Uiterst chaotische invoering opt-out bij Australisch elektronisch patiëntendossier

In Australië kent men sinds 2012 een Landelijk Elektronisch PatiëntenDossier(L-EPD) dat de eerste vijf jaren van het bestaan geplaagd werd door technische problemen, enorme kostenoverschrijdingen en beperkte deelname(op basis van opt-in-toestemming). Het heet My Health Record(MHR). Om dat laatste tegen te gaan gooide de regering het roer om en maakte er een opt-out-systeem van. Ieders medisch dossier in het systeem behalve als je het niet wilt. De opt-out-periode startte op 16 juli 2018 en eindigt 15 oktober 2018. Vanaf de eerste dag van dit tijdvak is het zowel logistiek, juridisch en parlementair een grote chaos. Ondanks zeventien jaar voorbereiding en twee miljard Australische dollars(1 A.D.=0,68 Euro) werd de Australian Digital Health Agency de eerste dagen op het logistieke vlak verrast door de grote aantallen mensen die hun opt-out wilden effectueren. Gevolg: de website kwam plat te liggen. Ook de Medicare-website die bij dat proces nodig is kwam plat te liggen. Mede naar aanleiding van een publicatie van de Parliamentary Library, het Australische equivalent van onze Raad van State, ontstond terzelfder tijd een forse discussie over de overdraagbaarheid van medische dossiers aan overheids- en opsporingsinstanties indien die dat nodig zouden achten.

Oud probleem

Het probleem van het door overheids-/opsporingsinstanties mogen inzien van medische dossiers in het My Health Record-systeem culmineerde vlak na de start van de opt-out-periode, maar is reeds in december 2016 gesignaleerd. Toen verscheen een artikel in het Australische Journal of Law and Medicine over dit onderwerp. Ik besteedde daar op 19 december 2016 ook aandacht aan. De crux zit in de My Health Records Act(MHR-A) en wel in de secties 63 t/m 70, betreffende "Collection, use and disclosure other than in accordance with access controls". Deze wet trad in november 2015 in werking. De uitleg die de Parliamentary Library ein juli 2018 er aan gaf is dat zonder wettelijk bevelschrift(warrant) die dat opgevraagd konden worden. De verantwoordelijk minister Greg Hunt stelde dat gebruik van die data alleen met een "warrant" uitgeschreven door een rechtbank kan geschieden maar dat staat nergens in de MHR-A.

Nederland

Australië gaat met haar mogelijkheid om medische data in te laten zien door regerings-/opsporingsinstanties onbegrijpelijk ver. De tegenstand ertegen is ook goed te begrijpen. In Nederland is het onmogelijk dat een rechter met een gerechtelijk bevel het medisch beroepsgeheim kan doorbreken. Het is bijzondere gevallen alleen aan de arts om indien er sprake is van een conflict van plichten bij zwaarwegende omstandigheden . De arts is dan genoodzaakt een keuze te maken tussen het belang van handhaving van het beroepsgeheim en een ander gewichtig belang, dus tussen twee zwaarwegende belangen. Een conflict van plichten kan echter niet te snel worden aangenomen. Vereist is onder meer dat het probleem niet langs andere weg kan worden opgelost dan via doorbreking van het beroepsgeheim.

Ander probleem

Een ander punt van zorg is sectie 98 van de MHR-A waarin het de Australina Digital Health Agency toegestaan is om één of

meer van haar functies over te dragen aan bureaucraten. Dat zou inhouden dat ook de mogelijkheid om zorginformatie zonder toestemming van de betrokkenen te delen met instanties uit handen wordt gegeven.

Vernietigen

Een ander punt dat veel reacties opriep was het beleid als een burger uit het MHR-systeem wil. Zijn/haar data worden dan pas echt dertig jaar na het overlijden of honderddertig jaar na de geboortedatum vernietigd. Het betekent dat het begrip "verwijdering van data" non-existent is.

Bakzijl

Geschrokken door alle reacties en ook de grote aantallen mensen die hun opt-out willen uitoefenen heeft minister Hunt bakzeil gehaald. Hij gaat nu de My Health Record Act aanpassen. Daarmee wil hij ook in de wet vastleggen dat overdracht van medische data aan regerings-/opsporingsinstanties uitsluitend met een gerechtelijk bevel, uitgeschreven door een rechtbank kan geschieden. Ook heeft hij toegezegd het vernietigen van reeds vastgelegde gegevens te doen plaatsvinden op het moment dat de burger dat wenst en niet dertig jaar na diens dood. Vermoedelijk zal de Australische overheid ook de opt-out-periode moeten verlengen vanwege het platliggen van de website voor het uitoefenen van de opt-out. Het trouwens vermakelijk om te lezen dat de minister zich ook voorgenomen heeft om een publiciteitscampagne op te zetten om samen met bestuurders uit de medische sector het publiek de voordelen van het My Health Record-systeem duidelijk te maken. Niet je af vragen of je wel op de goede weg bent, maar door pushen.

Daarmee lijkt het dan weer precies op de situatie rond het gebruik van het Landelijk SchakelPunt in Nederland.

