STAATSTOEZICHT OP DE VOLKSGEZONDHEID
INSPECTIE VOOR DE GEZONDHEIDSZORG

COLLEGE BESCHERMING PERSOONSGEGEVENS

Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm

Rapportage van een onderzoek in 2007 door het College bescherming persoonsgegevens en de Inspectie voor de Gezondheidszorg naar de informatiebeveiliging in 20 ziekenhuizen.

Den Haag, november 2008

Aan de minister van Volksgezondheid, Welzijn en Sport,

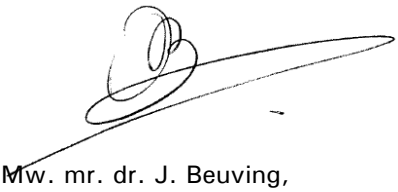
De toepassing van ICT in de zorg staat op het punt belangrijke vorderingen te maken. Zo zullen het landelijk elektronisch medicatiedossier (EMD) en het waarneemdossier huisartsen (WDH) binnenkort worden geïmplementeerd. In veel gezondheidszorg-instellingen wordt de toepassing van ICT enorm uitgebreid. Al deze toepassingen en uitbreidingen dienen vanzelfsprekend om de kwaliteit van de hulpverlening aan de patiënt te verbeteren. Toch kleven aan die toepassing van ICT risico's. Risico's die juist de veiligheid van de zorg kunnen bedreigen. Dat mag natuurlijk niet het geval zijn. Wanneer ICT toegepast wordt, moet het veilig voor de patiënt zijn. Daarnaast brengt de toepassing van ICT risico's voor de privacy van de patiënt met zich, terwijl het hier gaat om gevoelige gegevens die juist extra bescherming verdienen.
Het College Bescherming Persoonsgegevens (CBP) en de Inspectie voor de Gezondheidszorg (IGZ) hebben vanwege die risico's een onderzoek gedaan naar de wijze waarop ziekenhuizen in Nederland met de beveiliging van hun informatie en dus met de toepassing van ICT omgaan. Er is voor ziekenhuizen gekozen omdat het risico voor de veiligheid van de patiënt bij een onveilige toepassing van ICT in ziekenhuizen het grootst is. Vanuit het oogpunt van persoonsgegevensbescherming is van belang dat bij ziekenhuizen veelal sprake zal zijn van zeer omvangrijke verwerking van gevoelige persoonsgegevens. Vooral is nagegaan of ziekenhuizen zich bewust zijn van de risico's en voldoende maatregelen nemen om de kans dat er wat misgaat, zo klein mogelijk te maken.

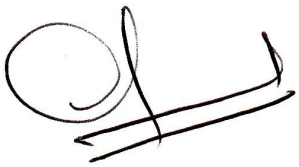
Het risicobewustzijn bij ziekenhuizen voor wat betreft de kans dat er met de verwerking van informatie iets misgaat, is maar zeer beperkt aanwezig. Zij nemen dan ook in het merendeel onvoldoende maatregelen om de beveiliging van hun informatie-verwerking op een voldoende niveau te krijgen. Dat is niet goed en zal moeten veranderen. Dat moet veranderen omdat de zorg veilig moet zijn en de privacy van de patiënt gewaarborgd moet zijn, maar ook omdat de verandering een voorwaarde is om aan te sluiten op het Landelijk Schakelpunt en zodoende op het landelijk Elektronisch Patiëntendossier (EPD). Het niet voldoen aan de NEN 7510 zou de realisatie van het landelijk EPD frustreren.
Met dit rapport maken het CBP en de IGZ het voorgaande duidelijk. Het CBP en de IGZ hebben van de onderzochte ziekenhuizen verwacht dat er voor 15 oktober een Plan van Aanpak is opgesteld waarin duidelijk wordt wat het ziekenhuis onderneemt om volledig aan de NEN 7510 norm te voldoen. Indien het CBP en de IGZ concluderen dat de onderzochte ziekenhuizen onvoldoende voortvarend werk maken van het verbeteren van de informatiebeveiliging, zullen de IGZ en het CBP overwegen bij de betreffende ziekenhuizen handhavend op te treden.

De inspectie zal niet alleen de bezochte maar ook de overige ziekenhuizen vragen een plan van aanpak op te stellen en dit beoordelen. Uit dit plan van aanpak moet blijken

hoe deze ziekenhuizen aan de NEN 7510 norm gaan voldoen. In 2010 moeten alle ziekenhuizen in Nederland aan de inspectie aan de hand van de resultaten van een externe audit aantonen dat zij voldoen aan een voldoende mate van informatie-beveiliging.

Hoogachtend,





Mw. mr. dr. J. Beuving,
Collegelid College Bescherming Persoonsgegevens

Prof. dr. G. van der Wal,
Inspecteur-generaal voor de Gezondheidszorg

Den Haag, november 2008

Samenvatting

Naar aanleiding van de resultaten van het door de IGZ in 2004 gepubliceerde rapport *ICT in ziekenhuizen* is opnieuw onderzoek verricht naar de stand van de informatiebeveiliging in ziekenhuizen, mede vanwege de op handen zijnde invoering van delen van het Elektronisch Patiëntendossier en de bijbehorende toename van het gebruik van ICT bij de directe patiëntenzorg. Het onderzoek is nu uitgevoerd door de IGZ en het CBP onder twintig ziekenhuizen door middel van gesprekken met een vertegenwoordiger van de Raad van Bestuur, de afdeling ICT en de medische staf.

Het doel van het onderzoek was het verkrijgen van een beeld van de stand van zaken van de implementatie van de NEN 7510 norm bij ziekenhuizen in het algemeen. Tevens werd de invulling van de informatiebeveiliging in de gekozen ziekenhuizen onderzocht en gecontroleerd of de getroffen maatregelen voldoen aan de relevante wet- en regelgeving.

Uit het onderzoek blijkt dat er vooral op technisch gebied in vergelijking met vier jaar geleden veel is verbeterd. Echter, zowel de leiding als de medewerkers zijn zich nog steeds onvoldoende bewust van de risico's die gebruik van ICT in ziekenhuizen met zich meebrengt. Over het algemeen wordt bewust omgegaan met het openstellen van het netwerk voor andere zorginstellingen. Wat betreft de NEN 7510 norm blijkt dat de meeste ziekenhuizen nog niet aan deze norm voldoen. Zo is informatiebeveiliging bijvoorbeeld nog te weinig omgezet naar uitgewerkt beleid en wordt veel 'in de praktijk' geregeld. Een andere belangrijke bevinding is het ontbreken van bewustzijn bij medewerkers van het belang van informatiebeveiliging. Informatiebeveiliging staat of valt met het gedrag van medewerkers en effectieve controle op gedrag ontbreekt nog te vaak.

Van de twintig onderzochte ziekenhuizen blijkt bij negen ziekenhuizen dat er geen sprake is van een passend beveiligingsniveau zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens (WBP), en dat evenmin is voldaan aan de voorwaarden om verantwoorde zorg te leveren zoals bedoeld in artikel 2 van de Kwaliteitswet zorginstellingen (KWZ). Bij vijf is sprake van onvoldoende passend beveiligingsniveau en bij zes ziekenhuizen is er nog niet in voldoende mate sprake van passend beveiligingsniveau.
De twintig onderzochte ziekenhuizen zullen duidelijk moeten maken hoe zij wel aan een passend beveiligingsniveau gaan voldoen. Zij moeten aan het CBP en de IGZ een plan van aanpak leveren waaruit blijkt hoe zij dat gaan bereiken en op welke termijn zij dat bereikt zullen hebben. Indien de inhoud van het plan van aanpak (of het geheel uitblijven van een plan van aanpak) daartoe aanleiding geeft, zal handhavend worden opgetreden.

De inspectie zal de overige ziekenhuizen in Nederland ook een plan van aanpak op laten stellen. Uit dit plan van aanpak moet blijken hoe deze ziekenhuizen aan de NEN 7510 norm gaan voldoen. Daarnaast zullen alle ziekenhuizen in 2010 aan de inspectie de resultaten moeten overleggen van een extern uitgevoerde audit, zoals in de NEN 7510 norm is bedoeld, waaruit blijkt wat het niveau van informatiebeveiliging op dat moment is. Zonodig zal op grond van het plan van aanpak een eerdere beoordeling door de inspectie plaatsvinden en handhavend worden opgetreden. Dat betekent dat bij onvoldoende planvorming om aan de totale NEN 7510 norm te voldoen, handhavingmaatregelen ingezet zullen worden.

