenticatie, autorisatie)
- Ongeveer 385.000 voorzien (1 op 50 in NL!)
- werkt alleen met persoonlijke 6-cijferige PIN
- geen beperking tot "behandelrelatie"
- gebruik wordt gelogd (wie, wanneer, welk dossier)
- logs zijn zichtbaar voor patiënten
  (en voor systeembeheerders, natuurlijk)

UZI-pas II

- ***theorie:*** gebruik is strikt persoonlijk
- ***praktijk:*** één persoon is steeds ingelogd, velen gebruiken die pas/identiteit
  - gevaarlijk ivm. onbevoegde toegang
  - ook aansprakelijkheidsrisico
- Aanvraag / gebruik / vervanging omslachtig
- Vereist nieuwe werkwijze & zorgvuldigheid
- Geruchten over problemen met UZI-passen
  (PIN code lijkt te achterhalen)

Wanneer toegangscontrole tot EPD?

- ***Vooraf***
  - lijkt logisch, op basis van behandelrelatie
  - die relatie is echter niet eenduidig
  - mogelijk beperkend in noodgevallen
- ***Achteraf***
  - flexibel
  - mogelijk meer misbruik

Gekozen is voor combinatie

Toegang tot eigen dossier

- Verplicht volgens wet (WGBO en WBP)
  - Gericht op inhoud van dossier
- Met EPD nieuwe mogelijkheden
  - ook logs zichtbaar (wie, wanneer, wat)
  - ook beperking toegang (deze arts wel, die niet)
  - zelfs totale afsluiting van eigen dossier

Krachtig controlemechanisme / nieuwe dynamiek

Autenticatie voor toegang via DigiD

- Huidig DigiD is te zwak: wachtwoord/SMS authenticatie aan te vragen per post
- Face-2-face authenticatie ontbreekt
- Plan: versterk DigiD met "SMS+"
  - burger moet eenmalig naar gemeentehuis
  - authenticeert zich traditioneel (bijv. paspoort)
  - ontvangt ter plekke SMS op bijbehorende 06
  - bewijst juiste koppeling 06 aan persoon

IV. Gevolgen

Zorgverleners

- Traditioneel goed gevoel voor privacy . . .
- maar weinig affiniteit met informatiebeveiliging
- Toch wordt dit nu indringend vereist
- Incidenten schadelijk voor de sector:
  - onterecht gluren in dossiers (bekenden/BNers)
  - slordigheid met UZI-passen
  - slecht beveiligde PCs of open netwerken
- Pers zal hier bovenop zitten

Reputatie zorgsector op het spel!

Zorgconsumenten

- Nieuwe keuzes:
  - wel of niet meedoen met EPD?
  - zo ja, in welke mate? (instellen wie wat mag)
- Nieuwe verantwoordelijkheden:
  - zorgvuldig omgaan met DigiD (als EPD-toegang)
  - mogelijk ook consistentie eigen dossier (detectie foute invoer / identiteitsfraude)
- Ultieme optie: massale terugtrekking uit EPD, bijv. na groot incident
- Belangrijk als *balancing force*

V. Conclusies

Belangrijke punten I

- EPD beveiligings/privacy risico's:
  - vooral gedrag zorgverleners, niet techniek
  - vergen groter bewustzijn mbt. informatiebeveiliging (wie is dit? hoe weet ik dat zeker? wat mag die?)
- Incidenten zullen ongetwijfeld optreden
  - individuele gevallen, bijv. door eigen schuld
  - hele praktijk/afdeling "open" (waarschijnlijk)
  - heel ziekenhuis open (zelden, hopelijk)
  - heel LSP open (nationale ramp; faillissement)
- Eigen inzage en afsluiting belangrijke controle/druk middelen

Belangrijke punten II

- EPD oorspronkelijk voor verbetering communicatie *tussen zorgverleners*
  - maar ook invloed op zorgverlener–zorgconsument (juist vanwege inzagerecht)
  - vereist meer transparantie & verantwoording
- Andere houding zorgverleners vereist?
  - bijv. zet 2 schermen op je bureau, één zodat patiënt altijd mee kan kijken in eigen EPD

Belangrijke punten III

- Problematisch: *function creep* mbt. EPD
  - oorspronkelijk voor doel A; later ook doel B
  - ruimer gebruik tast vertrouwen & waarde EPD aan (gevolg: er wordt minder opgeschreven)
  - bijv. EPD-toegang voor bedrijfsarts in zorgrol
  - politiek besluit hierover; terughoudendheid vereist.
- Verbeteringen:
  - opruimen locale ad hoc netwerken
  - uniforme toegang/interface voor burgers
  - zorgverleners gedwongen tot zorgvuldige toegang & transparantie

Wat doe ik zelf?

- Voorlopig zelf *geen* EPD
  - "kat uit de boom kijken" (beetje laf)
  - kinderziektes moeten er nog uit
  - discipline moet er nog inkomen
- Op dit moment (vooraf) is mij onduidelijk of voordelen opwegen tegen nadelen/risico's
- Uiteindelijk "decentrale" voorkeur, met gegevens onder beheer van burgers.

Dank voor de aandacht!

Slides te vinden op:

www.cs.ru.nl/B.Jacobs/TALKS