Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

Aanhangsel van de Handelingen

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

1895

Vragen van het lid **Leijten** (SP) aan de Ministers van Volksgezondheid, Welzijn en Sport en van Veiligheid en Justitie over *het bericht van de FBI «Health care systems and medical devices at risk for increased cyber intrusions for financial gain»* (ingezonden 2 februari 2016).

Antwoord van Minister **Schippers** (Volksgezondheid, Welzijn en Sport) (ontvangen 16 maart 2016). Zie ook Aanhangsel Handelingen, vergaderjaar 2015–2016, nr. 1557.

Vraag 1 en 2
Wat is uw reactie op het bericht «Health care systems and medical devices at risk for increased cyber intrusions for financial gain»?[1] Kende u dit bericht? Onderschrijft u de waarschuwing van de FBI dat medische dossiers waarde hebben voor het criminele circuit? Zo ja, wat gaat u doen om dit risico zo klein mogelijk te maken?

Antwoord 1 en 2
Net als de FBI stelt, kan ik mij voorstellen dat de inhoud van digitale medische dossiers waarde kan hebben voor commerciële doeleinden. Zeker ook in het licht van de steeds verder toenemende mogelijkheden om databestanden met verschillende data slim te combineren tot interessante big data. Dat is ook de reden dat de standaarden van de beveiliging van deze data, op een hoog niveau van beveiliging moeten liggen.
De informatiebeveiliging van patiëntgegevens moet voldoen aan Europese en nationale wettelijke voorschriften. De regels voor bijvoorbeeld de omgang met, de opslag en de beveiliging van persoonsgegevens zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp). Voor bijzondere persoonsgegevens (zoals gegevens betreffende iemands gezondheid) stelt de Wbp extra eisen. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving en kan dit zo nodig met (bestuursrechtelijke) sancties afdwingen. Op 15 februari heeft de AP in een open brief aan de Raden van Bestuur van zorginstellingen in Nederland nogmaals aandacht gevraagd voor de bescherming van patiëntgegevens.
Ter invulling van de eisen beschrijft de veldnorm NEN 7510 over informatiebeveiliging in de zorg maatregelen die zorginstellingen moeten treffen om via

[1] Health care systems and medical devices at risk for increased cyber intrusions for financial gain: http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf

ah-tk-20152016-1895
ISSN 0921 - 7398
's-Gravenhage 2016

een gecontroleerd proces op adequate wijze met (medische) gegevens om te gaan. De norm is van toepassing op alle organisaties in de gezondheidszorg, ongeacht de aard en de omvang van het bedrijfsproces. Via de AMvB die behoort bij de Wet voor het gebruik van het BSN in de zorg heeft de NEN 7510 een verplichtend karakter gekregen. De AP ziet toe op de naleving van de norm. De Inspectie voor de Gezondheidszorg (IGZ) ziet alleen toe op de naleving van de norm voor zover deze direct verbonden is met de kwaliteit en veiligheid van zorg. De AP en de IGZ hebben een samenwerkingsprotocol waarin zij wederzijdse afspraken hebben gemaakt over de wijze van samenwerking voor het uitoefenen van toezicht op de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer binnen de gezondheidszorg.

Vraag 3
Heeft u de waarschuwing van de FBI gedeeld met verantwoordelijken voor medische gegevens? Zo nee, gaat u dit alsnog doen? Zo ja, wanneer is dit gebeurd?

Antwoord 3
Zorginstellingen zijn wettelijk verplicht om veilig om te gaan met medische persoonsgegevens. Veilige omgang en informatiebeveiliging van medische persoonsgegevens is daarom ook één van de terugkerende thema's van het Informatieberaad. Het realiseren van structurele aandacht voor dit onderwerp is voor mij belangrijker dan attendering van zorgpartijen op elke publicatie over dit thema. Dit neemt niet weg dat de AP in een open brief aan de Raden van Bestuur van zorginstellingen nogmaals aandacht heeft gevraagd voor de bescherming van patiëntgegevens. Ook zal de IGZ de Nederlandse Federatie van Universitair Medische Centra en de Nederlandse Vereniging van Ziekenhuizen een brief sturen om ziekenhuizen op hun verantwoordelijkheid te wijzen rond de beveiliging van patiëntgegevens.
In het kader van verbetering van de informatiebeveiliging wordt door leden van het Informatieberaad gewerkt aan de ontwikkeling van een ZORG-Cert, een Computer Emergency Response Team, dat zich richt op het voorkomen en genezen van netwerk gerelateerde veiligheidsincidenten. Dit is één van de uitkomsten van de bespreking in het Informatieberaad om het risico dat gegevens in verkeerde handen komen te beperken.

