

De praktijk van NEN 7510

Jaap van der Wel (jvdwel@comfort-ia.nl) is directeur van Comfort-IA en lid van de norm-commissie voor Informatiebeveiliging in de zorg. Publicatie is onder persoonlijke titel.

De Inspectie voor de Gezondheidszorg constateerde na een onderzoek bij twintig ziekenhuizen dat: '(...) ziekenhuizen op dit moment onvoldoende aandacht schenken aan de risico's die de toepassing van ICT met zich meebrengt. De patiënt loopt hierdoor een reële kans op gevaar. Er kunnen bijvoorbeeld belangrijke gegevens verloren gaan, gegevens kunnen op de verkeerde plaats terechtkomen en behandelingen kunnen verstoord raken door niet goed functionerende apparatuur'¹. Recentelijk bleek weer hoe juist deze opmerking is: de poli van het Spaarne Ziekenhuis moest twee dagen de deuren sluiten omdat een computervirus het bedrijfsnetwerk had platgelegd. Ook de eerstelijnszorg kampt met problemen om de informatievoorziening stabiel te laten functioneren. Bij tal van HAP's en HOED's traden problemen op bij de overgang van het oude Elias systeem naar iets nieuws. Zo gingen brieven uit naar reeds overleden patiënten of werden historische gegevens niet goed overgenomen.

Wie is aan zet?

Directies van zorginstellingen en praktijkhouders in de eerste lijn realiseren zich de risico's gewoonlijk wel maar weten er niet altijd goed raad mee. Bij de zorginstellingen waar zich dit voordoet, moet het hoofd Informatievoorziening dan de problemen maar zien te voorkomen, met af en toe een bijdrage van de huisjurist over patiëntenprivacy. En in de eerste lijn geven de klanten hun ICT-leverancier onder uit de zak als er iets mis gaat, waarop de leverancier met wat gratis dienstverlening weer enige compensatie geeft.

Nu ICT steeds belangrijker wordt, gaat dit zo niet langer. De risico's moeten worden teruggedrongen. Daarvoor is teamwork nodig. In de zorginstellingen door het managementteam. In de eerste lijn door de gebruikers en alle betrokken ICT-leveranciers. De nieuwe norm voor Informatiebeveiliging in de zorg, NEN 7510, concretiseert dit. De norm maakt overigens ook duidelijk dat een professionele opzet van informatievoorziening een complexe



aangelegenheid is geworden. Zo complex dat een individuele praktijkhouder voor de keuze staat om ofwel het meeste uit te besteden ofwel studie te maken van netwerken en computers, om vervolgens nog veel tijd kwijt te zijn met de uitvoering.

Inventariseren als eerste stap

De norm bestaat uit een checklist die, afhankelijk van de manier van tellen, tussen de 125 en 200 punten bevat. Dat is teveel voor behandeling in dit artikel. Daarom beperken we ons tot de 'tien belangrijkste maatregelen', zoals die ook in de bijlagen van de norm worden vermeld (zie kader). Om te beginnen kan de checklist – de volledige

Dossiervoering en geheimhoudingsplicht vereisen nou eenmaal beveiliging van medische gegevens. Goed dat deze norm naadloos ingepast kan worden in het NIAZ en HKZ kwaliteitssysteem. Trouwens wel evenveel werk!

Hein van der Reijden, directeur patiëntenzorg Dianet Dialysecentra, namens de KNMG lid van NEN Normcommissie 7510



lijst of de tien punten van het kader – gebruikt worden om de eigen organisatie na te lopen. Managers van grotere organisaties, zoals ziekenhuizen, verpleegtehuizen, revalidatie-instellingen en instellingen voor thuiszorg, zouden dat ook met enige regelmaat moeten doen. Daarnaast is de checklist geschikt als toets van het samenwerkingsverband van kleinere zorginstellingen met ICT leveranciers. Ieder punt van de norm moet ergens in dit verband belegd zijn. In de praktijk vallen echter tal van punten tussen wal en schip. Vooral in de eerstelijnszorg dreigt dit risico. Daar kunnen meerdere ICT-leveranciers namelijk een complexe keten vormen: één voor ASP-diensten, een ander voor de huisartsensoftware, nog één voor de hardware en één voor datacentrum en netwerkdiensten en voor beveiligde opstellingen. Resultaat van de inventarisatie is niet alleen dat risico's zichtbaar worden, maar óók dat de waarde zichtbaar wordt van de goed geregelde zaken. Dat laatste is belangrijk, vooral waar men de specialistische kennis mist om zelf die waarde vast te stellen maar intussen wel aanhikt tegen een hoge prijs – bijvoorbeeld in de eerste lijn.

Met de genoemde tien punten lijst heeft men binnen de kortst mogelijke tijd een eerste indruk van de controle over de informatievoorziening en de nog te verbeteren punten. Bent u tevreden over uw score? Durft u te voorspellen wat de uitkomst is van een check op uw organisatie met de volledige lijst? Zijn de belangrijke beveiligingsmaatregelen getroffen? Krijgt het hoofd Informatievoorziening wel voldoende budget en steun van het managementteam? Volgen de huisartsen wel voldoende de aangeboden cursussen van de softwarefabrikant of bellen ze in plaats daarvan de helpdesk plat?

