Privacybewuste oppositie in VK buitengesloten bij discussie over big-data in de zorg

In het Verenigd Koninkrijk blijkt de privacy-bewuste oppositie tegen het vermarkten van big-data in de zorg op een heel bijzondere manier buiten spel te zijn gezet. In de adviesraad, die daarover moet adviseren, zijn deze groeperingen niet meer opgenomen, evidente voorstanders wel. 8 februari stond op de website The Register een in mijn ogen schokkend relaas hoe men tegenstanders in de privacy-discussie rond medische big-data buiten spel zet. De National Health Service(NHS) heeft rond 2012/2013 het Health and Social Care Information Centre (HSCIC) opgericht met databases, waarin geanonimiseerde patiëntengegevens van huisartsen worden opgeslagen. Het is de bedoeling, dat Care.data, een onderdeel van de NHS, deze gegevens beheert. De opzet is dat deze big-data van de zorg als basis dienen voor het optimaliseren van de zorg. Daarnaast wil men deze data ook verkopen aan derden. Ondanks negatieve ervaringen in o.a. 2014 met het vermarkten van medische data(ziekenhuisgegevens) wil de NHS doorgaan met dergelijke praktijken.

Discussie

De discussie over de opzet en bedoelingen van Care.data werd

in 2014 gestroomlijnd door het opzetten van een Advisory Group, die zeer breed van opzet was. Die Advisory Group werd in 2015 opgeheven en vervangen door de Strategic Oversight Board(SAB). Er is geen enkele ruchtbaarheid gegeven aan het opheffen van de Advisory Group. Alleen uit een overzicht van wat besproken was op een Care.data-meeting op 19 oktober 2015 wordt dit duidelijk. Zelfs de website van de opgeheven Advisory Group, is intact gelaten en is nu nog op het internet te vinden . In de SAB blijken twee zeer kritische organisaties op het gebied van privacy niet meer opgenomen te zijn. Het gaat om medConfidential en Big Brother Watch. Daarentegen is een organisatie als Patients4Data die gelieerd is aan een biotech-bedrijf en een apart voorstander van zorg-big-data gebruik, wel in de SAB opgenomen. Het is een schokkende manier om de tegenstanders de mond te snoeren en tegelijkertijd extra voorstanders in huis te halen.

Anoniem?

De verzamelde gegevens worden gecodeerd opgeslagen samen met de geboortedatum, het geslacht, de postcode en het NHS-verzekeringsnummer. De data zouden gepseudonimiseerd worden. De genoemde persoonskenmerken zouden nodig zijn om de data te kunnen koppelen met data uit andere databases. Er zijn mogelijkheden gecreëerd om de patiënten toch te identificeren door middel van zogenaamde “identifiers”. Die ontsleutel-mogelijkheid zou buiten het Care.data-systeem worden opgeslagen, maar het feit dat zulks mogelijk is, verontrust kritische burgers en organisaties. Ook de universiteit van Cambridge waarschuwde, blijkens het artikel in The Register.

Het is vergelijkbaar met de situatie met de gegevens in Nederland in het DBC-Informatie-Systeem(DIS). Daar blijkt dat de gepseudonimiseerde gegevens toch door bepaalde instanties tot personen herleidbaar te zijn. Dat gaf recent de Nederlandse Zorgautoriteit(NZa) toe in een rechtszaak. Het is dus aan beide zijden van de Noordzee zo dat gegevens uit de zorg dus niet echt anoniem worden uitgewisseld.

