Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

31 765 Kwaliteit van zorg

Nr. 259

BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 15 december 2016

Hierbij bied ik u het onderzoekrapport «Beveiliging van patiëntgegevens», van het adviesbureau PBLQ aan[1] en mijn reactie daarop. Met deze brief informeer ik u tevens over de toezeggingen van de Inspectie voor de Gezondheidszorg (hierna: inspectie) en de Autoriteit Persoonsgegevens (AP) die verband houden met de werkzaamheden rond het digitaliseren van patiëntendossiers door gevangenen wat een onderdeel is van het uitgevoerde onderzoek.

1. Aanleiding voor het onderzoek

Aanleiding voor dit onderzoek is in mijn brief van 16 maart 2016[2] toegelicht en mijn toezegging tijdens het Algemeen Overleg gegevensuitwisseling van 29 juni 2016 (Kamerstuk 27 529, nr. 140). Ik heb dit onderzoek laten uitvoeren, mede naar aanleiding van de diverse berichten in de media over het onzorgvuldig omgaan met privacygevoelige gegevens van patiënten. Het onderzoek gaat in op de vraag op welke wijze zorginstellingen (ziekenhuizen, zelfstandige klinieken en instellingen voor geestelijke gezondheidszorg) in de dagelijkse praktijk de beveiliging van hun patiëntgegevens kunnen verbeteren.

Tevens wil ik u met deze brief informeren dat parallel aan dit onderzoek in opdracht van de Inspectie voor de Gezondheidszorg door het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) ook twee onderzoeken voor het versterken van de toezichtfunctie op het gebied van ICT in de Zorg zijn uitgevoerd. De inspectie zal de uitkomsten van deze twee onderzoeken gebruiken voor het versterken van haar toezichtsfunctie. De conclusies van beide onderzoeken komen sterk overeen met de conclusies

[1] Raadpleegbaar via www.tweedekamer.nl

[2] Brief Verzoek uit Regeling van werkzaamheden inzake het bericht «Gevangenen kregen gevoelige patiëntgegevens onder ogen» (Rtl.nl, 1 maart 2016), 16 maart 2016 (Kamerstuk 31 765, nr. 196)

kst-31765-259
ISSN 0921 - 7371
's-Gravenhage 2016

van het PBLQ-onderzoek. De resultaten van de RIVM-onderzoeken kunt u vinden op een nieuwe webpagina «ICT in de zorg» op www.rivm.nl [3].

Tijdens het AO Gegevensuitwisseling (Kamerstuk 27 529, nr. 140) heb ik toegezegd de Kamer voor het einde van dit jaar te informeren of de inspectie meldingen heeft ontvangen naar aanleiding van een casus waarbij Belgische gedetineerden in Leuven werkzaamheden rond het digitaliseren van patiëntendossiers van Nederlandse ziekenhuizen hebben uitgevoerd. Daarbij zijn mogelijk delen van patiëntendossiers verloren gegaan. De inspectie heeft mij laten weten geen meldingen te hebben ontvangen.

2. Bevindingen van het onderzoek van PBLQ

De belangrijkste conclusies die in het onderzoek naar voren komen, zijn:
- De afgelopen jaren heeft de informatiebeveiliging en privacybescherming in de meeste zorginstellingen veel meer aandacht gekregen en is de bewustwording bij instellingen toegenomen.
- Hoewel sprake is van een positieve ontwikkeling rond informatiebeveiliging, zijn incidenten niet te voorkomen. Dit komt doordat waterdichte beveiliging feitelijk niet mogelijk is. Het is echter van belang dat er wordt geleerd en dat de informatiebeveiliging en privacybescherming continu worden verbeterd.
- In de praktijk staan de vertrouwelijkheid en de beschikbaarheid van gegevens soms op gespannen voet met elkaar.
- Uit het onderzoek komt geen indicatie naar voren dat verdere aanvulling van wet- en regelgeving voor informatiebeveiliging en privacybescherming in zorginstellingen noodzakelijk is. Uit de interviews en enquête blijkt wel dat er behoefte is aan het begrijpelijker maken van de huidige en komende wet- en regelgeving en het vertalen ervan naar basisprincipes en concrete handvatten voor de praktijk.
- Uit de interviews en de enquête blijkt dat niet alle zorginstellingen een compleet beeld hebben van welke bewerkers en subbewerkers hun patiëntgegevens bewerken. Niet alle zorginstellingen blijken met bewerkers contracten te hebben afgesloten. En daar waar dat wel het geval is, voldoen die niet altijd aan de eisen die de AP daaraan stelt. De borging van de bescherming van patiëntgegevens tussen zorginstellingen en (sub)bewerkers verschilt per zorginstelling.