Vraag 4
Is de beveiliging van de computersystemen en elektronische apparaten die gebruikt worden in Nederlandse zorgorganisaties en ziekenhuizen voldoende om de veiligheid van medische gegevens te garanderen? Worden medische en persoonsgegevens van Nederlandse patiënten en cliënten voldoende beveiligd?

Antwoord 4
De informatiebeveiliging van patiëntgegevens moet voldoen aan Europese en nationale wettelijke voorschriften. Ziekenhuizen en zorgverleners zijn hier zelf verantwoordelijk voor en moeten voldoende maatregelen treffen om de veiligheid van medische gegevens te kunnen borgen. De AP ziet toe op de naleving. Zowel de AP als de IGZ zien toe op de veldnorm, de NEN 7510, over informatiebeveiliging in de zorg wanneer de kwaliteit van zorg in het geding is als gevolg van het onveilig omgaan met medische persoonsgegevens. Zie ook mijn antwoord op vraag 2.

Vraag 5
Kunt u een overzicht geven van het aantal zorgorganisaties en ziekenhuizen dat in de afgelopen vijf jaar te maken heeft gekregen met problemen in de beveiliging van hun elektronische datasystemen en apparaten, waardoor de privacy en/of de (persoonlijke) gegevens van cliënten en patiënten in gevaar zijn geweest? Zijn er in die gevallen persoonlijke gegevens in handen van criminelen terecht gekomen? Zo ja, hoe vaak, en is hierop gehandhaafd? Is bekend wat criminelen met deze informatie hebben gedaan? Is hierin een toename te zien over de afgelopen jaren? Zo ja, hoe verklaart u deze toename?

Antwoord 5
Ik heb geen inzicht in het aantal zorgorganisaties en ziekenhuizen dat de afgelopen vijf jaar te maken heeft gekregen met problemen in de beveiliging van hun elektronische datasystemen en apparaten, waardoor de privacy en/of de (persoonlijke) gegevens van cliënten en patiënten in gevaar zijn geweest. Ook navraag bij het Openbaar Ministerie leert dat geen gegevens bekend zijn over persoonlijke medische gegevens die in handen van criminelen terecht gekomen zijn.
In 2013 heeft de AP onderzoek gepubliceerd naar de wijze waarop zorginstellingen aan medewerkers toegang verlenen tot digitale patiëntendossiers. Voor de scope en uitkomsten van het onderzoek verwijs ik naar de website van AP[2]. Hierin zijn negen uiteenlopende instellingen opgenomen, waarbij de AP aanwijzingen heeft gegeven tot verbeteringen. Tegelijkertijd concludeerde AP dat de problematiek naar verwachting breder speelde. In reactie hierop zijn door de brancheorganisaties handreikingen opgesteld om de beveiliging van medische gegevens te verbeteren.
Sinds 1 januari 2016 geldt er een meldplicht voor datalekken. Organisaties moeten een melding doen bij de AP zodra zij een ernstig datalek hebben en passende maatregelen treffen. De AP registreert de gemelde datalekken in een niet openbaar register. Ook de IGZ houdt geen openbare registratie hiervan bij.

Vraag 6
Hoe versterken of verzwakken de door u gewenste invoering van een landelijk schakelpunt (LSP), en de uitwisseling van persoonlijke gegevens binnen dat systeem, de veiligheid van medische gegevens? Kunt u uw antwoord toelichten?

Antwoord 6
Ook voor de uitwisseling van persoonsgegevens tussen meerdere partijen, via bijvoorbeeld een landelijk schakelpunt, zoals het LSP, gelden de regels over de omgang van persoonsgegevens zoals vastgelegd in de Wet bescherming persoonsgegevens (Wbp). Het is aan de AP om te oordelen in hoeverre praktijksituaties als deze aan wet- en regelgeving voldoen. Daarnaast moeten partijen ook hier voldoen aan de NEN 7510. Verder ligt het Wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens ter behandeling voor in de Eerste Kamer. Dit wetsvoorstel regelt de randvoorwaarden bij elektronische uitwisseling van gegevens tussen zorgaanbieders. In een algemene maatregel van bestuur (AMvB) behorend bij het wetsvoorstel worden op grond van artikel 26 Wbp specifieke functionele, technische en organisatorische eisen aan elektronische gegevensuitwisseling in zijn algemeenheid vastgelegd. In het hele proces blijft de aan de volgende stap aanleverende partij verantwoordelijk voor het treffen van voldoende maatregelen om te borgen dat de partij waaraan wordt aangeleverd zich aan de afgesproken regels rond beveiliging en geheimhouding houdt en dat de afspraken daarover worden nageleefd.