Ont-anonimiseren

In Nederland liet Matthijs Koot in 2012 in zijn proefschrift met als titel “Measuring en predicting anonimity” al zien dat met een zeer beperkt aantal gegevens toch individuen geïdentificeerd kunnen worden. Dat zelfs inlichtingendiensten moeite hebben om metadata van personen te de-identificeren moge blijke uit een publicatie van Tamir Israel en Christopher Parsons op 3 februari 2016 op de website www.justsecurity.org. In hun artikel genaamd ”Why We Need to Reevaluate How We Share Intelligence Data With Allies” gaat het om het uitwisselen van gegevens tussen inlichtingendiensten. Gegevens die het Canadese Communications Security Establishment(CSE) verzamelde, werden uitgewisseld met geheime diensten uit de Verenigde Staten, het Verenigd Koninkrijk, Australië en Nieuw Zeeland. Edward Snowden openbaarde dit Five-Eyes samenwerkingsprogramma. De CSE mocht alleen maar metadata van communicatie van niet-ingezetenen van Canada legaal vastleggen en uitwisselen, maar niet van Canadese burgers. Die data dienden geanonimiseerd te worden. Uit het artikel van Israel en Parsons blijkt, dat het niet-identificeerbaar maken van gegevens door de CSE niet goed ging. Met computertechnieken van de overige vier partners in het Five-Eyes-programma bleek het toch mogelijk de gegevens die uitgewisseld werden tot personen, in dit geval Canadese staatsburgers, te herleiden.

Onmogelijk

Uit het bovenstaande moge duidelijk zijn dat het eigenlijk onmogelijk is om data met enkele persoonsgegevens zo op te slaan dat die volledig anoniem zijn. Het is daarom uitermate dubieus wat de NHS nu met het Care.data-programma aan het doen is. Vermarkten van medische big-data dient niet plaats te vinden en gebruik van gegevens binnen de NHS dient met strenge regelgeving omgeven te zijn. Er dient volledige openheid te zijn over wat met welke data gebeurt. Door mist te creëren rond een adviesraad en bovendien bij de voortzetting onder een andere naam notoire tegenstanders buiten te sluiten en een

uitgesproken voorstander in huis te halen bewijst de NHS en de burgers van het Verenigd Koninkrijk een slechte dienst.

Voor Nederland is het een niet te veronachtzamen waarschuwing over hoe een staatsinstelling met privacy-bewuste organisaties en individuen omgaat.

Men zij gewaarschuwd.

W.J. Jongejan

Vlekkeloos elektronisch verhuizen van dossiers tussen huisartsen niet vanzelfsprekend

Het vastleggen van patiëntendossiers door huisartsen in computersystemen is rond 1990 begonnen. De huisartsinformatiesystemen(HIS-sen) hebben een voorspoedige introductie gekend. De beroepsgroep kende als eerste in de zorg een zeer hoge automatiseringsgraad. Toch is het elektronisch correct kunnen verhuizen van dossiers tussen HIS-sen zeker geen vanzelfsprekendheid geworden. Het vergt tot op

de dag van vandaag continu zorg en aandacht van meerdere partijen in de huisartsautomatisering om dossiers goed uit te wisselen. Bovendien is het resultaat van het elektronisch verhuizen ook niet per se altijd honderd procent correct. Wat een vanzelfsprekendheid zou moeten zijn, is dat in het geheel niet. Toch zijn de laatste paar jaar grote stappen gezet, maar het proces moet continu bewaakt worden. Dat gebeurt door de Stichting Inschrijving Op Naam (ION). Die doet veel goed werk om de uitwisseling kwalitatief op peil te houden en te verbeteren. ION is opgericht in 2006 met als doel om de inschrijving van alle Nederlandse ingezetenen bij een BIG-geregistreerde huisarts te bevorderen. Dit doet de stichting onder meer door het beheer van een database waarin van elke Nederlander zijn naam, verzekeringsnummer, geboortedatum en burgerservicenummer zijn gekoppeld aan de naam en unieke zorgverlenerscode van de eigen huisarts en die van uw zorgverzekeraar. Op die manier is de inschrijving op naam bij een eigen huisarts van iedere Nederlander vastgelegd.

Problemen

In de loop de jaren is het aantal vastgelegde data sterk toegenomen, maar ook de onderlinge relaties tussen de data. Het elektronisch verhuizen van huisartsdossiers werd er dus niet eenvoudiger op. Zeer complicerend is het gegeven dat er in de loop der jaren een behoorlijke aantal HIS-sen naast elkaar in de markt bleven. Thans zijn dat: Medicom, MicroHIS, Mira CGM Huisarts, OmniHis Scipio, Promedico ASP, Promedico VDF, TetraHis en WebHIS. Acht systemen dus met elk hun eigen programmatuur en operating system. Alle HIS-sen faciliteren hetzelfde, maar elk op een eigen manier. In het verleden bleek vaak dat niet elke HIS-leverancier zich precies aan de specificaties van het verhuisbericht hield. Daardoor kon het voorkomen dat een dossier wel kon verhuizen naar een identiek HIS, maar niet naar meerdere anderen. Daardoor getriggerd werd rond 2007 speciale aandacht hieraan besteed door NEDHIS, de vereniging van gebruiksverenigingen van geautomatiseerde