Samengevat geeft PBLQ de volgende aanbevelingen:
1. Het *bevorderen van goed gedrag*. Begin top-down door het management het goede voorbeeld te laten geven en verwijder drempels op de werkvloer die informatiebeveiliging en privacybescherming belemmeren.
2. Zorg ervoor dat *good practices* die in het onderzoek naar voren zijn gekomen navolging krijgen, zoals het NFU-normenkader rond informatiebeveiliging en het handboek NEN 7510. Ook beveelt het rapport aan om, zoals diverse zorginstellingen al doen, een geïntegreerd systeem en proces voor het registreren en afhandelen van datalekken op te zetten in de bestaande systematiek voor de afhandeling van (andere) veiligheidsincidenten (veiligheidsincidentmelding- (VIM) / veiligheidsmanagementsysteem (VMS)).
3. De *Krachten bundelen* waardoor de effectiviteit van informatiebeveiliging en privacybescherming kan worden vergroot. Zoals koepels die in overleg met toezichthouders (AP en de inspectie) en VWS meer

[3] www.rivm.nl/Onderwerpen/I/ICT_in_de_zorg

sectorale afspraken maken. Hierbij kan ook gedacht worden aan een model bewerkersovereenkomst.
4. Het *bieden van handvatten voor wet- en regelgeving*. VWS, koepels en toezichthouders dienen te faciliteren dat wet- en regelgeving goed begrepen kan worden door mensen die in de zorg werken via praktische handvatten voor de praktijk. Bijvoorbeeld door de regelgeving te presenteren in sectorale en beroepsgerichte gedragscodes en thematische richtsnoeren.
5. *Anticipeer op de komst van de Algemene Verordening Gegevensbescherming (AVG)* door de lat voor informatiebeveiliging en privacybescherming hoger dan de vigerende wet- en regelgeving te leggen. Een onderdeel hiervan is dat VWS en de AP duidelijk moeten aangeven in hoeverre en onder welke voorwaarden gepseudonimiseerde patiëntgegevens gebruikt mogen worden bij (wetenschappelijk) onderzoek en kwaliteitsregisters.

Ten aanzien van de (sub)bewerkersovereenkomsten geeft het rapport het advies aan zorginstellingen om in hun contracten met bewerkers te laten opnemen dat:
– De zorginstelling precies weet welke patiëntgegevens door welke (sub)bewerkers worden bewerkt.
– Bewerkers en (sub)bewerkerscontracten te laten voldoen aan de voorwaarden die de AP daaraan stelt. Op deze wijze is geen verdere aanvulling van wetgeving noodzakelijk en kan door middel van de bewerkersovereenkomst een incident als de bewerking van patiëntdossiers door gevangenen worden voorkomen.
– Te zorgen voor een standaard bewerkersovereenkomst waarmee alle partijen in de sector uit de voeten kunnen.

3. Beleidsreactie

De vertrouwelijkheid van medische informatie en de vertrouwelijke omgang met patiëntgegevens in de gezondheidszorg is essentieel en het is een kernwaarde voor zowel patiënten als zorgaanbieders. Het is goed dat op basis van het onderzoek geconstateerd kan worden dat de informatiebeveiliging en privacybescherming veel meer aandacht gekregen heeft en dat de bewustwording bij instellingen is toegenomen. De wil en het besef dat patiëntgegevens moeten worden beschermd is er bij zorginstellingen. Er blijkt echter uit het onderzoek ook dat een flink aantal zaken voor verbetering vatbaar is. Zorginstellingen en zorgverleners zijn hier in eerste plaats zelf voor verantwoordelijk en moeten voldoen aan Europese en nationale wettelijke voorschriften. De IGZ en AP zien hier op toe, het Ministerie van VWS kan daar waar nodig faciliterend optreden.

Lopende initiatieven verder ondersteunen

Ik heb waardering voor de initiatieven en inspanningen die de sector zelf al neemt. Hierbij denk ik aan de campagne «Zeker» die medewerkers van zorginstellingen op een toegankelijke en aansprekende manier bewust maakt van het belang van informatiebeveiliging. Ook ondersteun ik het initiatief tot het oprichten van een Zorg-Cert[4] waartoe de sector zelf het initiatief heeft genomen. Ik heb daarom een opstartsubsidie toegekend om de aanloopverliezen op te vangen. Ik zie de oprichting van de Zorg-Cert als een extra maatregel om bij datalekken als gevolg van cyberincidenten snel in actie te kunnen komen, en om snelle detectie en kennisdeling over informatiebeveiligingsincidenten te vergroten en

[4] Een Computer Emergency Response Team richt zich op het voorkomen en genezen van netwerk gerelateerde veiligheidsincidenten.

hiermee de impact van dergelijke incidenten tot een minimum te beperken.

