A-EPD My Health Record slaagt niet in adequaat managen cybersecurity-risico's

In The Guardian van maandag 25 november 2019 stond een interessant artikel over problemen bij het Australische Elektronische PatiëntenDossier(A-EPD), My Health Record. De verantwoordelijke instantie, de Australian Digital Health Agency(ADHA), blijkt fors te kort te schieten op het gebied van cybersecurity en interne controles. Het Australian National Audit Office(ANAO) stelt dat ADHA cybersecurity en privacy-risico's niet adequaat managede. De auditorganisatie schreef dat ADHA voor het centrale A-EPD systeem op zich passende maatregelen nam om de cyberveiligheid te garanderen. Maar men stelde tegelijk vast dat men naliet voor afdoende bescherming te zorgen tegen cyberaanvallen via sites/apps van derden en via zorgaanbieders-organisaties. Het betekent dat als je de voordeur beveiligt, maar de achterdeur open laat staan er grote cybersecurity-risico's bestaan voor in het systeem opgeslagen zorgdata. Het A-EPD is al jaren een bron van zorg en discussie in Australië. Ik schreef er al drie keer over. (In 2016, in 2017 , in 2018).

My Health Record

Het A-EPD startte al 2012. Het bestaat uit een centraal computersysteem waarnaar toe zorgdata van patiënten door zorgaanbieders opgestuurd worden. Het is dus totaal anders van opzet dan het Nederlandse Landelijke SchakelPunt(LSP). Daar blijven de data bij de bron. Men maakt die opvraagbaar door aan de patiënt een opt-in-toestemming er voor te vragen. Het Australische systeem kende aanvankelijk een opt-in-systeem. Dat veranderde men in een opt-out-systeem in 2018.

Aanvankelijk zou de overgangsperiode van 16 juli tot 15 oktober 2018 duren. Door chaotische toestanden vanwege het grote aantal mensen dat niet in het systeem wilde, moest men de periode verlengen tot 31 januari 2019. In die periode kozen 2,5 miljoen Australiërs ervoor om niet in het systeem opgenomen te worden. Dat is ongeveer 10 procent van de bevolking.

Onvoldoendes

Naast de inadequate bescherming tegen cyberaanvallen via software van derden en via systemen van zorgaanbieders deelde de Australian National Audit Office ook een onvoldoende uit voor het niet uitvoeren van een end-to-end privacy-impact-assessment(PIA) van het systeem onder het opt-out model. De laatste PIA dateerde van 2017, onder het opt-in-model. Daarnaast bleken vier privacy-reviews die tussen oktober 2017 en juni 2019 gedaan waren nooit voltooid te zijn en dus geen rapportage te kennen.

Onvoldoende controle spoedinzage

Het Australische systeem kent een zogenaamde noodtoegang tot de medische data, waardoor inzage mogelijk is verder dan waarvoor de burger toestemming gaf. Dat mag alleen als de omstandigheden een serieuze bedreiging vormen voor het leven van de betrokkene, diens gezondheid of veiligheid. Maar ook als er een serieuze bedreiging is voor de volksgezondheid of publieke veiligheid. Met die laatste twee condities doelt men o.a. op inzage door politie en/of veiligheidsdiensten bij zaken als als een terrorisme-dreiging. Het staat allemaal in de My Health Records Act. Deze trad in november 2015 in werking. Ik schreef er ook over in 2016. De Australian National Audit Office constateerde dat maar 8,2 procent van de inzageverzoeken volgens de regels verliepen. Het aantal keren per maand dat men deze mogelijkheid gebruikte steeg van 80 in juli 2015 tot 2015 in maart 2019.

Geen controles

De toezichthouder zag wel dat de ADHA de spoedaanvragen monitorde, maar geen procedures had voor wat er daarna dient te gebeuren. Dat zijn extra controles op de rechtmatigheid van de aanvraag en op het ontbreken van een respons van de kant van de opvragende partij. Daarnaast had de ADHA in geen enkel geval van een spoedinzage gemeld aan de nationale Information Commissioner. Hetgeen men wel had moeten doen.

Daarnaast maakte de Audit Office belend dat niet alle Australische zorgverleners voldeden aan het minimaal nodig geachte niveau van cyber-beveiliging. Met daarbij de opmerking dat in de zorgsector de meest opvallende datalekken voorkwamen van alle industrie- en dienstensectoren.

Conclusie, ook voor hier

Uit het rapport van de Australian National Audit Office valt te concluderen dat er het nodige rammelt aan het Australische systeem dat zorgdossiers centraal opslaat om van daar uit inzage mogelijk te maken. Het Nederlandse systeem is anders van opzet maar daar weten we niets over het al dan niet adequaat zijn van het beveiligingsniveau van de op het LSP aangesloten systemen. Zorgaanbieders moeten bij aansluiting zelf verklaren te voldoen aan de eisen van een Goed Beheerd Zorgsysteem. De Vereniging van Zorgaanbieders Voor Zorgcommunicatie, verantwoordelijk voor het LSP, zegt steekproefsgewijs controles te doen bij zorgaanbieders. Hoe vaak men dat doet en hoe veel keren er gebreken zijn gevonden maakt men niet bekend. Het is daarbij de slager die zijn eigen vlees keurt. Er is hier geen onafhankelijke toezichthouder die daar op toeziet, zoals in Australië.

W.J. Jongejan, 28 november 2019

Afbeelding van cocoparisienne via Pixabay