Inhoudsopgave

1 Inleiding

Aanleiding onderzoek

In 2004 is het IGZ-rapport *ICT in ziekenhuizen* gepubliceerd. Dat betrof de rapportage van een IGZ-onderzoek naar de stand van zaken rond de veiligheid van de toepassing van ICT in ziekenhuizen. De conclusie was dat er veel mankeerde aan die veiligheid en dat met name de NEN 7510 norm geïmplementeerd moest worden. De IGZ kondigde in het rapport een follow-up aan.
Er zijn meerdere signalen dat het nog steeds slecht gesteld is met de implementatie van de NEN 7510 norm en daarmee met de veiligheid rond de toepassing van ICT in de zorg. Dat geldt niet alleen voor ziekenhuizen, maar ook voor andere instellingen in de zorg en zeker daar waar tussen instellingen door middel van ICT wordt samengewerkt. De NEN 7510 norm, die handelt over de informatiebeveiliging in de zorg als afgeleide van de Code voor de informatiebeveiliging, is inmiddels ruim bekend. NEN heeft ten behoeve van verschillende typen instellingen de norm nog verder verfijnd zodat deze gemakkelijker toepasbaar is. (Zie voor meer informatie over de totstandkoming van de NEN 7510 de bijlage.) Er is alle reden om bij gezondheidszorginstellingen te peilen hoe het staat met de toepassing van de NEN 7510 norm. In 2006 is immers een start gemaakt met de invoer van een landelijk medicatiedossier (EMD) en met het waarneem-dossier huisartsen (WDH). Patiënten en hulpverleners worden daardoor voor de kwaliteit van de zorg steeds meer afhankelijk van de veiligheid van de informatie en dus van de ICT. Onder de veiligheid van informatie moet dan vooral verstaan worden dat de informatie toegankelijk, oorspronkelijk en juist is en dat de beoogde hulp-verleners er datgene mee kunnen doen wat bedoeld wordt. Daarnaast moet de toegang tot de gegevens of functionaliteit beperkt zijn tot diegenen die daartoe bevoegd zijn (vertrouwelijkheid). Omdat ziekenhuizen de meest complexe gezondheidszorg-instellingen zijn met de grootste gezondheidsrisico's voor de patiënt en het onderzoek zich in 2003/2004 ook richtte op ziekenhuizen is er weer voor gekozen het onderzoek bij ziekenhuizen uit te voeren. Voor het CBP is de uitvoering van dit onderzoek bij ziekenhuizen vooral aangewezen geweest vanwege de gevoeligheid van de gegevens en de omvang van de gegevensverwerking.
Omdat informatiebeveiliging in de zorg zowel het toezichtterrein van het College Bescherming Persoonsgegevens (CBP) als de Inspectie voor de Gezondheidszorg (IGZ) betreft, is het onderzoek nu door CBP en IGZ gezamenlijk uitgevoerd conform het samenwerkingsprotocol CBP-IGZ dat tussen het CBP en de IGZ is opgesteld en onder-tekend.

Belang onderzoek

Als de informatiebeveiliging in ziekenhuizen niet goed geregeld is, kan dit gevolgen hebben voor patiënten. Onjuiste invoer, miscommunicatie tussen verschillende programma's en gebruik van verouderde coderingstabellen leiden tot onjuiste gegevens. Dit kan ernstige gevolgen hebben, zoals bij onjuiste gegevens over de bloedgroep of allergieën van een patiënt. Uitval van systemen door bijvoorbeeld stroomstoring kan leiden tot verlies van gegevens en uitval van spreekuren of operatieprogramma's. Verder kan onzorgvuldig omgaan met inloggegevens door personeel en het kraken van het ziekenhuissysteem leiden tot ongeautoriseerde toegang tot privacygevoelige gegevens van patiënten. Veilig gebruik van ICT in ziekenhuizen is dus belangrijk.

Doelstelling onderzoek

Het algemene onderzoeksdoel was het verkrijgen van een beeld van de stand van zaken van de implementatie van de NEN 7510 norm in ziekenhuizen in het algemeen. In het

onderzoek moest ook duidelijk worden welk beeld ziekenhuizen zelf hebben van de wijze en de mate waarin hun informatiebeveiliging is vormgegeven. Kennen de ziekenhuizen de risico's op het gebied van informatiebeveiliging? De IGZ en het CBP wilden specifiek weten in hoeverre ziekenhuizen aan een aantal delen van de NEN 7510 norm, die vanuit het toezicht door de IGZ en het CBP van bijzonder belang worden geacht, voldoen.

Centrale vraagstelling

- Wat is de stand van zaken van de implementatie van de NEN 7510 norm bij ziekenhuizen in het algemeen?
- Hoe is invulling van de informatiebeveiliging in de onderzochte ziekenhuizen en voldoen de getroffen maatregelen aan de wet- en regelgeving?
- Hebben de onderzochte ziekenhuizen een beeld van de wijze waarop de informatiebeveiliging vorm is gegeven en welke risico's er op dat vlak zijn?

Onderzoeksmethode

Voor dit onderzoek is bij twintig aselect gekozen ziekenhuizen (twee academische ziekenhuizen, negen grote en negen kleine ziekenhuizen, ingedeeld op basis van het ziekenhuisexploitatiebudget) getoetst in hoeverre ziekenhuizen de NEN 7510 norm hebben geïmplementeerd. Er is voor dit aantal gekozen omdat op deze manier een redelijke doorsnede van de Nederlandse ziekenhuizen onderzocht wordt. Het onderzoek is uitgevoerd door middel van gesprekken met een vertegenwoordiger van de Raad van Bestuur, het hoofd van de afdeling ICT en een medisch specialist. Zo mogelijk werd ook een Functionaris Gegevensbescherming (FG) gesproken. Tijdens deze gesprekken is gebruikgemaakt van het instrument voor Toetsing van ICT in de zorg (TICTzorg instrument). Dit instrument is ontwikkeld in samenwerking met TNO en bedoeld om te beoordelen in hoeverre zorginstellingen voldoen aan de NEN 7510 norm. Het betreft een leidraad voor een interview, aan de hand waarvan verschillende onderdelen van de NEN 7510 norm aan bod komen. De onderzoekers die het instrument hanteerden, waren een medewerker van het CBP en een inspecteur van de IGZ.

De IGZ en het CBP hebben zes onderdelen van de NEN 7510 norm gekozen als indicatoren voor de toestand van de informatiebeveiliging. De IGZ en het CBP beoordelen de mate waarin ziekenhuizen aan deze specifieke onderdelen van de norm voldoen. Het onderzoek betreft dus niet een volledige toets aan de NEN 7510 norm. Voldoen aan deze zes indicatoren wil níet zeggen dat daarmee de gehele NEN 7510 norm voldoende geïmplementeerd is.

Tijdens het onderzoek zijn de zes volgende onderwerpen uit de NEN 7510 norm aan bod gekomen:

- Organisatie.
- Externe partijen.
- Beveiligingseisen ten aanzien van personeel
- Toegangsbeveiliging.
- Naleving wetgeving.
- Beveiligingsincidenten.

Per onderwerp zijn een aantal ijkpunten uit de NEN 7510 norm geselecteerd, aan de hand waarvan getoetst kan worden of ziekenhuizen aan de NEN 7510 norm voldoen. Deze ijkpunten zijn als uitgangspunt genomen bij de analyse van de interviews. Omdat de gesprekken semi-gestructureerd waren, zijn bij een aantal ziekenhuizen niet genoeg gegevens verkregen om alle ijkpunten te kunnen beoordelen. Hier is in deze

rapportage rekening mee gehouden. Als een bepaald ijkpunt bij meer dan vijftien ziekenhuizen beoordeeld kon worden, zijn uitkomsten weergegeven als percentages. Hierbij zijn ziekenhuizen waarvan geen gegevens bekend waren, niet in de berekening van de percentages meegenomen. Als er gegevens bekend waren van tien tot vijftien ziekenhuizen, zijn uitkomsten weergegeven in algemene bewoordingen (veel, weinig, meer, minder etc). Van de onderwerpen die bij minder dan tien ziekenhuizen behandeld zijn, worden geen algemene bevindingen gerapporteerd maar is een aantal opvallende uitkomsten apart opgenomen in een kader.
Waar mogelijk is een vergelijking gemaakt tussen ziekenhuizen met een laag en hoog exploitatiebudget. Of dit mogelijk was, was zowel afhankelijk van het aantal ziekenhuizen waarover gegevens bekend zijn als de verdeling van deze gegevens. Wanneer bijvoorbeeld van alle ziekenhuizen gegevens bekend zijn maar 90 procent van de ziekenhuizen overeenkomstige resultaten heeft, is vergelijking op grond van exploitatiebudget weinig zinvol.
Naast de interviews is de ziekenhuizen gevraagd een drietal documenten op te sturen voor zover deze aanwezig waren en ze betrekking hadden op informatiebeveiliging. Het ging hierbij om een eventuele risico-analyse, incidentenregistratie en een rapportage van een interne en/of externe audit. Deze documenten zijn in respectievelijk elf, tien en acht gevallen opgestuurd of ter plaatse ingezien.

Toetsingskader

De NEN 7510 norm speelt een prominente rol in dit onderzoek. Verder worden de volgende juridische kaders gehanteerd:

- Kwaliteitswet zorginstellingen.
- Wet op de beroepen in de individuele gezondheidszorg (Wet BIG).
- Wet op de geneeskundige behandelingsovereenkomst (WGBO).
- Artikel 13 Wet bescherming persoonsgegevens (WBP).

Artikel 13 Wet bescherming persoonsgegevens normeert de beveiliging van persoonsgegevens en luidt als volgt:
"De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."
Hierbij kan het volgende worden opgemerkt.

- Technische en organisatorische maatregelen dienen cumulatief te worden getroffen. Zij behoren daarbij een onderling samenhangend en afgestemd stelsel te vormen. Onder technische maatregelen kunnen worden geschaard de logische en fysieke maatregelen in en rondom de informatiesystemen (zoals toegangscontroles, vastlegging van gebruik en back-up). Onder organisatorische maatregelen kunnen worden geschaard maatregelen voor de inrichting van de organisatie en voor het verwerken van persoonsgegevens (zoals toekenning en deling van verantwoordelijkheden en bevoegdheden, instructies, trainingen en calamiteitenplannen).
- In het begrip '*passende*' ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het begrip '*passend*'' duidt mede op een proportionaliteit tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens. Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context

waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Er is in het algemeen geen verplichting om steeds de zwaarste beveiliging te nemen. Er moet sprake zijn van een adequate beveiliging.