Verdere actie nodig

Maar hiermee zijn we er nog niet. Gezien het aantal en de diversiteit van de aanbevelingen die PBLQ in het rapport gedaan heeft, is het noodzakelijk om met alle betrokken partijen de komende periode een «Actieplan (informatie)beveiliging patiëntgegevens» op te zetten. Hierbij zal een belangrijke rol zijn weggelegd voor de koepels van de ziekenhuizen, zelfstandige klinieken, GGZ-instellingen en Patiëntenfederatie, en ook voor VWS en de toezichthouders. Ik zal op korte termijn het initiatief nemen om met de genoemde organisaties te starten met het Actieplan. Daarbij zal ik mogelijk op een later moment ook koepels uit de andere sectoren betrekken. Ik verwacht van de organisaties dat iedereen zijn verantwoordelijkheid neemt: zowel bij het opstellen van het plan als bij de uitvoering ervan. Mocht dat nodig zijn, dan ben ik desgewenst bereid om hieraan financieel steun te verlenen, op basis van een concrete onderbouwing en op voorwaarde dat alle partijen hun eigen (financiële) verantwoordelijkheid nemen en rolvast zijn. Ik streef ernaar dat het Actieplan in het voorjaar van 2017 gereed is, waarna de implementatie direct kan starten voor zover dat nog niet is gebeurd. Ik wil alvast aangeven dat ik verwacht dat het genoemde Actieplan een meerjarig karakter zal hebben. Het Actieplan zal moeten leiden tot structurele verbeteringen in de dagelijkse werkpraktijk in de genoemde zorginstellingen: in de bestuurskamer en bij de stafdiensten, bij de artsen, bij verpleegkundigen en bij onderzoekers. Dat is een ambitieuze opgave, omdat het in de kern ook gaat over veranderingen in gedrag van mensen en verandering van de cultuur van organisaties.

Mijn voorstel voor het Actieplan sluit ook aan op de reactie van de koepelorganisaties op het rapport. Zij willen met VWS in overleg over mogelijkheden en randvoorwaarden hoe de inspanningen van het hele zorgveld geïntensiveerd, ondersteund en verbreed kunnen worden.

Bewerkersovereenkomsten

Ten aanzien van de bewerkerovereenkomsten concludeer ik als volgt. In het rapport staat dat – indien (sub)bewerkersovereenkomsten voldoen aan de voorwaarden die de AP stelt – er geen verdere aanvulling van wetgeving noodzakelijk is. Op dit moment is er dus geen aanvullende wetgeving noodzakelijk. Verbeteringen voor bewerkersovereenkomsten zijn mogelijk binnen de bestaande regelgeving. Het is aan de zorginstellingen om de bewerkersovereenkomsten op de juiste manier af te sluiten. De AP heeft onlangs nog richting de koepels expliciet aangegeven waaraan een bewerkersovereenkomst standaard moet voldoen. Zie hierover ook de brief van de AP van 12 mei 2016[5] waarin de AP constateert dat nog niet ieder ziekenhuis hieraan voldoet.

Het rapport beveelt voorts aan dat zorginstellingen en de bewerkers volstrekte duidelijkheid moeten hebben over welke patiëntgegevens door precies welke (sub)bewerkers worden bewerkt. In de gevallen dat gevangenen zijn ingezet voor werk aan patiëntendossiers, was die duidelijkheid er blijkbaar niet. Dat is betreurenswaardig. Overigens wil ik nogmaals volstrekt helder maken dat ik het onwenselijk acht dat gevangenissen werkzaamheden uitvoeren rond de bewerking van patiëntendossiers, zoals dit in het verleden heeft plaatsgevonden.

[5] Brief AP bewerkerovereenkomsten in de zorg, 12 mei 2016, kenmerk Z2016–10438

Om dit te benadrukken wil ik ervoor zorgen dat zorginstellingen op korte termijn gebruik kunnen maken van een standaard bewerkersovereenkomst, waarin dit punt nog een keer wordt geregeld.
Hierdoor kan door middel van de bewerkersovereenkomst een incident als de bewerking van patiëntdossiers door gevangenen worden voorkomen.

4. Slotopmerkingen

Ik wil tot slot benadrukken dat patiënten er op moeten kunnen vertrouwen dat de bescherming van medische informatie is gegarandeerd door de zorginstellingen. Beveiliging van patiëntgegevens is een doorlopend punt van aandacht en zal altijd een onderwerp blijven waar alle partijen zich voor moeten inzetten. Ik zal uw Kamer informeren over het Actieplan beveiliging patiëntgegevens zodra dit gereed is.

De Minister van Volksgezondheid, Welzijn en Sport,
E.I. Schippers