AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Prins Clauslaan 60, 2595 AJ Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Raad van Bestuur Zorginstelling (ziekenhuis, GGz-instelling, huisartsenposten)

Datum
15 februari 2016

Ons kenmerk
z2012-00179

Contactpersoon

Onderwerp
Gecontroleerde toegang voor medewerkers van zorginstellingen tot gegevens van de patiënt in het instellings-EPD

Geachte leden van de Raad van Bestuur,

De Autoriteit Persoonsgegevens krijgt regelmatig vragen en signalen over patiëntendossiers die onder ogen zouden zijn gekomen van medewerkers van zorginstellingen die daar niets mee te maken hadden; de 'kan-dat-zomaar'-vraag. Het ging bijvoorbeeld om een student met een bijbaan op de administratie van een ggz-instelling die een dossier van een medestudent zou hebben bekeken of collega's op een huisartsenpost of binnen een ziekenhuis die in elkaars behandeldossiers zouden hebben gekeken. De Autoriteit Persoonsgegevens deed naar aanleiding van deze signalen onderzoek bij negen zorginstellingen. Het voorkomen van dit soort incidenten en het daadwerkelijk goed regelen van gecontroleerde toegang tot patiëntgegevens bleek een complexe, maar niet onmogelijke opgave.

Als een patiënt zich tot een zorgverlener wendt in verband met een gezondheidsprobleem, dan weet die patiënt dat het prijsgeven van - soms zeer - privacygevoelige gegevens daarbij aan de orde zal zijn. Het waarborgen van een vertrouwelijke omgang met dergelijke gegevens is in de gezondheidszorg van groot belang. Mensen hebben recht op bescherming van hun persoonsgegevens. Onzorgvuldigheid hierbij zou mensen bovendien kunnen afschrikken om tijdig hulp te vragen. Uw sector heeft al veel maatregelen getroffen om het vertrouwen te kunnen behouden. Bij nieuwe ICT-voorzieningen kunnen zich nieuwe risico's voor de vertrouwelijke behandeling van patiëntgegevens aandienen. Die risico's moeten goed in beeld worden gebracht en op passende wijze worden ondervangen. Op het niveau van de Raad van Bestuur is alertheid en focus bij beslissingen over nieuwe ICT in zorginstellingen onmisbaar.

Bijlage(n) 1

Datum
15 februari 2016

Ons kenmerk
z2012-00179

Met deze open brief vraag ik Raden van Bestuur van zorginstellingen zich te beraden op de stand van zaken in hun eigen zorginstelling en daar waar tekortkomingen worden geconstateerd, alsnog gepaste maatregelen te nemen. Zodat zeker gesteld wordt dat alle zorginstellingen alles doen wat redelijkerwijs mogelijk is – gegeven de stand van de techniek en kosten van tenuitvoerlegging van maatregelen (artikel 13 Wet bescherming persoonsgegevens (Wbp)) – om te zorgen dat zij het vertrouwen van hun patiënten in de zorgvuldige omgang met hun gegevens niet schaden. Het zorgvuldig omgaan met persoonsgegevens van patiënten maakt integraal deel uit van de patiëntenzorg.

Ik informeer u hierbij over ons onderzoek, de huidige stand van zaken en de wettelijke vereisten. Daarbij verwijs ik naar documentatie die behulpzaam kan zijn bij eventuele verbetertrajecten voor uw instelling.

Onderzoek Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens deed vanaf 2012 diepgaand onderzoek bij negen uiteenlopende zorginstellingen naar de aanwezigheid van maatregelen om aan medewerkers op gecontroleerde wijze toegang te verlenen tot de gegevens van de patiënt in het elektronisch patiëntendossier (EPD) van de instelling. Het gaat daarbij om maatregelen op het gebied van autorisaties, logging en controle van logging. De conclusie was dat het beleid en de praktijk in de onderzochte zorginstellingen niet in overeenstemming waren met de vereisten van artikel 13 Wbp.

Bij de onderzochte instellingen:

- was sprake was van toekenning van *te ruime autorisaties* aan medewerkers voor toegang tot het instellings-EPD.

Zorginstellingen maakten – over het algemeen - te weinig gebruik van mogelijkheden om op grond van bijvoorbeeld behandelplan, specialisme, afdeling of werkcontext en consultatieverzoeken de autorisaties van medewerkers zo veel mogelijk te beperken tot gegevens van die patiënten waarbij ze een rol in de behandeling of verzorging vervullen. Er was ook sprake van organisatorische tekortkomingen, zoals een gebrek aan benodigde menskracht voor opbouw en onderhoud van een systeem voor autorisaties op naam. Daarnaast waren er technische problemen om de autorisaties goed te regelen, hiervoor ontbraken soms zelfs functionaliteiten in het gebruikte instellings-EPD.

