Waterdichte beveiliging patiëntgegevens onmogelijk

19 december 2016

De meeste zorginstellingen zijn de afgelopen jaren wel meer aandacht gaan besteden aan informatiebeveiliging en privacybescherming. Ook is de bewustwording bij instellingen op beide gebieden toegenomen. Dit concludeert PBLQ in een onderzoek naar de beveiliging van patiëntgegevens. Het onderzoek (pdf) is uitgevoerd in opdracht van minister Schippers van Volksgezondheid, Welzijn en Sport (VWS), nadat verschillende incidenten met patiëntgegevens aan het licht kwamen. Schippers heeft een actieplan aangekondigd om de veiligheid van patiëntgegevens te vergroten.

Dat die veiligheid niet altijd afdoende is, bleek in november nog uit cijfers van de Autoriteit Persoonsgegevens in het kader van de Meldplicht Datalekken. Bijna elke dag maakt een Nederlands ziekenhuis melding van dataverlies. Een kwart van alle in 2016 gemelde datalekken(ruim 4.000) vond plaats bij zorginstellingen.

Onduidelijkheid

Het onderzoek van PBLQ komt niet met indicaties dat verdere aanvulling van wet- en regelgeving voor informatiebeveiliging en privacybescherming in zorginstellingen noodzakelijk is. Wel blijkt dat de huidige en komende wet- en regelgeving niet altijd duidelijk is en begrijpelijker kan worden gemaakt. Ook is er behoefte aan een vertaling van wet- en regelgeving naar basisprincipes en concrete handvatten voor de praktijk. Koepelorganisaties KNMG, NHG, LHV en KNMP hebben mede hierom een handreiking gepubliceerd waarmee ze hun achterban willen ondersteunen in de omgang met deze Meldplicht.

Niet alle zorginstellingen hebben een compleet beeld van welke externe (sub)bewerkers hun patiëntgegevens mogen bewerken. Ook blijken niet alle zorginstellingen met bewerkers contracten te hebben afgesloten, of voldoen contracten niet altijd aan de eisen die de Autoriteit Persoonsgegevens (AP) hieraan stelt. De borging van de bescherming van patiëntgegevens tussen zorginstellingen en (sub)bewerkers verschilt per zorginstelling, aldus PBLQ. Het bureau adviseert dan ook te zorgen voor een standaard bewerkersovereenkomst voor alle partijen in de zorg.

In (sub)bewerkersovereenkomsten zou moeten worden opgenomen dat:

- zorginstellingen precies weten welke patiëntgegevens door welke (sub)bewerkers worden bewerkt.
- Afdwingbaar is dat bewerkers en (sub)bewerkerscontracten voldoen aan de voorwaarden die de AP hieraan stelt. Hierdoor is geen verdere aanvulling van wetgeving nodig.

Aanbevelingen

Het bureau komt verder op basis van alle bevindingen met een aantal aanbevelingen:

- Bevorder goed gedrag. Laat het management het goede voorbeeld geven en verwijder drempels op de werkvloer die informatiebeveiliging en privacybescherming belemmeren.
- Geef good practices uit het onderzoeksrapport navolging, zoals het NFU-normenkader rond informatiebeveiliging en het handboek NEN 7510. Ook adviseert het rapport een geïntegreerd systeem en proces voor het registreren en afhandelen van datalekken op te zetten. Verschillende zorginstellingen beschikken al over zo'n systeem.
- Bundel krachten om de effectiviteit van informatiebeveiliging en privacybescherming te vergroten. Denk hierbij aan koepels die in overleg met toezichthouders en VWS meer sectorale afspraken maken of een model bewerkersovereenkomst opstellen.
- Biedt handvatten voor wet- en regelgeving. VWS, koepels en toezichthouders moeten volgens PBLQ zorgen dat wet- en regelgeving begrijpelijk voor mensen die in de zorg werken. Dit kan door praktische handvatten voor de praktijk op te stellen en regelgeving te presenteren in sectorale en beroepsgerichte gedragscodes en thematische richtsnoeren.
- Anticipeer op de komst van de Algemene Verordening Gegevensbescherming (AVG) door de lat voor informatiebeveiliging en privacybescherming hoger te leggen dan de huidige wet- en regelgeving vereist. VWS als de AP zouden moeten aangeven in hoeverre en onder welke voorwaarden gepseudonimiseerde patiëntgegevens gebruikt mogen worden bij (wetenschappelijk) onderzoek en kwaliteitsregisters.

Maatregelen VWS

Minister Schippers heeft naar aanleiding van het onderzoeksrapport een brief naar de Tweede Kamer gestuurd. Zij stelt in de brief dat de vertrouwelijkheid van medische informatie en de vertrouwelijke omgang met patiëntgegevens in de gezondheidszorg essentieel en een kernwaarde voor zowel patiënten als zorgaanbieders.

De minister stelt waardering te hebben voor initiatieven en inspanning die de sector zelf neemt en wijst op de campagne 'Zeker' als voorbeeld. Deze campagne moet medewerkers van zorginstellingen op een toegankelijke manier bewust maken van het belang van informatiebeveiliging.

Ook ondersteunt de bewindsvrouw het initiatief om een Zorg-CERT (Computer Emergency Response Team) op te richten, dat als focus heeft het voorkomen en genezen van netwerkgerelateerde veiligheidsincidenten. Dit is volgens minister Schippers een extra maatregel om bij datalekken snel in actie te kunnen komen, lekken snel te detecteren, de kennisdeling over informatiebeveiliging te vergroten en de impact van incidenten te minimaliseren.

Verder komen er maatregelen onder de noemer 'Actieplan (informatie)beveiliging patiëntgegevens', met een belangrijke rol voor koepelorganisaties van ziekenhuizen, zelfstandige klinieken, GGZ-instellingen, Patiëntenfederatie, VWS en de toezichthouders. Zo nodig wil de minister hier geld voor beschikbaar stellen. Het actieplan moet in het voorjaar van 2017 afgerond worden en ook meteen uitgevoerd.

De minister stelt ten slotte dat zij een standaard bewerkersovereenkomst beschikbaar wil stellen voor de zorgsector.