Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid
Afdeling "Gezondheid"

SCSZG/15/010

AANBEVELING NR. 15/01 VAN 20 JANUARI 2015 BETREFFENDE EEN ONTWERP VAN OMZENDBRIEF VAN DE FOD VOLKSGEZONDHEID INZAKE HET GEBRUIK VAN CLOUD DIENSTEN IN ZIEKENHUIZEN

De afdeling gezondheid van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid (hierna "het Sectoraal Comité" genoemd),

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens;*

Gelet op de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform*;

Gelet op de adviesvraag van de Commissie voor de bescherming van de persoonlijke levenssfeer ontvangen op 1 december 2014;

Gelet op het auditoraatsrapport van het eHealth-platform van 9 januari 2015;

Gelet op het verslag van de heer Yves Roger,

Beveelt op 20 januari 2015, na beraadslaging, het volgende aan:

I. ONDERWERP VAN DE AANVRAAG

1. De Commissie voor de bescherming van de persoonlijke levenssfeer mocht op 18 september 2014 van de toenmalige minister van Sociale Zaken en Volksgezondheid een verzoek tot advies ontvangen betreffende een ontwerp van omzendbrief inzake het gebruik van cloud diensten opgesteld door de FOD Volksgezondheid.

2. De wijziging van artikel 20, §1, van de coördineerde wet van 10 juli 2008 op de ziekenhuizen en andere zorginstellingen maakt het thans immers wettelijk mogelijk voor ziekenhuizen om beroep te doen op cloud diensten. De ziekenhuissector is echter vragende partij voor een minimaal referentiekader dat de ziekenhuizen toelaat om het gebruik van cloud diensten zo rationeel mogelijk te evalueren met respect voor het hoogst mogelijke technische en juridische veiligheidsniveau en de bescherming van de persoonlijke levenssfeer van de patiënten.

3. Teneinde tegemoet te komen aan deze vraag, heeft de FOD Volksgezondheid een ontwerp van omzendbrief inzake het gebruik van cloud diensten in ziekenhuizen opgesteld.

4. Gelet op de specifieke bevoegdheid en competentie op het vlak van de bescherming van gezondheidsgegevens, o.a. in de ziekenhuissector, heeft de Commissie voor de bescherming van de persoonlijke levenssfeer het ontwerp van omzendbrief voor advies overgemaakt aan de afdeling gezondheid van het Sectoraal comité van de sociale zekerheid en van de gezondheid.

II. BEHANDELING VAN DE AANVRAAG

5. Het ontwerp van omzendbrief geeft een zeer omslachtige beschrijving van de context van cloud diensten, van de mogelijke risico's en van een aantal aandachtspunten. Het Sectoraal comité stelt echter vast dat de omzendbrief de ziekenhuizen onvoldoende begeleidt in concrete situaties.

6. Het gebruik van cloud diensten houdt een aantal inherente risico's in. De verwerking van gegevens in de cloud kan ertoe leiden dat de gegevens zich op verschillende servers en gegevenscentra bevinden. Daardoor kan de verantwoordelijke voor de verwerking potentieel de controle over zijn gegevens verliezen en zou de bescherming in gevaar kunnen komen (onvoldoende bescherming, verlies, misbruik, raadpleging door derden of buitenlandse overheden, …). Bovendien bestaat de mogelijkheid dat buitenlandse overheden die gegevens kunnen raadplegen en opvragen naargelang hun eigen wetgeving.

7. Actoren in de gezondheidszorg die overwegen om cloud computing in te voeren moeten aan de hand van een risicoanalyse nagaan welke de weerslag zal zijn op de beveiliging en de vertrouwelijkheid als er persoonsgegevens van de betrokken

personen in de cloud worden gezet. Deze analyse moet betrekking hebben op de hiernavolgende punten:

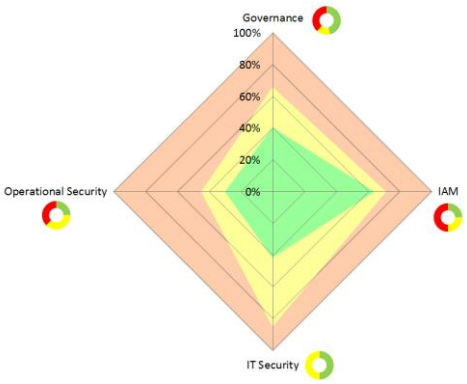
- nauwgezette evaluatie van de persoonsgegevens die al dan niet worden opgeslagen in de cloud, dit geldt in het bijzonder voor de zogenaamde "gevoelige gegevens" als bedoeld in de privacywet, waaronder persoonsgegevens die de gezondheid betreffen;
- analyse van de contractuele voorwaarden;
- evaluatie van de overeenstemming van de door de cloud provider voorgestelde beveiligingsvoorwaarden, waarbij de referentiemaatregelen opgesteld door de Privacycommissie als minimum standaard moeten gelden;
- garantie van de cloud provider op bepaalde rechten, vanaf de uitvoering tot beëindiging van het contract zodat hij zich kan richten naar zijn eigen verplichtingen inzake persoonsgegevensbescherming: clausule over de continuïteit en de kwaliteit van de dienstverlening, bepalingen inzake interoperabiliteit, omkeerbaarheid en overdraagbaarheid van de gegevens, …;
- het in aanmerking nemen van de consequenties van een mogelijke toegang tot de gegevens door personen buiten de zorginstelling, inzonderheid voor o.a. doeleinden van wetshandhaving;
- de mogelijkheid om tegemoet te komen aan de rechten van de betrokken patiënten, zoals het recht op inzage.