- Ter beoordeling van de maatregelen die moeten worden getroffen moet dus rekening worden gehouden met een aantal aspecten, waaronder de risico's die de verwerking en de aard van de te beschermen gegevens met zich brengen. In casu is sprake van persoonsgegevens betreffende de gezondheid, waarop het medisch beroepsgeheim van toepassing is. De beveiliging van dergelijke persoonsgegevens moet voldoen aan de hoogste normen. De maatregelen die moeten worden getroffen zijn tevens afhankelijk van de stand van de techniek en de kosten van de tenuitvoerlegging van de maatregelen.
- Bij de toetsing van de beveiligingsmaatregelen aan art. 13 WBP is de NEN 7510 norm als meetinstrument gebruikt. De NEN 7510 norm is een gezaghebbende sectorale uitwerking van art. 13 WBP; als een ziekenhuis voldoet aan de NEN 7510 norm, mag er van uit worden gegaan dat het ook voldoet aan bovengenoemde wettelijke bepaling. Andersom is dit geen volstrekt automatisme: een ziekenhuis kan ook op andere wijze aantonen dat de beveiliging in orde is, bijvoorbeeld door te voldoen aan de Code voor Informatiebeveiliging (ISO 17799).
- De IGZ ziet deze normen (artikel 13 WBP en NEN 7510 norm) als een norm ter invulling van het begrip 'verantwoorde zorg' als bedoeld in de Kwaliteitswet zorginstellingen en de Wet BIG. De voorwaarden om verantwoorde zorg te kunnen verlenen, zijn bij voldoening aan de norm wat dit betreft dan aanwezig.

Bij de beoordeling van meldingen van calamiteiten waarbij ICT een rol speelt, zal de IGZ het toetsingskader uit dit rapport hanteren.

2 Conclusies en maatregelen

2.1 Conclusies

2.1.1 Informatiebeveiliging in ziekenhuizen schiet nog steeds tekort

Vergeleken met vier jaar geleden is er al veel verbeterd rond de veilige toepassing van ICT in ziekenhuizen, vooral op technisch gebied. Uit het onderzoek rijst dan ook het beeld op dat de meeste ziekenhuizen informatiebeveiliging en gerelateerde risico's vooral als een technisch vraagstuk benaderen.
Het besef dat informatiebeveiliging staat of valt met de organisatie van de informatiebeveiliging en het gedrag van medewerkers, en dat daarvoor een verandering in de cultuur van het ziekenhuis noodzakelijk is, is in de meeste ziekenhuizen nog niet voldoende aanwezig. Er wordt door sommige ziekenhuizen wel aandacht aan gedragsaspecten geschonken, bijvoorbeeld door middel van bewustwordingscampagnes, maar effectieve controle op gedrag ontbreekt nog te vaak. Ook is men zich nog niet voldoende bewust van het gevaar van 'social engineering', waarbij iemand informatie los probeert te krijgen bij personeel, om zodoende toegang te krijgen tot het ziekenhuisnetwerk.

Gedrag: Social Engineering
Een mogelijk gevaar met betrekking tot gedrag dat weliswaar niet in de ijkpunten terugkomt, maar nog onvoldoende onder ogen wordt gezien, is social engineering. Hierbij probeert iemand informatie los te krijgen van personeel om zodoende toegang te krijgen tot het ziekenhuisnetwerk, bijvoorbeeld door zich voor te doen als een medewerker van de ICT-afdeling en naar wachtwoord en inlognaam te vragen. Men is zich waarschijnlijk niet voldoende bewust van het risico van social engineering, aangezien de meeste ziekenhuizen aangeven dat social engineering bij hen niet voorkomt. Slechts één ziekenhuis heeft via een onderzoek bekeken of medewerkers gevoelig zijn voor social engineering. In sommige ziekenhuizen was men zelfs geheel onbekend met het begrip.

Alhoewel er veel verbeteringen te zien zijn op technisch gebied, voldoen toch veel ziekenhuizen nog lang niet aan de onderzochte delen van de NEN 7510 norm. Het algemene beeld dat uit dit thematisch onderzoek naar voren komt, is dat informatiebeveiliging veelal ad hoc en soms zelfs opportunistisch, in de praktijk geregeld wordt en niet gebaseerd is op systematisch uitgewerkt beleid. Dat is niet acceptabel. Geen van de zes onderdelen van de NEN 7510 norm die in dit onderzoek zijn meegenomen, was voldoende opgenomen in de beleidsplannen van de onderzochte ziekenhuizen. Ziekenhuizen in het algemeen, maar zeker Raden van Bestuur in het bijzonder hebben maar een beperkt zicht op de risico's die zich voor kunnen doen als bedreiging voor de veiligheid van de informatie. Het ontbreken van een visie op het gebied van informatiebeveiliging is daar een belangrijk voorbeeld van. Slechts een beperkt aantal ziekenhuizen heeft een risicoanalyse uit laten voeren, terwijl daar wel de instrumenten voor bestaan. Raden van Bestuur kunnen hun verantwoordelijkheid zoals die door de Kwaliteitswet zorginstellingen wordt opgedragen, op deze wijze niet waarmaken.

2.1.2 Verantwoordelijkheid voor informatiebeveiliging onvoldoende ingebed

Wie op uitvoerend niveau verantwoordelijk is voor informatiebeveiliging is nog te vaak onduidelijk, zowel voor bestuurders als medewerkers. Deze onduidelijkheid kan leiden tot situaties waarin verantwoordelijkheden op elkaar afgeschoven worden. Ook komt dit de vorming van beleid rondom informatiebeveiliging niet ten goede en ontbreekt een duidelijk aanspreekpunt voor medewerkers.

Beoordeling van de informatiebeveiliging door externen ontbreekt of is onvoldoende. Informatiebeveiliging maakt vaak deel uit van een algemene beoordeling zoals deze wel wordt uitgevoerd in het kader van de accountantscontrole. Als de informatiebeveiliging in een algemene beoordeling is meegenomen, is deze evenwel meestal te beperkt en is er in elk geval geen sprake van een beoordeling of het ziekenhuis aan de NEN 7510 voldoet.

2.1.3 Uitwisseling van patiëntengegevens met derden buiten de instelling nog beperkt

Vaak beperkt de uitwisseling van elektronische gegevens zich tot het versturen van ontslagbrieven en labinformatie naar huisartsen. Ziekenhuizen zijn nog vrij terughoudend met het verlenen van toegang aan derden tot het ziekenhuissysteem. Contracten voor de gegevensuitwisseling zijn maar in beperkte mate afgesloten. Hierdoor zijn verantwoordelijkheden van verschillende partijen niet altijd duidelijk.

2.1.4 Beleid voor toegangsbeveiliging ontbreekt regelmatig

Verlening van toegang tot bepaalde ruimtes binnen het ziekenhuis, tot het ziekenhuisnetwerk en tot de patiëntgegevens is niet in alle gevallen goed geregeld. Beleid voor toegangsbeveiliging, in de vorm van een document waarin autorisatie per functiegroep is uitgewerkt, ontbreekt in een aantal gevallen. Ook komen onveilige situaties, zoals het gebruik van groepsaccounts of de afwezigheid van automatische schermbeveiliging, nog te vaak voor.

Toegangsbeveiliging: Follow-me
Om werken op elkaars account tegen te gaan, is in één ziekenhuis een systeem ingesteld waardoor als iemand op een tweede computer inlogt hij/zij op de eerste automatisch uitgelogd wordt. Op deze manier kan gemakkelijker op verschillende plekken gewerkt worden zonder dat computers onbeheerd toegankelijk zijn.

2.1.5 Onvoldoende bewustzijn bij personeel

Er is nog onvoldoende aandacht voor de gedragscomponent van informatiebeveiliging; er zijn te weinig ziekenhuizen die een gedragscode hebben die zich specifiek richt op de aspecten van informatiebeveiliging. Als er een gedragscode is, is deze onvoldoende bekend. Het gedrag van werknemers wordt onvoldoende gecontroleerd en maatregelen ontbreken regelmatig.

2.1.6 Naleving van wettelijke voorschriften (te) vanzelfsprekend

Naleving van wetgeving wordt door alle ziekenhuizen als vanzelfsprekend gezien, maar is niet altijd opgenomen in het beleid. Hierdoor bestaat het gevaar dat men niet kritisch toetst of men werkelijk aan de wet- en regelgeving voldoet. Zo ontbreken in enkele ziekenhuizen privacyrichtlijnen en wanneer deze wel aanwezig zijn, wordt de naleving hiervan nergens expliciet gecontroleerd.

2.1.7 Incidentenregistratie vaak nog onvoldoende specifiek

Registratie en rapportage van ICT-gerelateerde incidenten laat te wensen over. Incidenten worden overal geregistreerd, maar nergens zijn informatiebeveiligings-incidenten apart in de registratie terug te vinden. Ook vindt periodieke rapportage van incidenten aan de Raad van Bestuur nog te weinig plaats. Deze beide factoren bemoeilijken de mogelijkheid om van incidenten te leren en het informatiebeveiligingsbeleid aan te kunnen passen.

2.1.8 Spanning tussen veiligheid en werkbaarheid

Bij de conclusies van dit onderzoek moet rekening gehouden worden met het uiteenlopende gebruik van ICT binnen de onderzochte ziekenhuizen. In sommige ziekenhuizen werken enkele afdelingen al geheel elektronisch, terwijl andere ziekenhuizen nog bijna volledig op papier werken. De gevaren van gebrekkige informatiebeveiliging voor patiënten in laatstgenoemde ziekenhuizen zijn klein, maar door de invoering van het EPD zal goed functionerende informatiebeveiliging steeds belangrijker worden.
Inherent aan informatiebeveiliging is een spanningsveld tussen enerzijds veiligheid en anderzijds werkbaarheid. Toepassing van ICT in ziekenhuizen moet veilig gebeuren, om de privacy van de patiënt te beschermen en medische fouten door toedoen van ICT te voorkomen, maar het is tevens in het belang van de patiënt dat gegevens toegankelijk zijn op het moment dat een arts deze nodig heeft. Per situatie zal dus een goede balans gevonden moeten worden tussen deze twee belangen.

