Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

Aanhangsel van de Handelingen

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

3279

Vragen van de leden **Oosenbrug** en **Bouwmeester** (beiden PvdA) aan de Minister van Volksgezondheid, Welzijn en Sport en de Staatssecretaris van Veiligheid en Justitie over *de bescherming van persoonsgegevens in de zorg* (ingezonden 13 juli 2015).

Antwoord van Minister **Schippers** (Volksgezondheid, Welzijn en Sport), mede namens de Staatssecretaris van Veiligheid en Justitie (ontvangen 2 september 2015). Zie ook Aanhangsel Handelingen, vergaderjaar 2014–2015, nr. 2928.

Vraag 1
Heeft u kennisgenomen van de berichten «Zorg kent nieuwe privacyregels niet»[1] en «Artsen whatsappen elkaar patiëntinformatie»?[2]

Antwoord 1
Ja, ik heb kennis genomen van deze berichten.

Vraag 2 en 3
Bent u van mening dat de zorgsector onvoldoende op de hoogte is van nieuwe regels voor de bescherming van persoonsgegevens en de risico's voor de sector? Zo ja, welke kennis had u hier al verwacht? Zo nee, waarom niet?
Op welke wijze worden organisaties in de zorg, die zeer gevoelige data beheren, geïnformeerd over de wijzigingen in de Wet bescherming persoonsgegevens die op 1 januari 2016 van kracht worden? Hoe wordt er zicht gehouden op de voorbereidingen die zorginstellingen treffen voor de invoering van de meldplicht datalekken?

Antwoord 2 en 3
De wetswijziging waarop wordt gedoeld is de wet van 4 juni 2015 (Stb. 2015, 230) tot invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (meldplicht datalekken) alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens (CBP) om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens (Wbp) een bestuurlijke boete op te leggen. Deze wet treedt op 1 januari 2016 in werking (inwerkingtredingsbesluit van

[1] http://www.skipr.nl/actueel/id22970-zorg-kent-nieuwe-privacyregels-niet.html
[2] http://nos.nl/artikel/2045825-artsen-whatsappen-elkaar-patientinformatie.html

ah-tk-20142015-3279
ISSN 0921 - 7398
's-Gravenhage 2015

1 juli 2015, Stb. 2015, 281). De meldplicht voor datalekken heeft een algemene strekking en is derhalve niet uitsluitend gericht op de zorgsector. Het is in beginsel aan de zorgsector (net als bij andere sectoren) zelf zich de inhoud van de wet eigen te maken en deze toe te passen in de praktijk. Hierbij kan gebruik worden gemaakt van de beleidsregels in de vorm van richtsnoeren die zullen worden opgesteld door het CBP. Dit najaar zal het CBP een openbare consultatie houden over door hem opgestelde concept-richtsnoeren. Ik verwacht dat de zorgsector ook gebruik maakt van de mogelijkheid om te reageren. Op grond van artikel 67 van de gewijzigde Wbp overlegt het CBP voorafgaand aan het vaststellen van de richtsnoeren voor de meldplicht datalekken met de Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties. Daarnaast zal het kabinet, in samenspraak met het CBP, brede bekendheid geven aan de nieuwe regels.
Ik houd geen zicht op de voorbereidingen die zorginstellingen treffen, omdat het aan de zorginstellingen zelf is om aan de regelgeving te voldoen. Ik kan dus ook niet inschatten of de zorgsector voldoende op de hoogte is van de nieuwe regels. Het is uiteindelijk aan het CBP als toezichthouder om dit te controleren.
Voor zover in vraag 2 nog gedoeld wordt op de Europese privacyverordening, wil ik u erop wijzen dat deze verordening nog in ontwikkeling is en er nog geen datum bekend is waarop de verordening tot stand zal komen en in werking treedt. Daarna geldt een implementatietermijn van twee jaar voordat de verordening van toepassing wordt in de lidstaten. Ik verwacht dan ook niet dat de zorgsector reeds van de precieze inhoud van deze verordening op de hoogte is.