- *ontbrak het aan afdoende controle* op het gebruik door medewerkers van de hun toegekende toegangsrechten. Daardoor ontbrak het ook aan het daadwerkelijk opleggen van sancties bij misbruik van die toegangsrechten.

Zorginstellingen hadden weliswaar een sanctiebeleid, maar door onvoldoende te voorzien in logging van het gebruik van toegangsrechten en geen controle uit te voeren op de gegevens die uit de logging werden verkregen, gaven de instellingen hieraan in de praktijk geen invulling.

Bij die instellingen bleken intensieve verbetertrajecten nodig om de overtredingen te beëindigen. Inmiddels heeft de Autoriteit Persoonsgegevens geconstateerd dat de door de onderzochte zorginstellingen getroffen maatregelen voldoen aan de wettelijke vereisten.

Wettelijke vereisten
Duidelijk is geworden dat de geconstateerde tekortkomingen zich niet beperken tot de onderzochte zorginstellingen, maar zich ook bij veel andere zorginstellingen voordoen. Mogelijk ook bij uw instelling. Wettelijke bepalingen verplichten zorgverleners tot vertrouwelijkheid en zorgvuldigheid. Beschamen daarvan, door een of meerdere zorgverleners, kan een weerslag hebben niet alleen op de reputatie van de betrokken zorgverleners maar op de gehele sector. Negatieve gevolgen zijn veelal niet beperkt tot de patiënt van wie gegevens breder dan strikt noodzakelijk bekend zijn geraakt, maar kunnen het vertrouwen van alle patiënten schokken en uiteindelijk goede, toegankelijke hulpverlening belemmeren.

Om het vertrouwen van uw patiënten in een zorgvuldige omgang met hun medische gegevens te behouden, is het van belang dat u ook voor uw instelling regelmatig een analyse maakt van de situatie en beoordeelt of autorisaties, logging en controle op de logging up-to-date en in overeenstemming met de wettelijke vereisten zijn.

Een zorginstelling moet aan de vereisten van de Wbp voldoen, is de hoeder van de geheimhoudingsplicht en kan patiënten niet aan het risico blootstellen dat onbevoegden medische gegevens inzien. Natuurlijk moeten die gegevens altijd toegankelijk zijn voor medewerkers die betrokken zijn bij de behandeling of zorg voor een specifieke patiënt. Maar tegelijkertijd is vanzelfsprekend dat die gegevens niet in handen komen van medewerkers die niets te maken hebben met die specifieke patiënt. Maatregelen op het gebied van autorisaties, logging en controle van logging zijn daarvoor onontbeerlijk.

Aandacht Raad van Bestuur
In de onderzochte zorginstellingen is uiteindelijk gebleken dat kwaliteit, veiligheid en privacy van patiënten goed met elkaar in evenwicht te brengen zijn. Het slechten van vooroordelen ('privacybescherming gaat ten koste van de patiëntveiligheid') en het behoud van draagvlak bij medewerkers van zorginstellingen ('privacybescherming is nodig en niet alleen maar lastig') vergt echter wel doorlopende aandacht en support, met name ook vanuit de Raad van Bestuur. Een leidende rol van de Raad van Bestuur is ook nodig bij het bepalen van de vereisten waaraan bij de aanschaf en/of updating van ICT-voorzieningen moet worden voldaan. Het is onvoldoende om te vertrouwen op mededelingen van de leverancier, bijvoorbeeld dat het systeem 'Wbp-proof' is.

Uw leidinggevende rol zal bovendien ook vanuit het oogpunt van effectiviteit en ter voorkoming van reputatieschade van belang zijn. Alleen door waar nodig voortvarend verbetertrajecten in gang te zetten kan naleving van de Wbp en Wgbo worden gerealiseerd.

Om u behulpzaam te zijn bij de ijking van uw beleid en praktijk aan de vereisten van artikel 13 Wbp , verwijs ik naar het door ons in 2013 gepubliceerde onderzoeksrapport en de sindsdien door brancheorganisaties ontwikkelde handreikingen (zie daarvoor de websites van de Nederlandse Vereniging van Ziekenhuizen, GGZ Nederland en de Vereniging Huisartsenposten Nederland). Ik voeg ook een weerslag toe van de aan onderzochte zorginstellingen gegeven eindtaxaties van verbetertrajecten en –maatregelen bij beëindiging van het onderzoek.

Datum
15 februari 2016

Ons kenmerk
z2012-00179

Ik vertrouw erop dat u zo nodig binnen uw instelling de noodzakelijke verbetertrajecten in gang zult zetten. Ik wijs in dit verband ook op de meldplicht datalekken die sinds 1 januari van dit jaar van kracht is. De Autoriteit Persoonsgegevens kan, als zij signalen krijgt over onbevoegde toegang tot patiëntgegevens overigens altijd besluiten nieuw onderzoek te doen.

Hoogachtend ,

Autoriteit Persoonsgegevens,
Voor deze,

mr. W.B.M. Tomesen
Vice-voorzitter