2.2 Te nemen maatregelen en handhaving

De twintig onderzochte ziekenhuizen hebben het onderzoeksrapport over het eigen ziekenhuis in juli 2008 ontvangen. Van hen werd uiterlijk 15 oktober 2008 een plan van aanpak verwacht waarin duidelijk wordt wat het ziekenhuis onderneemt om volledig aan de NEN 7510 norm te voldoen en op welke termijn dit zal zijn gerealiseerd. Indien de inhoud van het plan van aanpak (of het geheel uitblijven van een plan van aanpak) daartoe aanleiding geeft, zal handhavend worden opgetreden.
Het is aannemelijk dat alle ziekenhuizen in Nederland aanmerkelijk meer aandacht zullen moeten schenken aan de veilige toepassing van de ICT. Ook de niet-onderzochte ziekenhuizen dienen de NEN 7510 norm volledig te implementeren. Deze ziekenhuizen zullen eveneens een plan van aanpak op moeten stellen waaruit duidelijk blijkt op welke wijze en op welke termijn zij aan alle onderdelen van de NEN 7510 norm zullen voldoen. De IGZ wil van de niet specifiek in dit onderzoek onderzochte ziekenhuizen vóór 1 februari 2009 een plan van aanpak te ontvangen. Daarnaast wil de inspectie van alle ziekenhuizen dat zij in 2010 een externe audit uit laten voeren op de implementatie van de NEN 7510 norm, zoals bedoeld in de NEN 7510 norm. De inspectie wil een exemplaar van deze audit te ontvangen. Zonodig zal op grond van het plan van aanpak een eerdere beoordeling door de inspectie plaats vinden en hand-

havend worden opgetreden. Dat betekent dat bij onvoldoende planvorming om aan de totale NEN 7510 norm te voldoen handhavingmaatregelen ingezet zullen worden.

3 Bevindingen

3.1 Organisatie: Verantwoordelijkheid voor informatiebeveiliging onvoldoende ingebed

IJkpunten

De volgende aspecten van de NEN 7510 norm zijn als ijkpunt genomen bij het onderdeel toewijzing en vastlegging van verantwoordelijkheid voor informatiebeveiliging van het hoofdstuk 'Organiseren van informatiebeveiliging':

- Er is iemand benoemd op directieniveau, die verantwoordelijk is voor informatiebeveiliging.
- Er is een beveiligingsfunctionaris aangesteld en actief.
- Het functioneren van de functionaris wordt geëvalueerd.
- Binnen de instelling speelt de beveiligingsfunctionaris een actieve rol bij implementatie van beveiligingsbeleid en bij het proces van bewustwording en handhaving van de afspraken.
- Beleidsaanpassingen zijn voorgenomen / worden doorgevoerd.

Bevindingen

De verantwoordelijkheid voor informatiebeveiliging op bestuursniveau is in het algemeen goed geregeld, want bij de meeste ziekenhuizen is iemand benoemd binnen de Raad van Bestuur die specifiek verantwoordelijk is voor dit onderwerp; in maar enkele ziekenhuizen (2/20) werd de gehele Raad van Bestuur verantwoordelijk gehouden. Verder waren in tweederde van de ziekenhuizen speciale ICT-commissies actief die de Raad van Bestuur adviseren, in zes gevallen specifiek over informatiebeveiliging of privacy.

De verantwoordelijkheid voor informatiebeveiliging op uitvoerend niveau is niet overal goed geregeld. Slechts bij één deelnemend, academisch, ziekenhuis was een aparte veiligheidsfunctionaris aangesteld. Bij de overige ziekenhuizen was in veel gevallen het hoofd ICT verantwoordelijk, al dan niet in samenwerking met bijvoorbeeld het hoofd beveiliging, medische administratie of logistiek. Bij een derde van de ziekenhuizen was zelfs onduidelijk wie verantwoordelijk was voor de informatiebeveiliging. Een groot gedeelte hiervan betrof ziekenhuizen met een laag exploitatiebudget. In een aantal van deze ziekenhuizen bestonden wel plannen om de verantwoordelijkheid voor informatiebeveiliging duidelijker te beleggen, maar was er discussie of dit een aparte functie moest worden of een onderdeel van een huidige functie. In figuur 1 is weergegeven hoe de verantwoordelijkheid was belegd in de deelnemende ziekenhuizen.

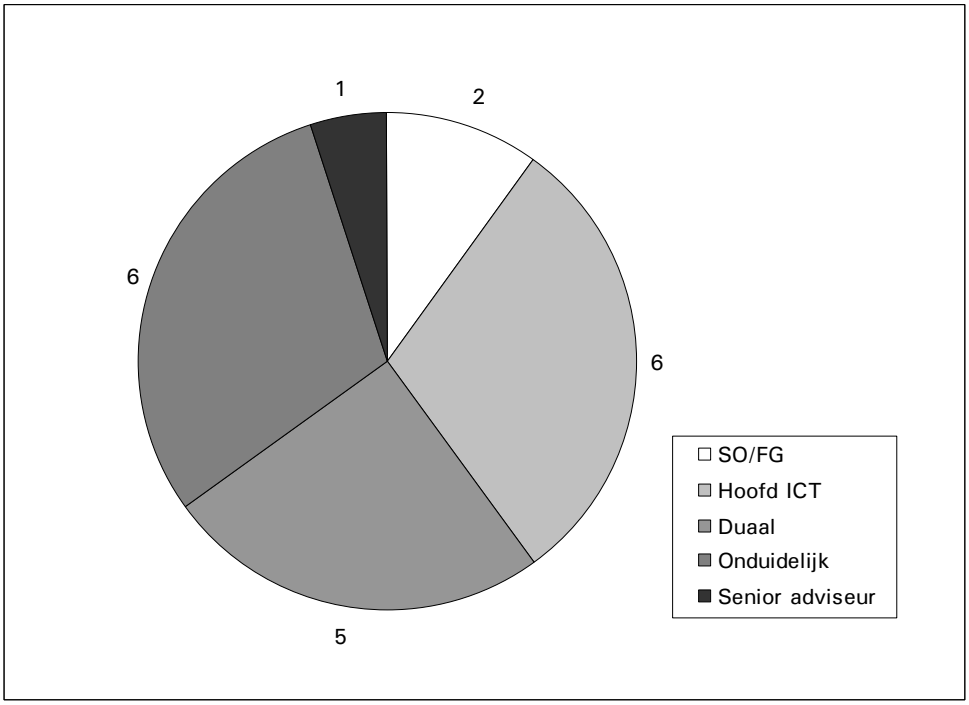
Wanneer de verantwoordelijkheid voor informatiebeveiliging op uitvoerend niveau wel duidelijk belegd was, waren de randvoorwaarden om een actieve rol in de organisatie te kunnen spelen lang niet altijd aanwezig. Zo was de verantwoordelijkheid voor informatiebeveiliging maar bij een klein aantal verantwoordelijken opgenomen in de taakomschrijving en werd het budget voor informatiebeveiliging in driekwart van de gevallen projectmatig geregeld.

Wel speelde de verantwoordelijke in veel gevallen een duidelijke rol bij het ontwikkelen en goedkeuren van nieuwe ICT-projecten. Of het functioneren van de verantwoordelijke geëvalueerd werd, kwam niet duidelijk uit het onderzoek naar voren.

De bekendheid van de verantwoordelijke binnen de organisatie liet te wensen over. Wanneer de verantwoordelijkheid duidelijk was belegd, was maar bij de helft van de geïnterviewde werknemers bekend wie het aanspreekpunt voor informatiebeveiliging was. Wanneer de verantwoordelijkheid niet duidelijk belegd was, hielden de werknemers het hoofd ICT en/of de directie verantwoordelijk.

Duidelijk beleid voor informatiebeveiliging was er lang niet in alle gevallen. In driekwart van de ziekenhuizen was er wel beleid voor informatiebeveiliging, maar bij bijna de helft daarvan was dit nog in ontwikkeling. Tekenend was, dat een aantal ziekenhuizen aangaf dat er (nog) geen officieel beleid was maar dat "dingen in de praktijk goed geregeld zijn". Hierbij speelde een rol dat een groot aantal ICT-afdelingen, namelijk elf, net een reorganisatie of fusie achter de rug hadden of daar plannen voor hadden. Dit werd vaak als reden genoemd voor de afwezigheid van volledig uitgewerkt beleid.

Figuur 1
Verantwoordelijke voor informatiebeveliging



In figuur 1 is aangegeven hoeveel ziekenhuizen een FG, een Hoofd ICT, een senior adviseur verantwoordelijk is voor de informatiebeveiliging dan wel dat zij dat duaal geregeld hebben.

Conclusie en beoordeling

De verantwoordelijkheid voor informatiebeveiliging is nog niet voldoende ingebed in de organisatie van ziekenhuizen. Er is veelal geen functionaris gegevensbescherming aangesteld, bij werknemers is het vaak onduidelijk wie er verantwoordelijk is en informatiebeveiliging heeft nog maar beperkt aandacht in beleidsplannen.

3.2 Organisatie: Externe beoordeling informatiebeveiliging nog te summier

IJkpunten

De volgende aspecten van de NEN 7510 norm zijn als ijkpunt genomen bij het onderdeel onafhankelijke beoordeling van het hoofdstuk 'Organiseren van informatiebeveiliging':

- Er is iemand verantwoordelijk voor het laten uitvoeren van externe audits voor de informatiebeveiliging.
- Er is een externe beoordeling uitgevoerd.
- Er is een rapportage van de bevindingen.
- De audit is uitgevoerd door een ter zake deskundig (geaccrediteerd) instituut.
- De audit heeft alle risicovolle aspecten omvat.