huisartsen. Op 19 maart 2008 werden aan alle toenmalige HIS-leveranciers certificaten uitgereikt voor het correct implementeren van het elektronische verhuisbericht. Er kon op een redelijke goede wijze dossiers uitgewisseld worden. Dit succes was niet van lange duur. Achteraf bleek dat al na twee weken na een update van één van de HIS-sen de uitwisseling niet meer correct liep. Het bleek helaas overduidelijk dat een éénmalige inspanning om de zaken op orde te brengen niet voldoende was.

Oplossing

Er is een duidelijke noodzaak om het gebeuren rond het elektronische verhuisbericht continu te monitoren en HIS-leveranciers constant bij de les te houden, zodat niet bij een update door onvoldoende aandacht voor deze materie het niet meer werkt. De vraag was alleen, welke organisatie dat op zou pakken. Op de HIS-demo-dag in oktober 2010 kwam het probleem opnieuw aan de orde en bood de Stichting Inschrijving Op Naam (ION) aan het proces te monitoren en iedereen scherp te houden. Sinds 2012 worden daartoe door ION kruistesten gedaan. Dat houdt in dat in elk HIS een verhuisdossier wordt ingelezen dat afkomstig is van alle andere grotere HIS-sen, inclusief het eigen HIS. Vervolgens wordt in tabellen aangegeven wat foutloos, goed (met op- en aanmerkingen) of echt fout verhuisd wordt naar een ander type HIS. Door de continue aandacht en het continue testen is de kwaliteit van het verhuisde dossier in de loop der tijd sterk verbeterd, maar niet honderd procent correct voor alle HIS-sen.

Vreemde zaken

Het kan voorkomen dat bepaalde gegevens niet op een plaats terecht komen in het ontvangende HIS die daarvoor bedoeld is. Ook kan een geneesmiddelenoverzicht niet bij de medicatiehistorie belanden maar wel alles op één datum in het journaal(de centrale overzichtsplaats in het HIS). Het kan voorkomen dat een huisarts drie elektronische dossiers van een

andere huisarts krijgt en maar twee van de drie kan importeren. Soms kan het voorkomen dat een huisarts een dossier niet kan importeren. Als hij dan de oude huisarts nogmaals vraag het dossier te exporteren lukt na verzending het importeren wel. In oktober 2014 nam ik deel aan een test, waarbij een verhuisbericht vanuit OmniHis, in MicroHIS ingelezen werd, vervolgens door verhuisde naar Mira, daarna weer MicroHIS en vervolgens naar OmniHIS. Bij elke verhuizing naar een ander HIS verloor het dossier een stuk van zijn kwaliteit en soms omvang. Na een paar keer verhuizen werden teksten van diagnosen in overzichten verhaspeld, werden medicatieoverzichten opeens korter etc. etc. Het lijkt apart om zo'n test te doen, maar het is in werkelijkheid voor te stellen dat bijv. een asielzoeker in korte tijd meerdere keren verhuist en telkens in een ander systeem terecht komt.

Volledigheid

Om toch zeker te zijn dat de ontvangende huisartspraktijk de volledige omvang van het oude dossier kent, bestaat een elektronische verhuizing tegenwoordig vaak uit drie, soms vier bestanddelen.

- Het EPD-overdracht bericht (vroeger: MEDOVD)
- Een pdf-bestand van het medisch dossier ter controle
- Een zip-bestand van alle correspondentie die niet is geïntegreerd in het EPD-overdrachtbericht
- Idealiter voegt een huisarts daar een vierde document aan toe: een brief met de belangrijkste medische gegevens en aandachtspunten betreffende de patiënt.

De huisarts dient dus altijd na ontvangst aan de hand van het pdf-bestand na te lopen of alle relevante informatie correct is ingelezen in zijn systeem. Om het transport van de bovengenoemde bestanddelen mogelijk te maken heeft ION de beveiligde ZorgMail File Transfer(ZFT) in het leven geroepen.