Vraag 4
Deelt u de mening dat de zorg voor de bescherming van persoonsgegevens niet gewaarborgd kan worden met enkel technische voorzieningen, maar dat het gedrag van de gebruikers even belangrijk is? Zo ja, hoe wordt ervoor gezorgd dat de verantwoordelijkheid van de bescherming van medische persoonsgegevens in de werkzaamheden van alle betrokkenen geïntegreerd wordt?

Antwoord 4
Ik deel uw mening dat het gedrag van mensen mede bepalend is voor de bescherming van persoonsgegevens. Het is aan de zorgsector zelf invulling te geven aan hetgeen in wet- en regelgeving hieromtrent is geregeld. De koepels van zorgverleners en diverse regionale (ICT-) samenwerkingsverbanden van zorgaanbieders hebben de wettelijke regels rond privacy en beroepsgeheim bij uitwisseling van patiëntgegevens praktisch toepasbaar gemaakt in de Gedragscode elektronische gegevensuitwisseling in de zorg (EGiZ).

Vraag 5
Bent u van mening dat een communicatieplatform als Whatsapp voldoende beveiligd is voor de uitwisseling van patiëntgegevens en foto's? Zo ja, waarom? Zo nee, welke risico's kleven er aan?

Antwoord 5
In zijn algemeenheid geldt dat uitwisseling van persoonsgegevens moet voldoen aan de bestaande wet- en regelgeving, met name de Wbp. Het CBP ziet hierop toe. Het CBP heeft in februari 2013 richtsnoeren vastgesteld waaraan de beveiliging van persoonsgegevens moet voldoen.

Vraag 6
Moet aan patiënten separaat toestemming gevraagd worden voor hun gegevens uitgewisseld mogen worden via een nieuw communicatieplatform als Whatsapp? Zo nee, waarom niet? Zo ja, hoe kan deze expliciete toestemming georganiseerd worden?

Antwoord 6
Voor alle systemen voor elektronische gegevensuitwisseling geldt dat ze moeten voldoen aan de bestaande wet- en regelgeving als de Wbp en de Wet geneeskundige behandelovereenkomst (WGBO). Voor gegevensuitwisseling is

toestemming van de patiënt nodig (met uitzondering voor waarnemers en rechtstreeks bij de behandeling betrokkenen). Uiteraard geldt daarbij dat elektronische gegevensuitwisseling alleen is toegestaan als er sprake is van passende beveiliging op grond van de Wbp.

Vraag 7
Wordt er binnen de medische sector nagedacht over en/of gewerkt aan een kader voor veilige manieren om snel en direct informatie uit te wisselen tussen medisch professionals, ook buiten hun vaste werkplek? Zo nee, wilt u de noodzaak hiervoor bespreken met de sector? Zo ja, op welke wijze draagt u aan dit proces bij met kennis en expertise?

Antwoord 7
Mijn verantwoordelijkheid is de randvoorwaarden te creëren waaronder gegevens veilig kunnen worden uitgewisseld. In aanvulling op de bestaande wet- en regelgeving (WGBO en Wbp) ligt mijn wetvoorstel Cliëntenrechten bij elektronische verwerking van gegevens ter behandeling bij de Eerste Kamer. In een algemene maatregel van bestuur (AMvB) op grond van artikel 26 Wbp worden specifieke functionele, technische en organisatorische eisen gesteld aan elektronische gegevensuitwisseling. In deze AMvB wordt voor de informatiebeveiliging in de zorg dwingend verwezen naar beschikbare normen van het Nederlands Normalisatie-instituut, te weten NEN 7510;2011 (NEN 7510) en de verdere uitwerking van deze algemene norm betreffende informatiebeveiliging in de zorg in NEN 7512 en NEN 7513. Als een zorgaanbieder de in NEN 7510 en overige genoemde normen aangegeven maatregelen heeft getroffen, mag er vanuit worden gegaan dat deze «passende technische en organisatorische maatregelen» heeft getroffen, als bedoeld in artikel 13 van de Wbp.
Het is aan de zorgsector zelf deze regels om te zetten in verantwoord gedrag. Zoals aangegeven bij het antwoord op vraag 4, hebben zorgaanbieders de bestaande wet- en regelgeving rond veilige gegevensuitwisseling «vertaald» in een praktische gedragscode voor zorgaanbieders: de gedragscode Elektronische gegevensuitwisseling in de zorg (EGiZ).