- Er is naar aanleiding van de resultaten van de audit actie ondernomen .
- Er is toezicht op implementatie van de aanbevelingen.
- De NVZ/ NEN monitor is toegepast.

Bevindingen

Een behoorlijk deel van de ziekenhuizen (60 procent) had de informatiebeveiliging laten beoordelen door een extern bedrijf. Hierbij is van belang te vermelden dat de beoordeling van de informatiebeveiliging vaak deel uitmaakte van een uitgebreidere accountantsbeoordeling. Het accent lag hierbij vaak op de vraag of de ICT-omgeving zodanig was dat er betrouwbare gegevens voor de jaarrekening gegenereerd konden worden. Informatiebeveiliging is echter veel breder dan dat en in veel gevallen voldeed de accountantsbeoordeling dan ook niet als externe audit. De mate waarin informatiebeveiliging binnen de totale beoordeling meegenomen werd, was erg wisselend. Ook waren de beoordelingen wisselend van aard, bijvoorbeeld vooral gericht op het technische of het organisatorische deel.
Over alle externe beoordelingen waren rapporten verschenen, maar de inhoud van de rapportages was erg wisselend. In sommige gevallen besloeg het deel over informatiebeveiliging niet meer dan een alinea, in andere gevallen het hele rapport. Bij de ziekenhuizen die geen externe beoordeling hadden laten uitvoeren, was bij een groot deel (70 procent) wel een interne controle uitgevoerd. Deze controle was eveneens wisselend van omvang en aard. Zes ziekenhuizen hadden zich, in opdracht, laten hacken, om op deze manier lekken in de beveiliging van het netwerk te achterhalen.
Driekwart van de externe beoordelingen hadden ook daadwerkelijk geleid tot aanpassingen, zowel op beleidsmatig, organisatorisch als technisch gebied. De resultaten van de beoordeling waren waarschijnlijk niet diep in de organisatie doorgedrongen, aangezien maar een klein deel van de geïnterviewde artsen, namelijk twee, op de hoogte bleek van de externe beoordeling. Dit resultaat was echter moeilijk op waarde te schatten, aangezien er maar één medisch specialist per ziekenhuis was geïnterviewd. Controle op de implementatie van de aanbevelingen uit de rapportage was er lang niet altijd, namelijk in iets minder dan de helft van de gevallen. Controle gebeurde meestal door het bedrijf dat de externe beoordeling had uitgevoerd.
Door de academische ziekenhuizen was een zogenaamde UMC-monitor ontwikkeld, waarmee ziekenhuizen zelf konden nagaan of ze aan de NEN 7510 voldeden. De NVZ vereniging van ziekenhuizen had dit instrument doorontwikkeld voor algemene ziekenhuizen. Deze NVZ-monitor werd maar door een klein deel van de ziekenhuizen gebruikt.

Conclusie en beoordeling

Beoordeling van de informatiebeveiliging door externen ontbreekt of is onvoldoende. Informatiebeveiliging maakt vaak (beperkt) deel uit van een algemene beoordeling en de mate waarin informatiebeveiliging binnen de totale beoordeling meegenomen werd is erg wisselend. Ziekenhuizen hebben daardoor geen of onvoldoende beeld van hun informatiebeveiliging.

3.3 Externe partijen: Uitwisseling van patiëntengegevens met derden buiten de instelling nog beperkt

IJkpunten

De volgende aspecten van de NEN 7510 norm zijn als ijkpunt genomen bij het onderdeel ‘Externe partijen’:

- Risico’s met betrekking tot uitwisseling van informatie met en verlenen van toegang aan derden zijn onderkend en afgewogen in de risicoanalyse.

– De voorwaarden voor uitwisseling met derden zijn contractueel vastgelegd en de voorwaarden worden door alle betrokkenen in acht genomen.
– Regelmatig (en bij verlenging/herziening van contracten) worden deze voorwaarden geëvalueerd.

Bevindingen

Bij alle ziekenhuizen was sprake van uitwisseling van gegevens met externe partijen, zij het dat in de meeste gevallen uitwisseling van patiëntgegevens met betrekking tot het primaire zorgproces nog vrij beperkt was. Zonder uitzondering was er uitwisseling met huisartsen, waarvan het grootste deel (90 procent) verloopt via EDIFACT-berichten. In een meerderheid van de gevallen (60 procent) ging het om eenrichtingsverkeer vanuit het ziekenhuis, bijvoorbeeld versturen van labuitslagen en ontslagbrieven. In 40 procent van de ziekenhuizen ging het om interactief contact, waarbij huisartsen bijvoorbeeld patiënten konden doorverwijzen. Bij drie ziekenhuizen konden huisartsen of artsen uit een ander ziekenhuis rechtstreeks in het ziekenhuissysteem bij de gegevens van hun eigen patiënten en bij één ziekenhuis waren hier plannen voor. Het betrof hier vier ziekenhuizen met een relatief groot exploitatiebudget. Over het algemeen waren ziekenhuizen terughoudend in het aansluiten van derden op hun ziekenhuissysteem. Zij gingen er weloverwogen mee om.
Uitwisseling met andere zorginstellingen was regelmatig georganiseerd in de vorm van regionale netwerken van samenwerkende ziekenhuizen en huisartsen, maar ook verzorgings- en verpleeghuizen, thuiszorginstellingen en huisartsenlaboratoria namen deel. 35 procent van de ziekenhuizen had een verbinding met andere zorginstellingen en nog eens 30 procent had plannen om zo'n verbinding aan te gaan. Deze vorm van uitwisseling leek vaker te bestaan bij ziekenhuizen met een hoog exploitatiebudget.
Andere partijen die vaak toegang hadden tot het ziekenhuisnetwerk waren de software- en netwerkleveranciers. Vaak hadden zij toegang via een inbelverbinding en in enkele gevallen hadden ze toegang via een token[1]. In veel gevallen was toestemming nodig om toegang te krijgen tot het ziekenhuisnetwerk, maar in enkele gevallen hadden leveranciers toegang zonder tussenkomst van ziekenhuismedewerkers. Toezicht op de precieze werkzaamheden die leveranciers uitvoeren, ontbrak vaak.
Contracten voor de gegevensuitwisseling met externe partijen waren bij driekwart van de ziekenhuizen afgesloten. Echter te veel gevallen betrof dit uitsluitend contracten met leveranciers, zowel van software als van de netwerken zelf. Deze contracten met leveranciers waren vooral op de toegang tot het systeem gericht en kenden veelal geen bepalingen ten aanzien van de bevoegdheden van de leverancier als deze toegang had verkregen tot het systeem. Hiervoor zou in de toekomst meer aandacht moeten zijn.
Een overzicht van de aanwezige contracten wordt gegeven in tabel 1.

Conclusie en beoordeling

Uitwisseling van patiënteninformatie betreffende het primaire zorgproces met externe partijen is in veel gevallen nog vrij beperkt, maar wel groeiende. Er is nog te weinig aandacht voor het contractueel vastleggen van onderlinge verplichtingen. Positief is dat ziekenhuizen weloverwogen omgaan met het aansluiten van externen, inclusief huisartsen, op het ziekenhuissysteem.

---

[1] Dit apparaat toont een code die na een bepaalde tijd verandert. Een gebruiker kan dan met behulp van een pincode en die tokencode inloggen op het ziekenhuisnetwerk.

Tabel 1
Contracten met externe partijen over gegevensuitwisseling

	Aantal ziekenhuizen n = 20
Huisartsen	5
Andere ziekenhuizen	1
Regionale netwerken	3
Leveranciers	13

3.4 Beveiliging ten aanzien van personeel: Onvoldoende bewustzijn bij personeel

IJkpunten
De volgende aspecten van de NEN 7510 norm zijn als ijkpunt genomen bij het onderdeel 'beveiligingseisen ten aanzien van personeel':
- Er is een gedragscode vastgesteld.
- De gedragscode is bij alle werknemers bekend.
- Men houdt zich aan deze code.
- Afwijkingen worden gerapporteerd en adequaat afgehandeld.

Bevindingen
In iets meer dan de helft van de ziekenhuizen was een gedragscode ten aanzien van geheimhouding van kracht. Tweederde van de ziekenhuizen had alleen of daarnaast een code die zich beperkte tot het gebied van ICT, bijvoorbeeld voor het gebruik van e-mail en internet. De bekendheid van de gedragscode onder de geïnterviewde werknemers liet echter te wensen over, aangezien het bestaan van een gedragscode maar bij de helft van de geïnterviewde artsen bekend was. Wanneer de code bij hen niet bekend was, wezen zij meestal op hun beroepsgeheim. Echter, het bestaan van een beroepsgeheim maakt een gedragscode niet overbodig. In een gedragscode op het gebied van informatiebeveiliging zal bijvoorbeeld inzage van gegevens of communicatie via e-mail geregeld moeten worden.

De aandacht voor de gedragscode ten aanzien van geheimhouding (al dan niet beperkt tot ICT) vanuit de ziekenhuisorganisatie was wisselend. De gedragscode kwam maar bij tweederde aan bod tijdens de introductie of de aanstelling. Er waren echter ook enkele ziekenhuizen waar wel aandacht besteed werd aan de gedragscode en waar men de bekendheid van de gedragscode probeerde te vergroten door deze bijvoorbeeld tijdens het opstarten van de computer op het scherm te tonen of door deze als schermbeveiliging of muismat te gebruiken.
Bij tweederde van de ziekenhuizen waren voorbeelden bekend van medewerkers die zich niet aan de gedragscode ten aanzien van geheimhouding hadden gehouden. De geconstateerde afwijkingen betroffen vooral ongeoorloofde inzage van patiëntengegevens. De mogelijkheid tot controle van inzage in het ziekenhuissysteem was bij driekwart van de ziekenhuizen aanwezig, maar dit gaf nog geen garantie dat de patiënt ook daadwerkelijk die inzage zou krijgen. In sommige andere ziekenhuizen bestond wel de mogelijkheid tot logging, maar werd hier geen gebruik van gemaakt omdat het

systeem daardoor te traag werd. Bovendien werden verzamelde gegevens ook niet altijd bekeken. Er werden ook lang niet altijd maatregelen genomen tegen werknemers die zich niet aan de gedragscode hielden. Potentiële maatregelen werden namelijk maar door 45 procent van de ziekenhuizen gemeld. De genomen maatregelen varieerden van een aantekening in het personeelsdossier tot ontslag.