Nalopen van de organisatie met de volledige checklist hoeft niet veel werk te zijn als goed gebruik gemaakt wordt van de aanwezige kennis en ervaring. Wie kent de sterke en zwakke plekken beter dan de medewerkers van de eigen organisatie? Een objectieve kijk van buiten is daarbij wel wenselijk want wie heeft er beter geleerd om zijn mond maar te houden over steeds terugkerende problemen dan de medewerkers van de eigen organisatie? En wie heeft er beter geleerd om medewerkers-met-stokpaardjes maar een beetje te laten voor wat ze zijn dan het eigen management?

Vervolgens: beleid

Nadat de risico's zichtbaar zijn geworden, kan het management van de zorginstelling het beleid vaststellen waarin prioriteiten worden bepaald, taken verdeeld en budgetten toegewezen. Prioriteiten hangen af van de gevolgen van falende informatievoorziening en de risico's dat dit gebeurt. Voor wat betreft de taken is de ene keer het hoofd Informatievoorziening aan zet om, bijvoorbeeld, het systeembeheer te verbeteren of om, samen met een jurist, ervoor te zorgen dat de uitbestedingscontracten aan de Wet Bescherming Persoonsgegevens gaan voldoen. Maar in andere gevallen is de directie aan zet, bijvoorbeeld om problemen op te lossen die ontstaan door slecht samenspel tussen de afdeling informatievoorziening, medici en verplegend personeel. Slecht samenspel uit zich bijvoorbeeld in gemopper over de ingewikkelde aanlogprocedures (de ontwerper daarvan: het moest toch veilig zijn?) waarvan het lijnmanagement nooit heeft gezegd hóe veilig die moesten zijn.

Beveiliging kost tijd en geld. Dat is niet het gevolg van de norm voor informatiebeveiliging in de zorg, die is slechts een hulpmiddel. De investeringen zijn nodig om risico's te beheersen zoals die voor patiëntenzorg, imagooverlies en het omzetverlies dat daarop volgt als de potentiële klandizie over problemen leest in een Elsevier-test en vervolgens wegblijft. Draagvlak is belangrijk en wordt onderhouden met quick wins. Kosten worden beheerst door de invoeringsmomenten van maatregelen ook op langere termijn te plannen. Sommige maatregelen kunnen direct worden ingevoerd; voorbeelden zijn het invoeren van een beveiligingsbeleid, het instellen van een beveiligingsorganisatie en het treffen van personele maatregelen (de hoofdstukken 5, 6 en 8 van de norm voor Informatiebeveiliging in de Zorg). Een ander deel kan alleen worden gerealiseerd als het gebruikte softwarepakket wordt aangepast. Deze aanpassingen moeten als wens worden ingebracht in de gebruikersgroep en door de leverancier worden opgenomen in de releaseplanning. Een voorbeeld vormen de functies voor toegangsbeveiliging, die in tal van softwarepakketten tekort schieten². Formeel moet de toegangsbeveiliging voldoen aan de wettelijke regeling voor het medisch beroepsgeheim. Maar in de praktijk is dat problematisch omdat de huidige wetgeving nog uitgaat van het papiertijd-perk³. Wellicht brengt de invoering van de Landelijke Verwijsindex ook op dit punt verbetering.

Al met al blijkt de lijst van noodzakelijke en wenselijke maatregelen gewoonlijk voor jaren werk op te leveren. Informatiebeveiliging is niet een kwestie van een verbeterprojectje doen maar een proces van voortdurende verbeteringen dat gelijke tred moet houden met de toenemende automatiseringsgraad.

En dan aan de slag⁴

Bij de realisatie van de beveiligingsmaatregelen moet men het niet te mooi maken. Het kenmerk van goede informatiebeveiliging is niet de perfectie van de afzonderlijke maatregelen maar het evenwichtige samenspel. Een kwestie van geld zijn de technologische maatregelen. Een grote uitdaging is ervoor zorgen dat iedereen verantwoord omgaat met die technologie.

1 Inspectie voor de Gezondheidszorg, ICT in de ziekenhuizen, Een inventariserend onderzoek bij twintig ziekenhuizen, uitgevoerd najaar 2003, den Haag augustus 2004, zie www.igz.nl

2 Zie Jaap van der Wel, Nanne Homma, *Gegevensbeveiliging aan alle kanten lek*, Automatisering Gids 5 september 2003, te vinden op www.comfortia.nl/ag1.pdf

3 Zie Jaap van der Wel, *Spoort de medische praktijk nog met de wettelijke regeling voor het beroepsgeheim?*, Journaal Privacy in de Gezondheidszorg van 18 april 2005, zie www.comfort-ia.nl/wgbo.pdf

4 Zie www.nen7510.org voor praktische voorbeelden

5 De vragen zijn afkomstig uit bijlage B die is opgenomen in de drie toetsbaar voorschriften NEN7510 waarvan de ontwerpnorm op 18 mei 2005 is gepubliceerd (het 'groentje' door het Nederlands Normalisatie-instituut (NEN))

Afkortingen

ASP: Application Service Provider, een

leverancier die rekencentrumdiensten levert.

