Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

27 529 Informatie- en Communicatietechnologie (ICT) in de Zorg

Nr. 124 **BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 18 juni 2013

In de afgelopen periode heeft het College bescherming persoonsgegevens (College) onderzoek gedaan bij zorginstellingen naar maatregelen getroffen in verband met toegang tot digitale patiëntendossiers in zorginstellingen. Het rapport is vandaag aangeboden (zie bijlage[1]).

Het College heeft aanleiding gezien te onderzoeken op welke manier de zorginstellingen de toegang van medewerkers tot digitale patiëntendossiers hebben geregeld en of op dit punt de beveiliging van persoonsgegevens in de zorgsector op het door de Wet bescherming persoonsgegevens vereiste passende niveau is. Het College heeft aanbevolen om ter bepaling van hetgeen in een concrete situatie «passend» is, gebruik te maken van algemeen geaccepteerde beveiligingsstandaarden. Voor de informatiebeveiliging in de zorg zijn normen beschikbaar van het Nederlands Normalisatie-instituut, te weten NEN-normen. NEN 7510 is algemeen toepasbaar op informatiebeveiliging in de zorg en NEN 7.513 handelt volledig over de logging, het vastleggen van acties op elektronische patiëntendossiers, zodat het mogelijk is de rechtmatigheid van de toegang tot dossiers te controleren. Zoals ik heb opgenomen in de toelichting bij het wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens, zal naar deze NEN-normen bij algemene maatregel van bestuur dwingend worden verwezen.[2]

De bevindingen van het onderzoek van het College naar toegangsbeveiliging van medische gegevens binnen de zorgsector vallen uiteen in twee onderwerpen:
– De wijze van autoriseren: hoe bepaalt de verantwoordelijke voor de zorginstelling wie wanneer toegang tot welke patiëntendossiers krijgt?

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer
[2] Kamerstuk 33 509, nr. 3.

kst-27529-124
ISSN 0921 - 7371
's-Gravenhage 2013

– Logging en controle: houdt de verantwoordelijke voor de zorginstelling bij wie wanneer een dossier raadpleegt en wordt dit gecontroleerd?

Ik heb met zorg kennis genomen van de bevindingen en conclusies van het College aangaande het maatschappelijk belangrijke thema van privacybescherming van patiënten.

Het College heeft geconstateerd dat er binnen de onderzochte zorginstellingen tekortkomingen zijn op het gebied van autorisatie van zorgmedewerkers, autorisatie van administratief-ondersteunende medewerkers, logging en controle van logging.

Dit betekent dat de betreffende zorginstellingen niet voldoen aan hetgeen hierover op grond van NEN 7510 en NEN 7513 is aangegeven en dat zij daarom niet voldoen aan de wettelijke vereisten met betrekking tot toegangsverlening voor medewerkers tot patiëntendossiers en de controle op die toegang.

Volgens het rapport voldoet de autorisatie niet in die zin dat met technologische middelen wel de toegangsrechten van medewerkers afhankelijk van functie *of* functie en werkcontext worden beperkt, maar dat niet door middel van technologische middelen wordt afgedwongen dat alleen toegang wordt verleend als er daadwerkelijk sprake is van een behandelrelatie met een specifieke patiënt. Hiervoor zijn de medewerkers zelf verantwoordelijk. Dit wordt in communicatie over en in beleidsdocumenten, zoals gedragscodes en autorisatiebeleid, bij hen onder de aandacht gebracht.
Wat betreft logging en controle heeft het College geconstateerd dat niet in alle onderzochte zorginstellingen van alle acties op patiëntgegevens logging plaatsvindt en dat niet is voorzien in een systematische, consequente controle van alle logging.
Volgens de onderzochte zorginstellingen ligt de oorzaak waarom niet voldaan kan worden aan de wettelijke vereisten, met name in technologische beperkingen. Deze beperkingen zijn gelegen in het ontbreken van technologische mogelijkheden, dan wel technologische ondersteuning, maar ook in beperkingen van de software zelf. Ook het ontbreken van menskracht en financiële beperkingen worden door de zorginstellingen genoemd.
Het College concludeert echter dat door de zorginstellingen geen valide redenen in de sfeer van stand der techniek, patiëntveiligheid en kosten van tenuitvoerlegging gegeven zijn om niet aan de wettelijke vereisten te voldoen.

De besturen van de onderzochte zorginstellingen zijn verantwoordelijk voor de uitwerking van de taak om verantwoorde, veilige zorg te verlenen en daarbij de persoonlijke levenssfeer van patiënten te beschermen. Zij hebben afspraken gemaakt met het College om de wijze van toegangsverlening voor medewerkers tot patiëntendossiers en de controle op die toegang te verbeteren. Het College zal erop toezien dat in deze door de zorginstellingen voortvarend gehandeld wordt en zal zo nodig handhavend optreden.
Het feit dat de onderzochte zorginstellingen afspraken hebben gemaakt met het College, toont mijns inziens aan dat deze instellingen zich inmiddels bewust zijn van hun verantwoordelijkheid. In dit kader benadruk ik ook het belang van het streven van het College om met dit rapport ook de niet onderzochte instellingen te bereiken zodat ook zij zich verantwoordelijk tonen voor het realiseren van adequate bescherming van persoonsgegevens en daartoe de benodigde maatregelen en voorzieningen treffen.

Zoals gezegd zullen bij algemene maatregel van bestuur eisen worden gesteld aan de (hoge) mate van beveiliging van de toegang tot gegevens. Dit betekent dat gebruikte informatiesystemen aan die eisen moeten voldoen, zodat de patiënt erop kan en mag vertrouwen dat zorgvuldig wordt omgegaan met de (privacygevoelige) gegevens in het patiëntendossier. En dat achteraf altijd transparant kan worden gecontroleerd wie er op welk moment toegang heeft gehad tot de gegevens.

Deze eisen zijn en worden tijdig gecommuniceerd, zodat iedere instelling zich daarop ook kan voorbereiden. Het is van groot belang dat instellingen dit rapport serieus nemen en zonodig hun procedures en techniek daarop aanpassen.

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