Conclusie en beoordeling

Er is nog onvoldoende aandacht voor de gedragscomponent van informatiebeveiliging; er zijn te weinig ziekenhuizen die een gedragscode hebben die zich specifiek richt op de aspecten van informatiebeveiliging. Als er een gedragscode is, is deze onvoldoende bekend, gedrag van werknemers wordt onvoldoende gecontroleerd en maatregelen ontbreken regelmatig.

Uitlekken gegevens

Een pijnlijk incident voor een ziekenhuis en patiënt was het uitlekken van een operatieverslag. Via een advocaat werd het ziekenhuis gemeld dat een operatieverslag van een patiënt, compleet met naam en toenaam, op internet circuleerde. Deze zaak is zeer hoog opgenomen door het ziekenhuis en na verder onderzoek bleek dat het uitlekken in dit geval niet aan medewerkers van het ziekenhuis te wijten was.

3.5 Toegangsbeveiliging: Beleid voor toegangsbeveiliging ontbreekt regelmatig

IJkpunten fysieke beveiliging en beveiliging van omgeving

De volgende aspecten van de NEN 7510 norm zijn als ijkpunt genomen bij het onderdeel ‘fysieke toegangsbeheersing’

- Er is beleid voor toegangsbeheersing.
- Dit beleid is volledig gerealiseerd.
- Het beleid wordt jaarlijks geëvalueerd en herzien.
- Er zijn noodprocedures aanwezig, het risico van social engineering is onderkend en hiertegen zijn maatregelen getroffen. Er zijn voorts maatregelen voor het beheer van papieren dossiers getroffen.

IJkpunten beveiliging toegang tot informatie

De volgende aspecten van de NEN 7510 norm zijn als ijkpunt genomen bij het onderdeel ‘Toegang tot informatie’:

- Er is beleid voor het verlenen van toegang tot informatie.
- Het beleid is volledig gerealiseerd.
- Het beleid wordt jaarlijks geëvalueerd en herzien.

Bevindingen

Toegang tot ruimten

Een volledig uitgewerkt toegangsbeleid, waarin toegang tot kritische ruimtes per functiegroep vastligt, was maar bij 60 procent van de bezochte ziekenhuizen aanwezig. Wel was bij alle ziekenhuizen de toegang praktisch geregeld waarbij autorisatie niet strikt vastlag, maar per persoon bepaald werd. Uitgewerkt beleid was veel vaker aanwezig bij ziekenhuizen met een groot budget.

De manier van toegangsbeveiliging verschilde binnen de ziekenhuizen. Bij 85 procent van de ziekenhuizen werd toegang geregeld door middel van pasjes en/of codes en bij 15 procent uitsluitend door middel van sleutels. Een overzicht van de manieren van toegangsbeveiliging wordt gegeven in tabel 2.

Tabel 2
Manier van toegangsbeveiliging

	Aantal ziekenhuizen n = 20
Pasje	15
Toegangscode	5
Sleutel	5

Toegang tot patiëntengegevens

Ook uitgewerkt beleid voor toegang tot computers en de verschillende programma's daarop ontbrak regelmatig. Dit was echter een vereiste voor veilig gebruik van ICT. Driekwart van de ziekenhuizen had een (uitgewerkte) autorisatiestructuur, waarin toegang tot computers en de verschillende programma's daarop per functiegroep vastlag. Van de overige ziekenhuizen hadden twee plannen voor zo'n autorisatiematrix. Alle ziekenhuizen in dit onderzoek met onvolledig beleid waren ziekenhuizen met een klein exploitatiebudget.

Bij ruim tweederde van de ziekenhuizen waren nog groepsaccounts aanwezig, waarbij meerdere mensen onder één inlognaam en wachtwoord werkten. Dit betrof vooral verpleegafdelingen en de eerste hulp. Veelal was dit om praktische redenen ingesteld, namelijk zodat medewerkers niet voortdurend apart hoefden in te loggen. Door het gebruik van groepsaccounts was echter niet meer te achterhalen wie een dossier had ingezien of veranderd. Een gevolg daarvan was dat dan ook niet meer te achterhalen was wie een dossier ongeoorloofd had ingezien.

Een andere groep die in sommige gevallen geen persoonlijk account had, waren de groepen co-assistenten en arts-assistenten. Vanwege het relatief grote verloop bij deze groepen werd vaak met een aantal standaard gebruikersnaam- en wachtwoord-combinaties gewerkt die werden doorgegeven aan opvolgers. Toch is het belangrijk om deze groepen ook voor een korte periode een persoonlijk account te geven, omdat anders inloggegevens ook na beëindiging van werkzaamheden voor het ziekenhuis nog gebruikt zouden kunnen worden.

Bij de meeste ziekenhuizen (81 procent) moest na het inloggen op de computer voor toegang tot verschillende programma's apart ingelogd worden. Doordat medewerkers gemakkelijk op het account van een ander onder hun eigen naam in een programma

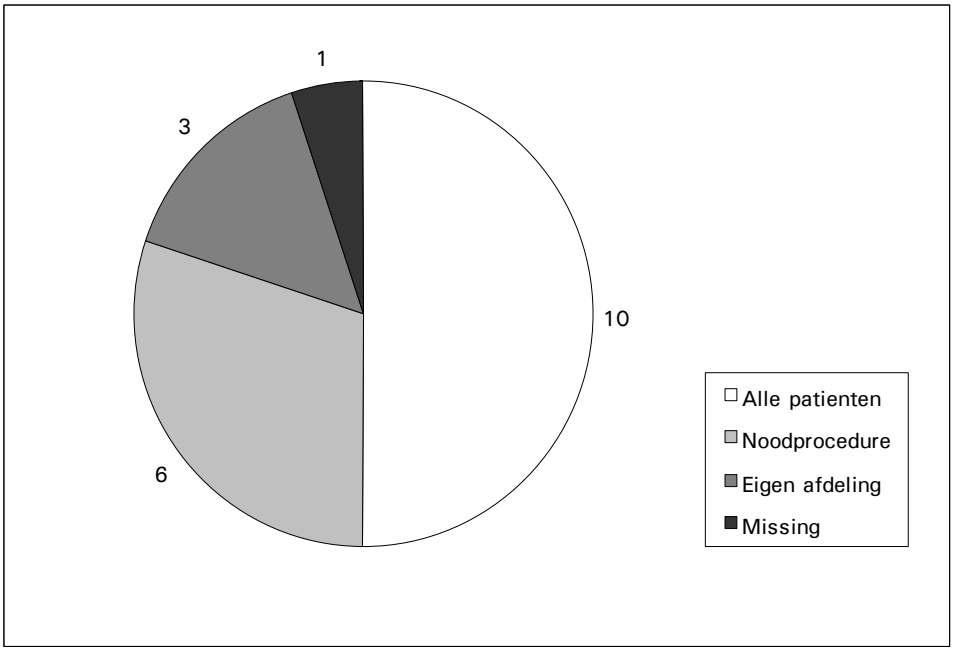
konden inloggen, was gebruik van elkaars account erg verleidelijk. Nadeel hiervan was dat op deze manier mogelijk ook patiëntgegevens waarvoor iemand zelf niet geautoriseerd was, toegankelijk waren. Daarentegen was door het apart inloggen wel duidelijk wie het programma gebruikte. Bij enkele ziekenhuizen hoefden werknemers maar één keer in te loggen om toegang te krijgen tot alle programma's, waartoe de betreffende medewerker geautoriseerd was, ofwel het zogenaamde single sign on. Behalve dat dit praktische voordelen heeft, werkt dit gebruik van elkaars account tegen.

Een andere maatregel om gebruik van elkaars account te voorkomen is het instellen van schermbeveiliging, waarbij opnieuw ingelogd moet worden nadat een computer een bepaalde tijd niet is gebruikt. Dit was aanwezig bij driekwart van de ziekenhuizen. Het instellen van schermbeveiliging bleek in een aantal gevallen tot praktische bezwaren bij het personeel te leiden. Discussiepunt hierbij was de tijdsduur waarna een computer in het slot valt. Hierbij moest een middenweg gezocht worden tussen functionaliteit, namelijk onnodig vaak inloggen, en beveiliging, namelijk voorkomen dat computers onbeheerd toegankelijk zijn.

Een ander punt van discussie binnen ziekenhuizen was of artsen toegang krijgen tot gegevens van alle patiënten, wat men vanuit medisch oogpunt wenselijk vindt, of alleen tot patiënten waarmee ze een directe behandelrelatie hebben, wat men vanuit privacyoogpunt wenselijk vindt. Een oplossing hiervoor is het inbouwen van een noodprocedure, waarbij een arts een melding krijgt wanneer hij/zij de directe behandelrelatie overschrijdt. Dit kan vervolgens gelogd worden. Op welke manier artsen toegang hebben tot patiëntengegevens, is weergegeven in figuur 2.