De oude huisarts doet een upload van de dossierbestanden naar de computer van ZFT. De nieuwe huisarts kan daar de bestanden ophalen. Dat er veel al van gebruik gemaakt wordt blijkt uit de cijfers uit 2015. Alleen al in september 2015 ruim 50.000 uploads van dossiers en 40.000 downloads.

Vanzelfsprekendheid

Uit het bovenstaande moge blijken dat het correct verhuizen van een elektronisch medisch dossier bij de huisarts zeker geen vanzelfsprekendheid is. Het is een proces dat nog verder verbeterd moet worden. Eén van de stappen die daarbij genomen moeten worden is het verlaten van de EDIFACT-standaard als basis van het overdrachtsbericht en de omschakeling naar een ander type bericht.

De continue bewaking van het proces door de mensen van ION is conditio sine qua non. De medewerking van de HIS-leveranciers bij het wegwerken van fouten in de overdracht door het aanpassen van de programmatuur is van even groot belang.

W.J. Jongejan

Risicobewustzijn in de zorg t.a.v. ICT is zorgwekkend: lezing op Enigma 2016 conferentie

Het schort nogal aan het risicobewustzijn in de zorg als het om ICT-gebruik gaat. Dat is de belangrijke boodschap van prof. Avi Rubin op de Enigma 2016 conferentie, die van 25 tot en met 27 januari 2016 in San Francisco voor het eerst werd gehouden. Deze conferentie werd door USENIX, the Advanced Computing Systems Association in de Verenigde Staten georganiseerd. Deze organisatie bestaat sinds 1975 en heeft als doel om ingenieurs, systeembeheerders, wetenschappers en technici, die het neusje van de zalm zijn qua computerkennis en –kunde, bij elkaar te brengen. Elk jaar worden meerdere conferenties gehouden. De Enigma-conferentie is opgezet voor werkers uit de industrie en research om de bedreigingen en cyberaanvallen met een frisse blik gezamenlijk onder ogen te zien. Avi Rubin, hoogleraar computerwetenschappen en directeur van het Health and Medical Security Lab van de John Hopkins Universiteit in Baltimore(VS), hield een fraai betoog over hoe het in grote ziekenhuizen in de VS toegaat in de zorg-ICT. De titel was: "Hacking Health: Security in healthcare IT-systems"" Uit dit verhaal zijn ook lessen te trekken voor de Nederlandse situatie.

Zijn verhaal van rond de 20 minuten staat hier op YouTube.

Risicobewustzijn

Rubin vergeleek de situatie qua risicobewustzijn met diverse andere maatschappelijke sectoren, waarin hij risico-evaluaties had gedaan. In de financiële wereld bleek men de zaken aardig op orde te hebben, in de retail-sector(winkels/supermarkten) was het een stuk slechter, maar in de zorg was het 't slechtst ermee gesteld. Aan de hand van een aantal voorbeelden, waarin

hij potentiële gevaren en gevaarlijk gedrag identificeert, schetst hij een duidelijk beeld. Eén van de zaken die hem erg verbaasde was het feit dat in de ziekenhuizen vrijwel alle werkers dezelfde toegangsrechten tot medische dossiers hadden. Er was geen duidelijke gelaagdheid aangebracht wie wat mag zien. Ook werd computerapparatuur gebruikt voor doelen waarvoor die niet was bedoeld of aangeschaft.

Gedrag

Daarbij komen aan de orde:

- Workarounds om beveiligingszaken te omzeilen. Op een radiologieafdeling bleek bijv. een personeelslid voor de daar werkzame specialisten de inlog in de werkstations elke 45 minuten opnieuw te verzorgen. De inlogsessies verlipen elke 50 minuten. Door zo te handelen konden de doktoren doorwerken zonder telkens opnieuw zelf in te loggen. Het is te vergelijken met het plakken van post-it-briefjes op beeldschermen met inlogcode en wachtwoord.
- Specialisten logden vanuit huis in via een VPN(Virtual Private Network)-verbinding via het internet op computers/laptops, waar ook hun kinderen spelletjes op speelden etc.