Vraag 7
Wat is uw reactie op de tv-uitzending van omroep Max waaruit blijkt dat Belgische gevangenen medische dossiers ongemerkt laten verdwijnen, omdat zij per kilo verwerkt papier krijgen betaald?[3]

Antwoord 7
Ik vind het onwenselijk als (in Belgische gevangenissen) onzorgvuldig met patiëntendossiers is omgaan. Patiënten moeten erop kunnen vertrouwen dat de bescherming van medische informatie voldoende is gegarandeerd door de ziekenhuizen. Deze werkzaamheden laten uitvoeren door Belgische gevangenen zorgt voor onrust en onzekerheid. Ik heb begrepen dat het uitvoeren van

[2] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-patientendossiers-binnen-zorginstellingen.pdf
[3] Zie http://www.uitzendinggemist.net/aflevering/343762/Meldpunt.html

deze werkzaamheden in gevangenissen inmiddels niet meer voorkomt. Zie verder ook mijn antwoorden op eerdere vragen over dit onderwerp[4].
De Autoriteit Persoonsgegevens (AP) heeft mij laten weten al eerder contact te hebben opgenomen met de Belgische privacytoezichthouder die inmiddels een onderzoek is gestart naar de gang van zaken in de Belgische gevangenissen. Tevens heeft de AP aangegeven dat ze zich door ziekenhuizen zekerheidshalve laat informeren over de afspraken die gemaakt zijn in bewerkersovereenkomsten met derde partijen voor het uitvoeren van werkzaamheden op het gebied van gegevensverwerking.
Overigens zal over dit onderwerp door uw Kamer binnenkort een debat worden gepland, naar aanleiding van de Regeling van werkzaamheden van d.d. 2 maart 2016. Voorafgaand aan dit debat zal ik uw Kamer nog een aparte brief doen toekomen.

Vraag 8
Erkent u dat veilige omgang met medische gegevens, dus ook opslag, het digitaliseringsproces en vernietiging na verstrijken van de bewaartermijn, integraal onderdeel zijn van de patiëntveiligheid? Zo nee, waarom niet? Zo ja, op welke wijze wilt u goede omgang met medische gegevens door zorgorganisaties en zorgverleners versterken?

Antwoord 8
Veilige omgang met medische gegevens valt daar als zodanig alleen onder als er een link is met mogelijk lichamelijk of psychisch leed. Overigens ben ik van mening dat veilige omgang met medische gegevens een belangrijk fundament onder vertrouwen van de patiënt in de gezondheidszorg is.

Vraag 9
Is de Inspectie voor de Gezondheidszorg (IGZ), gelet op de lauwe reactie op de recente onthullingen, voldoende doordrongen van de ernst van de situatie? Kunt u uw antwoord toelichten?

Antwoord 9
De IGZ is voldoende doordrongen van de ernst van de situatie en heeft mij al aangegeven dat zij toezicht houden op de veldnorm NEN 7510 over informatiebeveiliging in de zorg. Een goed informatiebeveiligingsbeleid houdt ook in dat bewerkersovereenkomsten op een verantwoorde wijze zijn gesloten tussen ziekenhuizen en partijen die gegevens in opdracht van deze ziekenhuizen bewerken. Ook zal de IGZ de Nederlandse Federatie van Universitair Medische Centra en de Nederlandse Vereniging van Ziekenhuizen een brief sturen om ziekenhuizen op hun verantwoordelijkheid te wijzen.

Vraag 10
Hoe voorkomt de IGZ dat gevoelige medische gegevens, over bijvoorbeeld bekende Nederlanders, in handen komen van criminelen die dit mogelijk kunnen gebruiken voor chantagedoeleinden? Is dit al wel eens eerder voorgekomen, voor zover u weet?

Antwoord 10
Zorginstellingen moeten voldoen aan de geldende wet- en regelgeving en in eerste plaats zelf ervoor zorgen dat dit niet mogelijk is. De AP en IGZ zien toe op de naleving van de wet- en regelgeving. Het Openbaar Ministerie en de politie treden op indien medische gegevens worden misbruikt voor chantagedoeleinden. Navraag bij het Openbaar Ministerie leert dat er geen gegevens bekend zijn of deze situaties zich in Nederland hebben voorgedaan.

Vraag 11
Heeft de IGZ, die toeziet op naleving van het medisch beroepsgeheim, geregeld overleg over dit onderwerp met (bijzondere) opsporingsdiensten, zoals de politie of de Inspectie SZW? Zo nee, is het daar volgens u dan niet de hoogste tijd voor?

---

[4] Eerdere vragen terzake van de leden Klever (PVV), ingezonden 26 januari 2016 (vraagnummer 2016Z01443), De Lange (VVD), ingezonden 27 januari 2016 (vraagnummer 2016Z01580) en Oosenbrug (PvdA), ingezonden 27 januari 2016 (vraagnummer 2016Z01560).

Antwoord 11
De inspectie voert regelmatig overleg met onder meer het Openbaar Ministerie en de AP. In dit overleg komt ook dit onderwerp aan de orde.