Figuur 2

Toegang artsen in ziekenhuissysteem



In figuur 2 is aangegeven tot welke gegevens de artsen in het ziekenhuis toegang hebben. Soms zijn dat de gegevens van alle patiënten, soms van alleen hun eigen patiënten. Ook is aangegeven in hoeveel gevallen er sprake is van een noodprocedure waarbij artsen toegang tot alle patiëntengegevens kunnen krijgen.

Conclusie en beoordeling
Zowel de toegang tot ruimten als tot patiënteninformatie is nog te weinig vastgelegd in uitgewerkt beleid. Ook komen onveilige situaties, zoals het gebruik van groepsaccounts of de afwezigheid van automatische schermbeveiliging, nog te vaak voor.

Koppeling met salarisgegevens
Om onrechtmatige toegang tot het ziekenhuisnetwerk te voorkomen is het belangrijk om het wachtwoord regelmatig te veranderen. Er zijn echter een paar ziekenhuizen waar dit niet standaard hoeft te gebeuren. Als reden wordt gegeven dat men dan makkelijker zijn/haar wachtwoord vergeet en dat dit gemakkelijk te omzeilen is. Een mogelijke oplossing hiervoor is het koppelen van het account met persoonlijke informatie van het personeel, bijvoorbeeld door het verzenden van de salaris-gegevens per e-mail. Wanneer vertrouwelijke informatie over medewerkers zelf op hun account aanwezig is, zullen zij hoogstwaarschijnlijk voorzichtiger met hun toegangscodes omgaan.

3.6 Naleving: Naleving van wettelijke voorschriften (te) vanzelfsprekend

IJkpunten
De volgende aspecten van de NEN 7510 norm worden als ijkpunt genomen bij het onderdeel 'Naleving':
- Er is beleid ten aanzien van de naleving van wetgeving.
- Er is een analyse gemaakt van de toepasselijke wetgeving.
- Hieruit zijn consequenties getrokken voor de interne bedrijfsvoering en dit is vertaald in reglementen, procedures en maatregelen.
- Er is toezicht op de naleving hiervan.

Bevindingen:
Bijna alle ziekenhuizen gaven aan dat ze zich aan de wetgeving houden. Dit sociaal wenselijke antwoord viel te verwachten. Naleving van wetgeving was echter bij een vijfde van de ziekenhuizen niet opgenomen in het ziekenhuisbeleid. Of er een analyse was gemaakt van de toepasselijke wetgeving kwam uit het onderzoek niet naar voren. Bij bijna alle ziekenhuizen was wetgeving wel vertaald in reglementen, procedures en maatregelen. Hierbij was vooral aandacht voor de voorlichting van de patiënt. Alle ziekenhuizen hadden bijvoorbeeld procedures voor inzage in het medisch dossier door patiënten, en een aantal had ook procedures voor wijziging of verwijdering van gegevens op verzoek van patiënten. Hoewel hierbij aangetekend moet worden dat verwijdering van digitale gegevens erg moeilijk was, omdat bijna niet te achterhalen is op welke plekken informatie over een bepaalde patiënt precies staat. Bovendien werden papieren dossiers soms gedigitaliseerd door ze in te scannen op optische schijven die niet meer te wissen waren. Wel konden gegevens (gedeeltelijk) ontoegankelijk gemaakt worden. Het betreft vooral de consequenties van de WGBO waar men rekening mee had gehouden. De wijze waarop de eisen van de WBP in de ziekenhuisregelingen zijn verwerkt, bleek veel minder duidelijk.
Minder aandacht werd besteed aan de naleving van wetgeving door personeel. Het werd ook door medewerkers zelf als vanzelfsprekend gezien dat zij zich aan de wetgeving houden. In enkele ziekenhuizen werd er op dit gebied onderwijs gegeven door een juridisch medewerker, om zo de medewerkers up-to-date te houden. Specifieke

privacyrichtlijnen voor personeel waren in een groot deel van de ziekenhuizen van kracht, of bestonden daar plannen voor. Controle op naleving van de richtlijnen ontbrak echter.

Conclusie en beoordeling
Naleving van wetgeving wordt teveel als vanzelfsprekend gezien; naleving van wetgeving is nog onvoldoende opgenomen in het beleid en onvoldoende uitgewerkt ten behoeve van interne bedrijfsvoering. Daarnaast is het uiterst zorgelijk dat men niet kan garanderen dat alle informatie over een patiënt verwijderd kan worden omdat met niet weet waar alle gegevens over één patiënt zich precies bevinden.

3.7 Incidenten: Incidentenregistratie vaak nog onvoldoende specifiek

IJkpunten
De volgende aspecten van de NEN 7510 norm worden als ijkpunt genomen bij het onderdeel 'Incidenten':
- Er is beleid voor het melden, registreren en afhandelen van incidenten vastgesteld.
- Deze afspraken zijn bij alle werknemers bekend.
- Men houdt zich aan deze afspraken.
- Afwijkingen van deze afspraken worden gerapporteerd en adequaat afgehandeld.

Bevindingen
In tabel 3 is weergegeven welke 'ICT-incidenten' door ziekenhuizen gemeld werden. Wat in het kader van informatiebeveiliging door de geïnterviewde personen onder een incident werd verstaan, bleek zeer divers te zijn. Dit varieerde van onrechtmatige inzage in gegevens tot uitval van systemen.

Incidenten: Onrechtmatige inzage
In één ziekenhuis is de directie wel heel persoonlijk geconfronteerd met het belang van informatiebeveiliging. Tijdens een opname van de voorzitter van de Raad van Bestuur in zijn eigen ziekenhuis hebben namelijk verschillende medewerkers, die hem niet behandelden, zich toegang verschaft tot zijn elektronisch medisch dossier. In eerste instantie is besloten hier geen verdere consequenties aan te verbinden, maar op aandringen van de IGZ en het CBP is dit opnieuw in overweging genomen.

In een groot deel van de ziekenhuizen werd aangegeven dat ICT-incidenten gemakkelijk gemeld werden, waarbij aangemerkt moet worden dat maar één medisch specialist per ziekenhuis is geïnterviewd. In het onderzoek wordt het beeld bevestigd dat verpleegkundigen gemakkelijker melden dan specialisten. Alle ondervraagde medisch specialisten gaven wel aan een MIP-melding (melding incidenten patiëntenzorg) te doen als er een patiëntgebonden incident met betrekking tot ICT voorkwam. In één ziekenhuis liep op het moment van het gesprek een bewustwordingscampagne om het meldingsgedrag te verbeteren en bij nog drie andere ziekenhuizen stonden bewustwordingscampagnes gepland.
Vijf ziekenhuizen namen deel aan het project 'Sneller Beter' en vier (andere) ziekenhuizen zijn pilot-ziekenhuis voor het VMS Zorgproject. Tegen de verwachting in geven juist in deze ziekenhuizen medewerkers aan dat er niet gemakkelijk gemeld wordt. Dit zou mogelijk verklaard kunnen worden door een beter bewustzijn van de noodzaak tot

incidentmelding, waardoor medewerkers de meldingscultuur binnen het ziekenhuis reëler inschatten.
Bij alle bezochte ziekenhuizen was een incidentenregistratie aanwezig, maar de inhoud en uitgebreidheid daarvan verschilde sterk. Zo bevatte de ICT-incidentenregistratie van één ziekenhuis vooral gebruikersvragen aan de ICT-afdeling. Ook waren incidenten met betrekking tot informatiebeveiliging nog nergens apart in de registratie te herkennen.
ICT-incidenten waren maar bij een klein aantal ziekenhuizen in het algemene noodplan opgenomen, maar er waren in enkele ziekenhuizen zogenaamde Computer Emergency Response Teams die bijvoorbeeld bij uitval van systemen snel in actie konden komen. Dit gaf echter geen garantie dat zich geen problemen ten aanzien van de informatie-beveiliging voor konden doen, want het herstellen van systemen nam vaak enige tijd in beslag. Het is dus van belang dat er procedures zijn voor het geval er een risico is dat gegevens gecorrumpeerd zijn of dat gegevens zijn zoekgeraakt.
Bij veel ziekenhuizen werd aangegeven dat de Raad van Bestuur snel op de hoogte gesteld werd bij relevante ICT-incidenten. Het gevaar bestond echter dat minder ernstige ICT-incidenten aan de aandacht van de Raad van Bestuur ontsnapten.
Periodieke rapportage van ICT-incidenten aan de Raad van Bestuur vond namelijk nog weinig plaats. In slechts een kwart van de ziekenhuizen was er regulier overleg, bijvoorbeeld tussen het hoofd van de ICT afdeling en (een lid van) de Raad van Bestuur, over ICT-incidenten die in de afgelopen periode hadden plaatsgevonden.

Conclusie en beoordeling
Registratie en rapportage van informatiebeveiligings-gerelateerde incidenten schiet nog tekort. Incidenten worden overal geregistreerd, maar nergens zijn informatie-beveiligingsincidenten apart in de registratie terug te vinden. Ook vindt periodieke rapportage van ICT-incidenten aan de Raad van Bestuur nog te weinig plaats. Deze beide factoren bemoeilijken analyse van incidenten ten behoeve van beleid.

Tabel 3
'Incidenten' die tijdens het onderzoek gemeld werden

	Aantal ziekenhuizen n = 20
Uitval systeem	13
Onrechtmatige inzage medische gegevens	5
Aanval op de firewall	3
Verwisseling medische gegevens	2
Misbruik internet	2
Uitlekken operatieverslag	1
Geen incidenten	3

4 Summary

Further to a previous study conducted by the Health Care Inspectorate, the results of which were published in the 2004 report *ICT in ziekenhuizen* ['ICT in hospitals'], it was decided to perform a follow-up investigation of data security procedures in Dutch hospitals. This decision was also prompted by the imminent (partial) introduction of the 'Electronic Patient Dossier' and the growing use of ICT in direct patient care. The current study by the Health Care Inspectorate and the Dutch Data Protection Authority (DPA) examined procedures in twenty hospitals, based on interviews with representatives of the Board of Directors, the ICT department and the medical staff.

