Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2008–2009

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

Nr. 43

BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 13 november 2008

In 2007 hebben de Inspectie voor de Gezondheidszorg (IGZ) en het College Bescherming Persoonsgegevens (CBP) een onderzoek uitgevoerd naar de informatiebeveiliging in zieken-huizen. Hierbij bied ik u het rapport *Informatiebeveiliging ziekenhuizen voldoet niet aan de norm* aan[1] en geef ik een reactie op de conclusies en aanbevelingen.

Aanleiding voor het onderzoek

In 2004 heeft de IGZ het rapport *ICT in ziekenhuizen* gepubliceerd. Belangrijke conclusie was destijds dat de norm NEN 7510 geïmplementeerd diende te worden. De norm NEN 7510 gaat over informatiebeveiliging binnen de zorg. Dat wil zeggen: het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die nodig is om patiënten verantwoorde zorg te kunnen bieden. In het onderzoek dat ik u vandaag aanbied, is een beeld verkregen van de stand van zaken van de implementatie van de norm NEN 7510 in ziekenhuizen. Voor het onderzoek zijn 20 ziekenhuizen bezocht. Er is juist gekozen voor ziekenhuizen omdat dit de meest complexe gezondheidszorginstellingen zijn met de grootste gezondheidsrisico's voor de patiënt.

Conclusies en aanbevelingen

De belangrijkste conclusie van de IGZ en het CBP is dat de informatiebeveiliging van zieken-huizen nog tekort schiet. Het besef dat informatiebeveiliging staat of valt met de organisatie van de informatiebeveiliging en het gedrag van medewerkers, en dat daarvoor een cultuur-verandering nodig is, is onvoldoende aanwezig. Informatiebeveiliging wordt veelal ad hoc in de praktijk geregeld, niet gebaseerd op een systematisch uitgewerkt beleid. Ik ben het met de IGZ en het CBP eens dat dit niet acceptabel is.

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

KST124486
0809tkkst27529-43
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2008

Aan alle onderzochte ziekenhuizen is gevraagd uiterlijk 15 oktober 2008 een plan van aan-pak aan te leveren waarin duidelijk wordt wat het ziekenhuis onderneemt om volledig aan de norm NEN 7510 te voldoen en op welke termijn dit zal zijn gerealiseerd. Inmiddels hebben alle ziekenhuizen een plan van aanpak bij de IGZ aangeleverd. Ook alle andere ziekenhuizen moet een dergelijk plan van aanpak uiterlijk 1 februari 2009 aanleveren. Tot slot moeten alle ziekenhuizen in 2010 een externe audit laten uitvoeren op de implementatie van de norm NEN 7510. Bij onvoldoende planvorming zal de IGZ handhavingsmaatregelen inzetten.

Ik ben blij met de aandacht van de IGZ en het CBP voor informatiebeveiliging in de zorg. De zorg is een zeer informatie intensieve sector. Ook neemt elektronische informatie-uitwis-seling in de zorg een grote vlucht. Het gaat daarbij zowel om uitwisseling van patiënt-gegevens binnen het ziekenhuis als om uitwisseling via lokale en regionale netwerken. De informatie-beveiliging van zowel papieren als elektronische dossiers dient daarbij uiteraard op orde te zijn.

Ook de invoering van het landelijk elektronisch patiëntendossier (EPD) vergt een adequate informatiebeveiliging. De beveiliging van het landelijk EPD is ook vorige week aan de orde gekomen in het spoed Algemeen Overleg. De beveiliging van het EPD-systeem voldoet aan de hoogste normen. Gezien de gevoeligheid van de uit te wisselen gegevens zijn vanaf het begin zeer hoge eisen gesteld aan de beveiliging van de gehele EPD-keten. Het landelijk schakelpunt (LSP), een volledig gesloten systeem dat – anders dan bij de recente aandacht-trekkende gebeurtenis in de Verenigde Staten waarbij patiëntengegevens in verkeerde handen terechtkwamen – niet via het openbare internet bereikbaar is, voldoet aan zeer hoge beveiligingseisen. Deze hoge eisen gelden ook voor de zorginformatiesystemen van zieken-huizen die aansluiten op het landelijk schakelpunt ten behoeve van het kunnen inzien van het elektronisch medicatiedossier via het LSP. Bovendien geldt dat ziekenhuizen bij gebruik van het BSN – een voorwaarde om te kunnen aansluiten op het LSP – reeds op grond van het besluit BSN in de zorg wettelijk moeten voldoen aan de NEN 7510. Voordat de ziekenhuizen kunnen aansluiten op het LSP, moet aan de volgende voorwaarden zijn voldaan:

1. Beschikken over een gekwalificeerd ziekenhuisinformatiesysteem. Het Nationaal ICT Instituut in de Zorg (Nictiz) verzorgt deze kwalificatie.
2. GBZ-verklaring. Het voldoen aan een passend en adequaat niveau van informatiebeveiliging is één van de eisen die wordt gesteld aan het goed beheerd zorgsysteem (GBZ) van de zorgaanbieder. Het hebben van een GBZ is een voorwaarde voor de zorgaanbieder om te kunnen aansluiten op het landelijk schakelpunt. Hierdoor is een waarborg ingebouwd die moet voorkomen dat niet adequaat beveiligde ziekenhuizen aansluiten op het landelijk schakelpunt.

Voorafgaand aan de aansluiting wordt de veilige werking in technische testen door Nictiz getoetst. De adequate werking kan in een ketentest tussen zorgaanbieders worden getest, hiervoor zijn separate omgevingen beschikbaar.
Een zorgaanbieder kan alleen toegang krijgen met een persoonlijke UZI-pas (een elektronisch paspoort met persoonlijke inlogcode) die face-toface is uitgegeven. Bovendien wordt permanent vastgelegd wie de gegevens inziet (logging).

Invoering van het landelijk elektronisch patiëntendossier zal mijns inziens gaan bijdragen aan extra aandacht voor informatiebeveiliging en een versnelde opschaling van het niveau van informatiebeveiliging van ziekenhuizen.

De minister van Volksgezondheid, Welzijn en Sport,
A. Klink