W.J. Jongejan, 8 augustus 2018

Hackers bieden Australische Medicare-card-data te koop aan. Les voor Nederland

Op 4 juli 2017 werd duidelijk dat op het zogenaamde Dark Web, een alleen met een speciale browser toegankelijk deel van het internet, gegevens te koop waren van Australische Medicare-ID-kaarten. Dat zijn kaarten met een magneetstrip, die de bezitter toegang geeft tot behandeling in de eerstelijnszorg en zorg in publieke ziekenhuizen. De melding kwam van een journalist van The Guardian, die op het Dark Web voor 22 US dollar, of 0,0089 bitcoin, de data van zijn eigen medicare-card kocht. Degene die de data verkocht had sinds oktober 2016 data van tenminste 75 Medicare-kaarten verkocht. De kaarten worden uitgegeven door het Australische Department of Human Services. De details van de kaarten, zoals nummer, tenaamstelling en expiratiedatum zijn niet publiek toegankelijk en zijn alleen de eigenaar van de kaart bekend. Door criminelen wordt de informatie als waardevol beschouwd. omdat ze het mogelijk maken om nep-Medicare-kaarten te maken

met bestaande gegevens. Die kunnen dan gebruikt worden voor identiteitsfraude.

Waardevol

Al enige tijd is het duidelijk dat diefstal van medische gegevens veel lucratiever is dan het bemachtigen van creditcardnummers. Cybersecurity-adviseurs denken dat medische gegevens, inclusief de polis- en persoonsnummers(social-security-numbers of BSN) tot tien keer meer waard zijn dan creditcarddata. De gegevens op de kaarten kunnen gebruikt worden door criminelen voor de aanschaf van goederen, bijv. auto's. Ook kunnen uitbetalingen van Medicare aan de burger doorgesluisd worden naar frauduleuze bankrekeningen. Al in 2015 had een politie-eenheid een criminele groep opgespoord die Medcare-card data gebruikte om zich frauduleus terugbetalingen toe te eigenen. Een probleem in Australië is tevens dat de Medicare-card ook als identificatiemiddel(Digital Verification Service) buiten de zorg wordt gebruikt. Dat bleek toen de Australische belastingdienst, de Australian Tax Office met onmiddellijke ingang aangaf dat de Medicare-card niet meer gebruikt mocht worden als identiteitsverificatie bij belastingzaken. Het vreemde was dat nog geen 24 uur later dezelfde dienst aangaf dat de kaart weer als identificatiemiddel mocht worden gebruikt.

Overheid

Zoals te verwachten probeerde de overheid bij monde van de minister van het Department of Health Services direct het belang te downplayen onder andere dat het ging om kleine aantallen. De stelling van minister Tudge is dat het hier niet om een hack ging maar om een "traditional criminal activity" gaat en niet om een groot datalek. De minister bleek tot aan 5 juli 2017 niets van de diefstal van card-data te weten ook al waren de data al vanaf oktober 2016 te koop op het Dark Web. De berichtgeving via de pers schudde het ministerie wakker.

Medische data

Naar verluidt zijn bij de diefstal van de kaartdata niet rechtstreeks medische data in handen van criminelen gekomen. Wel zijn bij de diefstal de koppeling van naam en Medicare-nummer van de betrokkenen buitgemaakt. Om bij de medische data te komen zijn elektronische NASH en/of PKI-certificaten nodig. Die worden echter door de overheid naar duizenden zorgverleners verstuurd en naar verluidt zijn daarvan meerdere "zoekgeraakt". Misbruik is dus niet uit te sluiten.

Medicare

Het gecentraliseerde Medicare-ysteem stond en staat bloot aan veel kritiek en is toch doorgeduwd. Medische data worden in een centrale database opgeslagen. In noodgevallen mogen artsen de medische gegevens van burgers in "My Health Record" zonder toestemming van de patiënt inzien. De overheid mag de medische data zonder toestemming inzien als fraude vermoed wordt of bij rechtszaken. Medicare gaat ook onzorgvuldig om met data. Recent werden deels versleutelde databestanden openbaar beschikbaar gesteld die door enkele academici binnen korte tijd vergaand te ontcijferen waren. De vreemde reactie van de overheid was toen om het ontcijferen strafbaar te stellen in plaats van het te accepteren als een waarschuwing!!!

Nederland

Wat leert deze materie ons Nederlanders? Wij hebben ook een gecentraliseerd systeem met het Landelijk SchakelPunt(LSP). De data zijn niet centraal opgeslagen, maar zijn bij de bron raadpleegbaar via het LSP. De toegang is geregeld met UZI-passen en kaartlezers. Diefstal van UZI-pas en pincode van de gebruiker maakt het in principe mogelijk dat door die dief vanaf een werkstation plus kaartlezer met malafide intenties ingelogd kan worden en data opgevraagd worden. Uiteraard vindt logging plaats van het gebeurde en is de toegangsweg te identificeren, maar het kwaad is dan al geschiedt zonder dat

men weet wie de dader is. Men weet alleen wiens pas gebruikt is en mogelijk welke werkplek. Bovendien zal het de gedupeerde burger niet altijd duidelijk zijn dat zijn of haar data ingezien zijn als deze geen abonnement heeft op meldingen van inzage in de medische gegevens via het LSP.

Kortom: het kan ook hier gebeuren, het is alleen de vraag wanneer en hoe uitgebreid.

W.J. Jongejan