The objective of the study was to gain a general impression of the current status of implementation of the NEN 7510 standard among Dutch hospitals. The data protection measures in the selected hospitals were also examined in detail to determine the degree of compliance with extant legislation.

The study reveals that significant improvements have been made in the four years since the previous investigation, particularly with regard to the technical aspects of data security. However, there remains a lack of awareness, among both management and staff, with regard to the risks which attach to the use of ICT in hospitals. In general, due care is taken when allowing other care institutions access to the host organization's network. However, it would appear that the majority of hospitals do not yet comply in full with the requirements of the NEN 7510 norm. In many cases, data security procedures have not been laid down in a formal policy, and too much is still arranged on an *ad hoc* basis. Another significant finding is that staff are not adequately aware of the importance of data security. Staff behaviour is the most crucial component of good data security practice. There are still too many instances in which no effective supervision of that behaviour is in place.

Of the twenty hospitals examined, nine did not have an 'appropriate level of security' as defined under Article 13 of the Personal Data Protection Act and additionally failed to meet the 'conditions of responsible care' set out in Article 2 of the Care Institutions (Quality) Act. Five hospitals were found to have a security level well below the required standard. Six other hospitals had indeed taken some measures, but their security level remained unacceptable.

The twenty hospitals are now required to explain how they intend to implement an appropriate level of data security. They must submit an Action Plan to both the Inspectorate and the DPA, setting out the intended remedial action and the date by which all measures will be in place. If they fail to submit this plan, or if the content of the plan is deemed unsatisfactory, enforcement action will be taken.

The Inspectorate further intends to request all other hospitals in the Netherlands to produce an Action Plan setting out how they intend to ensure compliance with the NEN 7510 standard. In 2010, all hospitals will also be required to present the results of an external audit, as required by the NEN 7510 standard, establishing the exact status of data security measures and procedures at the time of the audit. Again, if the content of the Action Plan is unsatisfactory, i.e. it does not make clear how *all* requirements of the NEN 7510 standard are to be met, the Inspectorate will conduct an interim assessment and will take appropriate enforcement action if necessary.

BIJLAGE 1 Lijst met afkortingen

CBP	College bescherming persoonsgegevens
EMD	Elektronisch medicatiedossier
EPD	Elektronisch patiëntendossier
FG	Functionaris Gegevensbescherming
ICT	Informatie Communicatie Technologie
IGZ	Inspectie voor de Gezondheidszorg
ISO	International Standardisation Organisation
LSP	Landelijk Schakelpunt
MIP	Meldingen Incidenten Patiëntenzorg
NEN	Nederlands Normalisatie Instituut
NVZ	Nederlandse Vereniging Ziekenhuizen
TICTzorg	Toetsing ICT in de zorg
UMC	Universitair Medisch Centrum
VMS	Veiligheidsmanagementsysteem
Wet BIG	Wet op de beroepen in de individuele gezondheidszorg
WBP	Wet bescherming persoonsgegevens
WDH	Waarneemdossier huisartsen
WGBO	Wet op de geneeskundige behandelingsovereenkomst

BIJLAGE 2 Lijst met onderzochte ziekenhuizen

Ziekenhuis	*Plaats*
Albert Schweitzer Ziekenhuis	Dordrecht
Alysis Zorggroep	Arnhem
AMC	Amsterdam
Antoni van Leeuwenhoek Ziekenhuis (NKI-AVL)	Amsterdam
Atrium MC	Heerlen
Canisius-Wilhelmina Ziekenhuis	Nijmegen
Diaconessenhuis	Leiden
Erasmus MC	Rotterdam
IJsselmeerziekenhuizen	Lelystad
Maasziekenhuis Pantein	Boxmeer
Medisch Centrum	Alkmaar
Medisch Centrum Haaglanden	DenHaag
Medisch Spectrum Twente	Enschede
Rijnland Ziekenhuis	Leiderdorp
St. Anna Ziekenhuis	Geldrop
St. Jans Gasthuis	Weert
St. Lucas Ziekenhuis	Winschoten
Van Weel-Bethesda Ziekenhuis	Dirksland
Wilhelmina Ziekenhuis	Assen
Ziekenhuis Lievensberg	Bergen op Zoom

BIJLAGE 3 De NEN 7510 (bron: www.nen7510.org)

Het Nederlands Normalisatie-Instituut (NEN) faciliteert processen om te komen tot Nederlandse veldnormen. NEN brengt veldpartijen bij elkaar en realiseert volgens een vast procedure de totstandkoming van normen. De norm NEN 7510 is volgens de NEN procedures tot stand gekomen en gaat over informatiebeveiliging binnen de zorgsector. Onder informatiebeveiliging in de zorg wordt verstaan: het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die benodigd is om patiënten verantwoorde zorg te kunnen bieden. Naast het borgen van deze kwaliteitscriteria vereist deze norm ook dat de informatiebeveiligingsmaatregelen op controleerbare wijze zijn ingericht voordat kan worden gesproken over adequate informatiebeveiliging. De norm kan beschouwd worden als een kader. Binnen dit kader kan elke proceseigenaar de voor zijn/haar proces relevant geachte informatiebeveiliging specificeren, inclusief de daarbij behorende maatregelen.

Historie van NEN 7510

NEN 7510 is gebaseerd op de in april 2005 gepubliceerde revisie van de Code voor Informatiebeveiliging. De Code voor Informatiebeveiliging is internationaal geaccepteerd als ISO/IEC 17799. In een verklaring van de voorzitters van NEN normcommissies 'Beveiligingstechnieken', 'Informatiebeveiliging in de zorg' en het Centraal College van Deskundigen - Informatiebeveiliging, wordt de relatie van de documenten beschreven.

Uitgangspunten NEN 7510

De kwaliteit van dienstverlening in de zorgsector is van groot belang, soms zelfs van levensbelang. Om patiënten het gewenste niveau van dienstverlening te kunnen bieden is het noodzakelijk dat zorgverleners op ieder moment over betrouwbare informatie kunnen beschikken. Tegelijk is het van belang dat gevoelige informatie niet in handen van ongeautoriseerde partijen valt om de privacy van de patiënt te beschermen.
De flexibiliteit van informatievoorziening en de beveiliging van de informatie lijken vaak met elkaar op gespannen voet te staan. De enige manier om tegelijkertijd de gewenste beveiliging en de noodzakelijke flexibiliteit in de informatievoorziening te kunnen bewerkstelligen, is om een afgewogen stelsel van beveiligingsmaatregelen te implementeren.
De complexiteit van informatiebeveiliging in de zorgsector wordt helemaal duidelijk als men kijkt naar het netwerk van zorgaanbieders, patiënten, zorgverzekeraars, overheidsinstanties en andere belanghebbenden die een rol spelen in het verzamelen, opslaan, verwerken en transporteren van informatie.
Het gezamenlijk gebruik van informatie door meerdere verschillende partijen, vraagt om standaarden voor informatie opslag, berichtopmaak, communicatieprotocollen, definities en codering van medische termen en, niet in de laatste plaats, informatiebeveiliging.

NEN 7511: Toetsbare Voorschriften

Na de publicatie van NEN 7510 in april 2004 heeft het ministerie van VWS (de directie Innovatie, Beroepen en Ethiek) aan NEN gevraagd het onderwerp ‘Informatiebeveiliging in de zorg’ daadkrachtig ter hand te nemen. Het ministerie wil er op toezien dat de toenemende (elektronische) gegevensuitwisseling goed en veilig functioneert. Zij is van plan om een verplicht karakter te geven aan de implementatie van de informatie-

beveiliging in iedere zorginstelling. In november 2005 zijn NEN 7511-1, -2 en -3 gepubliceerd als uitwerking van de algemene norm NEN 7510.

Resultaat

Onder de verantwoordelijkheid van de normcommissie 'Informatiebeveiliging in de Zorg' van NEN zijn drie toetsbare voorschriften opgesteld voor de hele zorgsector. Door naleving van de norm, in combinatie met een toetsbaar voorschrift, wordt voldaan aan passende beveiliging rondom het gebruik van het identificatienummer in de zorg. Volgens de regels die NEN gebruikt, zijn alle belanghebbende partijen bij dit proces betrokken.

Nut en noodzaak

De normcommissie heeft zorgorganisaties, die min of meer van dezelfde beveiligingsrichtlijnen gebruikmaken, ingedeeld in drie clusters. De informatievoorziening van een huisarts verschilt van die van een academisch ziekenhuis evenals de manier waarop zij hun beveiligingsproblemen oplossen. Voor de drie clusters zullen de te treffen maatregelen voor het waarborgen van informatiebeveiliging hierdoor ook wezenlijk van elkaar verschillen. De aanpak zou echter voor allen in beginsel hetzelfde kunnen zijn: richt je organisatie op een goede manier in en kijk daarbij goed naar de risico's die samenhangen met klanten, omgeving en eigen organisatie. De clusterindeling is als volgt:

1 Complexe organisaties zoals algemene ziekenhuizen, universitaire medische centra, gezondheidscentra, GGD- en GGZ-instellingen.
2 Samenwerkende organisaties zoals thuiszorginstellingen, verpleeghuizen, bloedbanken, ambulances en revalidatie-instellingen.
3 Solopraktijken zoals apothekers, alleen praktiserende en in samenwerkingsverband praktiserende huisartsen, fysiotherapeuten, psychiaters, psychologen en tandartsen.

IGZ 08-50; 500 exemplaren