8. Teneinde de ziekenhuizen toe te laten om een dergelijke risico-analyse te kunnen uitvoeren, acht het Sectoraal comité het aangewezen dat een praktische methode om de beveiliging van cloud diensten te evalueren, aan de ziekenhuizen en andere actoren in de gezondheidssector ter beschikking zou worden gesteld.

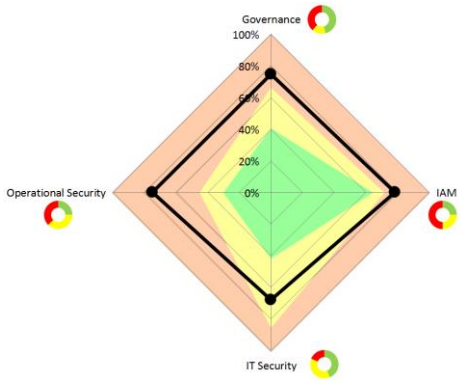
9. Hierna wordt een tweevoudig model beschreven dat toelaat om aan de hand van een eenvoudig, evolutief rooster enerzijds het maturiteitsniveau in verband met de beveiliging van een specifieke cloud dienst te evalueren en anderzijds het gebruik van een specifieke cloud dienst te evalueren naargelang het soort gegevens die men ernaar wil overbrengen.

10. In concreto bestaat de voorgestelde methode uit twee luiken:

- een luik A bestaat uit de vragenlijst "Security-assessment-cloud-service.xlsm" waarmee het maturiteitsniveau in verband met de beveiliging van een specifieke cloud dienst geëvalueerd kan worden. Deze evaluatie moet enkel steunen op de publieke gegevens die de evaluator op voorhand heeft kunnen verzamelen (bv. op de officiële website van de cloud dienst). De figuur hieronder is een voorbeeld van een analyseresultaat voor een cloud dienst zodra de vragenlijst van luik A ingevuld is. Het resultaat wordt weergegeven in de vorm van een radar.



- een luik B bestaat uit de vragenlijst "Client-guide-cloud-assessment.xlsm" waarmee men de mogelijkheid kan evalueren om een specifieke clouddienst te gebruiken naargelang het soort gegevens die men ernaar wil overbrengen. De figuur hieronder is een voorbeeld van het resultaat van een vergelijking. De figuur herneemt de radar verkregen na de toepassing van luik A op een clouddienst. De zwarte lijn komt overeen met de behoeften en eisen van de gebruiker die de vragenlijst van luik B heeft ingevuld. Het eindresultaat van luik B baseert zich dus op een radar die resulteert uit luik A, aangevuld door de evaluatie van de gebruiker.



11. De belangrijkste beveiligingsaspecten die geëvalueerd worden door het model worden gegroepeerd in 4 hoofdcriteria: governance, identiteitsbeheer en toegangscontrole, IT-beveiliging en tot slot operationele beveiliging. In de context van sociale zekerheid en gezondheidszorg evalueert het model ook de conformiteit van de cloud dienst met de 'Veiligheidspolicy met betrekking tot Cloud Computing Services', gepubliceerd door de Kruispuntbank van de Sociale Zekerheid[1]. Deze conformiteit wordt in de luiken A en B weergegeven door de donuts (een donut per hoofdcriterium).

12. De kleurcodes zijn hetzelfde voor donuts of radars. De groene zone, genaamd "confidence zone", vertegenwoordigt het percentage dat een cloud dienst met zekerheid aan een hoofdcriterium voldoet. De gele zone, genaamd "doubt zone", vertegenwoordigt het percentage dat een cloud dienst mogelijk aan een

[1] https://www.ksz-bcss.fgov.be/binaries/documentation/nl/securite/policies/isms_050_cloud_computing_policy_nl.pdf.

hoofdcriterium voldoet. We spreken van “mogelijk voldoet” om de geëvalueerde cloud dienst niet te bestraffen: de “doubt zone” geeft dus de vragen van de vragenlijst “Security-assessment-cloud-service.xlsm” weer waar we onmogelijk met zekerheid op kunnen antwoorden. De rode zone, genaamd “death zone“, vertegenwoordigt het percentage dat een cloud dienst niet aan een hoofdcriterium voldoet.

13. De figuren hieronder tonen een vergelijking tussen 5 verschillende cloud diensten en de behoeften/eisen van een klant die de vragenlijst van luik B ingevuld heeft. Het model vergelijkt zo de cloud dienst per criterium om de analyse te vergemakkelijken.

14. Beide vragenlijsten van luik A en luik B worden aan deze aanbeveling als bijlage toegevoegd en zullen, samen met de aanbeveling, worden gepubliceerd op de hiertoe bestemde webpagina[2].

15. Het gebruik van dit model een ziekenhuis of eender welke actor in de gezondheidszorg toelaten om zelf te evalueren in welke mate het veiligheidsniveau van een bepaalde cloud dienst voldoet aan de specifieke behoeften. Zodoende kan de betrokken actor in de gezondheidszorg op gefundeerde wijze de diverse risico’s inschatten alvorens op eigen verantwoordelijkheid gebruik te maken van een bepaalde cloud dienst.

[2] https://www.ehealth.fgov.be/nl/over-het-ehealth-platform/organisatie/sectoraal-comite/presentatie

Om deze redenen, beveelt

de afdeling gezondheid van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid

aan de actoren in de gezondheidszorg het gebruik van de in het voorliggend document beschreven methode aan om – op eigen verantwoordelijkheid – de beveiliging van cloud diensten te evalueren.

Yves ROGER
Voorzitter