Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2407

Vragen van het lid **Joba van den Berg** (CDA) aan de Minister van Volksgezondheid, Welzijn en Sport over *het wissen van patiënteninformatie door het Albert Schweitzer ziekenhuis* (ingezonden 25 maart 2022).

Antwoord van Minister **Kuipers** (Volksgezondheid, Welzijn en Sport) (ontvangen 13 april 2022).

Vraag 1
Kent u het bericht dat het Albert Schweitzer ziekenhuis duizenden oude patiëntdocumenten heeft gewist?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u aangeven welke procedures bij een dergelijke transitie normaliter gevolgd dienen te worden, zoals een logboek bijhouden, vier ogen principe hanteren en batch-gewijs iets uitproberen? Kunt u aangeven in hoeverre deze procedures in dit specifieke geval wel of niet zijn gevolgd?

Antwoord 2
Als met een dergelijke transitie de invoering van het EPD wordt bedoeld, dan heeft het ziekenhuis mij laten weten dat passende procedures zijn gevolgd bij het inrichten van de software en het digitaliseren van het bestaande archief. Voor de inrichting van de software betekende dit een samenwerking tussen de consultants van ziekenhuissoftware leverancier Chipsoft en eigen personeel van het ziekenhuis. Voor wat betreft de digitalisering van het bestaande archief is gebruikgemaakt van een gefaseerde aanpak, met een bijbehorende eindcontrole op het correct opslaan en de raadpleegmogelijkheid van de gedigitaliseerde gegevens.

[1] NU.nl, 21 maart, 2022, «Albert Schweitzer ziekenhuis wist per ongeluk 513.000 oude patiëntdocumenten» (Albert Schweitzer ziekenhuis wist per ongeluk 513.000 oude patiëntdocumenten | NU – Het laatste nieuws het eerst op NU.nl)

ah-tk-20212022-2407
ISSN 0921 - 7398
's-Gravenhage 2022

Vraag 3
Kunt u aangegeven wat u vindt van de veiligheid van een systeem zoals deze van Chipsoft, waarbij het blijkbaar mogelijk is om volgnummers twee keer te gebruiken?

Antwoord 3
Ik vind het van groot belang dat zorgaanbieders en softwarebedrijven zoals Chipsoft hun informatie en systemen ten alle tijden goed beveiligd en beschermd moeten hebben en houden. Het Albert Schweitzer ziekenhuis heeft mij laten weten dat generieke veiligheid van het elektronisch patiëntendossier (ChipSoft HiX) voldoende is, hoewel het (onbedoeld) overschrijven van data in een dergelijke applicatie te allen tijde technisch voorkomen had moeten worden. Inmiddels heeft, zoals aangegeven door het ziekenhuis, Chipsoft een technische aanpassing doorgevoerd door aan alle HiX-gebruikende ziekenhuizen een software-update aan te bieden.
Dat er gegevens overschreven zijn is een unieke combinatie van drie factoren: een verkeerd gekozen nummerreeks, het niet beveiligd zijn van data tegen overschrijven én de gekozen manier van back-up van de gegevens, waarbij elke nieuwe full back-up in de plaats komt van de vorige full back-up. Hierdoor kwamen de niet opgemerkte fouten gaandeweg ook in de back-ups terecht). Ook dit is inmiddels verholpen doordat Chipsoft een nieuw manier van back-up heeft geïmplementeerd.

Vraag 4
Wat vindt u ervan dat pas een jaar na dato is opgemerkt dat er wat is misgegaan? Hoe kan dit voorkomen worden? Welke controles zijn er niet gedaan? Welke veiligheidskleppen of signalen hadden dat kunnen voorkomen?

Antwoord 4
Uit het feitenrelaas van het ziekenhuis[2] en daarna intensief contact, blijkt dat er geen mogelijkheden tot controle zijn geweest om deze fout eerder en/of tijdig te kunnen signaleren. Dat het opmerken van het incident lang heeft geduurd ligt in het feit dat er, vanaf het moment van optreden van de gevolgen van de fout in 2020, weinig tot geen gebruik meer werd gemaakt van de betreffende archiefdata van voor 2017 bij lopende behandeltrajecten van patiënten. De constatering dat een bestand was overschreven, die leidde tot de ontdekking van het incident in volle omvang, had eerder maar ook later kunnen plaatsvinden. Wat vast staat is dat er in de tussenliggende circa elf maanden door individuele behandelaren intern geen melding is gemaakt van onregelmatigheden. Een eerdere melding had de omvang van de gevolgen van dit incident kunnen reduceren, maar er zijn naar de mening van het ziekenhuis geen controles *niet* uitgevoerd waardoor de fout eerder te constateren zou zijn geweest.
De gevolgen van het incident hadden voorkomen kunnen worden wanneer:
1. In de Chipsoft-software het (onbedoeld) overschrijven van gegevens onmogelijk zou zijn geweest, ofwel met een waarschuwing was beveiligd. Dit is inmiddels aangepast door Chipsof door de software aan te passen waardoor de gebruiker tijdig wordt waarschuwt.
2. Het kiezen voor een back-upmethode waarbij kan worden teruggegrepen naar een restore van de gegevens vanuit een willekeurig punt in het verleden. Omdat het om statische data ging, is voor dit specifieke archiefontwerp een afwijkend regime gekozen waarbij elke geslaagde periodieke back-up de vorige overschreef. Hierdoor kon de fout in elke back-up ongemerkt iets verder doorwerken. Deze methode is inmiddels gewijzigd. Een herhaling van dit specifieke incident is daarmee uitgesloten.