Onderzoeksapparatuur

Niet altijd realiseert men zich dat er steeds meer onderzoeksapparatuur eigen software bevat, die door buitenstaanders aan te vallen is. Te meer omdat die machines gekoppeld zijn met het netwerk van het ziekenhuis.

- Medicatierobots die in de ziekenhuisapotheken de verdeling van de medicatie regelen
- Röntgenapparatuur zoals scanapparatuur
- Bestralingsapparatuur, waarbij complexe doseringsberekeningen uitgevoerd worden.
- Infuuspompen en andere intensive-care-apparatuur

- Bloedanalyseapparatuur in ziekenhuislaboratoria.

Het is geen luchtfietserij, omdat gebleken is dat hackers gericht dit soort apparatuur aanvallen. Medische informatie wordt ook als het nieuwe goud voor criminelen gezien, zelf tien keer waardevoller dan creditcards. Niet alleen kan gedacht worden een het misbruik maken van data die verkregen is, maar ook zogenaamde “ransomware”(tegen betaling weer werking mogelijk maken) kan een organisatie ernstig ontregelen.

Autorun

Apart staat Rubin stil bij de machines op de róntgenafdelingen, die dvd’s branden om het mogelijk te maken bijv. scanonderzoek elders in te zien. Op de dvd’s worden de afbeeldingen gebrand, maar ook een viewer. Dit programma kan met een autorun-programma elders op een computer afgespeeld kan worden ongeacht welk besturingssysteem daarop staat. Het “targetten” van een machine die deze dvd’s maakt in een ziekenhuis, maakt het een hacker mogelijk om via deze weg zeer vele computers elders te besmetten met malware. Gerichte beveiliging van dit soort machines is van groot belang.

Personeelszaken

Ook de computers van de personeels- en managementafdelingen van ziekenhuizen zijn als risico te identificeren bijv. vanwege de consequenties voor de inzet van personeel bij uitval door een cyberaanval van een hacker.

Aparte wereld

Rubin analyseert ook waarom het vaak zo slecht gesteld is met het risicobewustzijn. Hij schetst de ziekenhuiswereld als een omgeving die bevolkt wordt door werkers die hun focus totaal elders hebben liggen en het denken in termen van risico’s en beveiliging als een last ervaren bij het behandelen van patiënten. Hij ziet de gezondheidszorg als een unieke sector,

waarin veel mensen veel verschillende rollen hebben, met aparte regelgeving. De sector is zeer afhankelijk van software, moet opgeslagen gegevens snel toegankelijk hebben en neigt tot steeds meer gebruik van mobiele apparatuur en gebruik van de cloud. Het bijzondere aan de zorg is echter dat het ons allen aangaat.

10 aanbevelingen

Aan het eind komt hij tot 10 aanbevelingen, die snel zoden aan d dijk zetten, om het risicobewustzijn te verbeteren en tot beter risicogedrag te komen.

- voorkom dat ongeautoriseerde programma's op apparatuur kan draaien(Application whitelisting)
- Zorg voor goede hygiëne ten aanzien van backend-systemen.
- Houdt in de gaten of er geen abnormale zoekopdrachten(queries) gegeven worden
- Zorg voor multi-factor-authenticatie bij toegang van buiten het ziekenhuis.
- Zorg voor toegang via een virtual-machine bij toegang tot klinische data.
- Zorg voor universele versleuteling van data. Bij dataverlies is toegang niet zo maar mogelijk
- Zorg voor goede uniforme afspraken/uniforme juridische regelingen als gebruik wordt gemaakt van opslag in de cloud.
- Beveilig de toegang tot overzichten en tabellen en log de toegang
- Let bijzonder goed op de privacy t.a.v. zelf identificerende uitslagen van onderzoek(DNA, genome-sequencing)
- Authenticatie van personeel via badges met bepaling wie wat mag doen/inzien.

Het leek mij nuttig deze materie ook een keer hier onder de aandacht te brengen, juist omdat menselijk gedrag universeel

is, zeker in de medische wereld.

Wilt u meer zien van Avi Rubin dan is de TEDx-talk van hem uit 2011 ook zeer leerzaam. Die gaat o.a over het hacken van pacemakers, ICD’s en auto’s.

W.J. Jongejan