HAP: Huisartsen Post, samenwerkingsverband rondom vervangings-/weekenddiensten.

HOED: Huisarts Onder Eén Dak, samenwerkingsverband rondom gezamenlijke faciliteiten zoals huisvesting

NEN: Nederlands Normalisatie-instituut

We moeten natuurlijk wél uiterst voorzichtig omgaan met vertrouwelijke, medische informatie van mensen. De veiligheid met betrekking tot het inzien van de gegevens dient goed geregeld te zijn.

Hans Hoogervorst, Minister van VWS, (uitgesproken op het Medisch-Informatica Congres)



Geef uw informatiebeveiliging een rapportcijfer!⁵

Tel één punt voor ieder antwoord dat met ja beantwoord wordt. Nul punten ingeval van nee, of onbekend of 'lossen we op als we tegen een probleem oplopen'. Een aftrekpunt als vraag 10 met nee wordt beantwoord.

Vraag	Directies van zorginstellingen	Directies van zorginstellingen
	<i>Voorbeeld: Ziekenhuis met twee locaties</i>	<i>Voorbeeld: HAP waarbinnen de huisartsen gezamenlijk de huisartsen software hebben geselecteerd</i>
1 Beleidsdocument voor informatiebeveiliging	Zijn zwakke plekken bekend? Is een selectie gemaakt om het komende jaar aan te pakken?	Voorbeeld: Analyse van de rapportage van de beveiligingsincidenten van vraag 10/Bundeling van de ervaring van huisartsen met hun gezamenlijke leverancier. Met selectie van actiepunten voor het komend jaar.
2 Toewijzing en vastlegging van verantwoordelijkheden voor informatiebeveiliging	Bijvoorbeeld in de vorm van inventarisatie van de taken van het lijnmanagement, de afdeling Informatievoorziening, de directie en gezamenlijke goedkeuring.	Zijn checklistitems van NEN7510 verdeeld over de con-tractpartners en in contracten (of nadere brieven) opgenomen?
3 Bewustwording, opleiding en training voor informatiebeveiliging	Worden de ervaringen van nieuwkomers na enkele maanden geïnventariseerd, lettend op snelheid van inwerken, opvallende punten, punten die beter zouden moeten?	1) Is er een opleiding voor het gebruik van het pakket (inclusief beveiliging zoals backup procedures, beveiliging tegen diefstal e.d.), 2) Volgen huisartsen die opleiding?
4 Maatregelen tegen kwaadaardige programmatuur	Virusscanner, firewall, mogelijkheden van medewerkers om zelf software te installeren (verbiedt bijvoorbeeld 'handige programmaatjes' van derden die via internet contact leggen met de buitenwereld)	Virusscanner, firewall, wie neemt dit voor zijn rekening (gewoonlijk de ASP leverancier)
5 Ontwikkelen en implementeren van continuïteitsvoorzieningen en -plannen	Is er een dergelijk plan? Wordt er jaarlijks/twee jaarlijks wel eens een oefening gehouden?	Welke afspraken zijn er met de ASP leverancier? Heeft u zich laten rondleiden langs de apparatuur en voor de hand liggende vragen gesteld?
6 Intellectueel eigendom	Worden bijvoorbeeld alle plekken van kantoor-automatisering afgerekend?	Worden alle installaties van de huisartsensoftware afgerekend met de pakketleverancier?
7 Beveiliging van bedrijfsdocumenten (Voorbeelden zijn medische dossiers, declaraties e.d.)	Blijven deze toegankelijk, worden deze conform de wettelijke bewaartermijn (nu voorlopig 15 jaar) vernietigd?	Extra aandachtspunt is de overgang van een oud naar een nieuw huisartsensysteem: worden alle gegevens meegeconverteerd, zo niet, blijven de gegevens uit het oude systeem gemakkelijk beschikbaar de komende jaren?
8 Bescherming van persoonsgegevens	Worden de goede gegevens in de medische registratie vastgelegd (niet te veel, niet te weinig, zie het groene boekje van de KNMG)	
9 Naleving beveiligingsbeleid	Wordt de naleving af en toe geëvalueerd en onafhankelijk gecontroleerd? (zien is geloven)	Testen is een notoir probleem in de eerste lijn omdat het teveel werk kost om dat grondig te doen.
10 Het rapporteren van beveiligingsincidenten	Is er een overzicht van problemen ('incidentenregistratie')	Is er een overzicht van problemen, per huisarts bijgehouden (spreadsheet, nog mooier: storingsadministratie van de ASP leverancier)