Vraag 5
Is het zo dat in een jaar tijd geen enkele arts historische gegevens nodig heeft gehad, aangezien men de fout pas na een jaar heeft ontdekt? Vindt u dat op zich al niet vreemd?

---

[2] https://www.asz.nl/nieuws/nieuwsberichten/2022/3/30416/,

Antwoord 5
Het Albert Schweitzer ziekenhuis heeft mij laten weten dat de overschreven informatie voornamelijk uit historische gegevens bestaat waarvan in 2017 al de inschatting is gemaakt dat ze niet meer nodig waren voor lopende behandelingen. De bestanden bevonden zich niet in het actieve elektronische patiëntendossier, maar in een digitale archiefomgeving.
Deze data vielen nog wel onder de bewaarplicht maar werden zo goed als niet meer geraadpleegd bij het verstrijken van de tijd. Dat is niet vreemd, noch uitzonderlijk.

Vraag 6
Wat vindt u van de communicatie naar patiënten (brief bijgevoegd) met de zinsnede: het gaat om informatie die in 2017 al niet meer van belang werd geacht voor uw behandeling. De kans dat er nu nog gevolgen zijn voor uw behandeling, is verwaarloosbaar klein. Alleen in bijzondere situaties waarin u in de toekomst uw volledige dossier zou willen opvragen, kunnen wij daaraan helaas niet 100 procent tegemoetkomen? Wat gaat het ziekenhuis doen als deze mensen per ongeluk toch verkeerd behandeld zouden worden, dan wel bijvoorbeeld hun UWV-uitkering niet meer kunnen krijgen?

Antwoord 6
Het Albert Schweitzer ziekenhuis heeft me laten weten dat de communicatie naar patiënten zorgvuldig en naar waarheid is opgesteld, gebaseerd op het soort informatie in de verdwenen bestanden. Het ziekenhuis geeft daarnaast aan dat het uitvoerig intern onderzoek heeft gepleegd bij alle betrokken medische vakgroepen, naar de vraag of sprake kan zijn geweest van verkeerd medisch handelen als gevolg van het ontbreken van data. Deze uitvraag heeft geen reden tot verder onderzoek opgeleverd. Ook verwacht het ziekenhuis dat informatie van het type dat verwijderd is, niet nodig zal zijn bij aanvragen of procedures. Juist het type informatie dat daarbij doorgaans wel nodig is, heeft een actuele en actieve status en bevindt zich veilig in het reguliere elektronische dossier van patiënten. Mocht toch ooit een niet meer beschikbaar document vereist zijn, dan helpt het ziekenhuis de eventuele gedupeerden aan een alternatief voor de bewijsstukken. Ook hierover is informatie voor patiënten te vinden op de in het antwoord bij vraag 4 vermelde webpagina. Tevens heeft het ziekenhuis een e-mailadres ingesteld voor patiënten die denken of verwachten dat ze op enigerlei manier nadeel ondervinden van het verlies van historische gegevens.

Vraag 7
Is dit ziekenhuis aangesloten bij Z-Cert? Welke ondersteuning levert Z-Cert bij dit soort transities?

Antwoord 7
De ziekenhuizen die onderdeel zijn van de brancheverenigingNederlandse Vereniging van Ziekenhuizen (NVZ) zijn collectief aangesloten bij Z-CERT. Hier valt het Albert Schweitzer ziekenhuis ook onder. Ondersteuning bij dergelijke transities is geen onderdeel van Z-CERT haar producten en diensten. Z-CERT richt zich primair op ondersteuning bij cyberincidenten, het vroegtijdig waarschuwen omtrent cyberkwetsbaarheden en dreigingen, en in het algemeen het verhogen van de digitale weerbaarheid van zorginstellingen.