STAATSTOEZICHT OP DE VOLKSGEZONDHEID

INSPECTIE VOOR DE GEZONDHEIDSZORG

www.igz.nl

RAPPORT

ICT in ziekenhuizen

Beveiliging van informatie nog onvoldoende voor een betrouwbare papierloze patiëntenzorg

Een inventariserend onderzoek bij twintig ziekenhuizen, uitgevoerd najaar 2003

Den Haag, augustus 2004

Inspecteur-Generaal

STAATSTOEZICHT OP DE VOLKSGEZONDHEID
INSPECTIE VOOR DE GEZONDHEIDSZORG

Aan de minister van Volksgezondheid, Welzijn en Sport,

Hierbij bied ik u het verslag aan van een onderzoek naar het gebruik van informatie- en communicatietechnologie (ICT) in ziekenhuizen. In twintig ziekenhuizen is onderzocht hoe ziekenhuizen invulling geven aan verantwoorde toepassing van ICT.

Steeds meer processen in de zorg zijn afhankelijk van het gebruik van ICT en ook in ziekenhuizen gaat het beeldscherm de plaats van het papier innemen. Het is bijna niet meer verantwoord om geen gebruik te maken van ICT. Nagenoeg alle ziekenhuizen staan aan de vooravond van een ziekenhuisbrede introductie van het elektronische patiëntendossier en op röntgenafdelingen wordt digitale opslag en verwerking van het beeldmateriaal de standaard. Ziekenhuizen schenken op dit moment echter nog onvoldoende aandacht aan de risico's die de toepassing van ICT met zich meebrengt.

Dit onderzoek bevestigt bevindingen uit de (inter)nationale literatuur, waaruit blijkt dat ICT zowel een bedreiging voor de kwaliteit van de zorg kan zijn als een bijdrage aan die kwaliteit kan leveren. De inspectie zal daarom meer aandacht aan ICT in de zorg schenken.

Ondanks alle voordelen van het gebruik van ICT – zoals de betrouwbare beschikbaarheid van informatie - loopt de patiënt hierdoor mogelijk onnodig gevaar. Ziekenhuizen moeten daarom meer aandacht geven aan het verantwoorde gebruik van ICT. Informatiebeveiliging is daarbij een belangrijk aandachtspunt. Een ander belangrijk aandachtspunt is het gebrek aan normen en standaarden. Ziekenhuizen vragen daar massaal om. Ik ben van mening dat het ministerie van VWS daar een belangrijker rol in moet vervullen.

Hoogachtend,

Prof. Dr. J.H. Kingma

Den Haag, augustus 2004

Samenvatting

Vanwege de kans dat onjuist en ondeskundig gebruik van informatie- en communicatie-technologie (ICT) de veiligheid van de patiënt in gevaar brengt, heeft de Inspectie voor de Gezondheidszorg onderzoek gedaan naar de voorwaarden waaronder ICT in de zorg wordt geïntroduceerd, toegepast en beheerd.

Het onderzoek betrof een thematisch onderzoek bij een steekproef onder de Nederlandse ziekenhuizen. In tien ziekenhuizen uit de groep van vijftig ziekenhuizen met het hoogste exploitatiebudget en in tien ziekenhuizen uit de groep van vijftig ziekenhuizen met het laagste exploitatiebudget is het onderzoek uitgevoerd.

Uit het onderzoek is gebleken 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. De bijna overal in gang gezette introductie van het elektronisch patiëntendossier vraagt om meer aandacht voor een betrouwbare beschikbaarheid van informatie. De normen voor beveiliging van informatie zullen daarom strak gevolgd moeten worden, anders is de toepassing van ICT niet meer veilig te noemen. Er zijn geen verschillen vastgesteld tussen grote en kleinere ziekenhuizen.

De inspectie zal in de toekomst systematischer aandacht schenken aan de veiligheid van de toepassing van ICT in de zorg, door het onderwerp op te nemen in het algemeen toezicht. Daartoe zullen ook op dit onderwerp meer prestatie-indicatoren worden ontwikkeld. Behalve in ziekenhuizen zal de inspectie ook in andere zorginstellingen aan de toepassing van ICT aandacht schenken. In 2005 zal nagegaan worden of in ziekenhuizen de 'NEN 7510 Informatiebeveiliging in de Zorg' norm wordt gevolgd.

Inhoudsopgave

1 Conclusies en aanbevelingen

Conclusies

Ziekenhuizen schenken op dit moment onvoldoende aandacht aan de risico's die de toepassing van ICT met zich meebrengt. De patiënt loopt hierdoor de kans op gevaar. Dat gevaar valt nu nog mee vanwege de beperkte toepassing van ICT, maar omdat door de bijna overal in gang gezette introductie van het elektronisch patiëntendossier binnen korte tijd de toepassing van ICT enorm zal zijn toegenomen, wordt dat gevaar aanzienlijk groter. In het onderzoek zijn geen duidelijke verschillen tussen de grotere en kleinere ziekenhuizen waargenomen.

Ook de beveiliging van de IC-applicaties en -apparatuur is onder de maat. De 'NEN 7510 Informatiebeveiliging in de Zorg' norm, die duidelijk aangeeft waar op gelet moet worden, wordt in ziekenhuizen niet systematisch nageleefd. De veiligheid van de informatie die in ziekenhuizen aanwezig is, wordt hierdoor bedreigd. Dat betreft niet alleen de beveiliging van de gegevens zodat onbevoegden er geen kennis van kunnen nemen, maar ook aanwezigheid van de gegevens op het juiste moment bij de juiste persoon. Of de gegevens op zich wel juist zijn (de integriteit van gegevens) is een onderwerp dat eveneens onder de beveiliging van gegevens valt, maar waar onvoldoende aandacht naar uitgaat.

De inhoud van de ICT-applicaties krijgt minder aandacht dan de technische kant. Dat komt onder meer doordat de technische aspecten, dat wil zeggen de apparatuur, de bekabeling en de netwerksoftware vallen onder de centraal gepositioneerde ICT-afdeling. De inhoudelijke kant, ook wel aangeduid met het gebruikersaspect, van de ICT-applicatie berust bij applicatiebeheerders die deel uitmaken van de zorgafdelingen. De verantwoordelijkheid en deskundigheid is daarmee versnipperd en wat betreft continuïteit bedreigd.

Behalve de bovenstaande conclusies zijn nog meer conclusies opgenomen bij de respectievelijke beschrijvingen van de bevindingen in hoofdstuk 3.

Aanbevelingen

De inspectie beveelt een aantal maatregelen aan die in het bijzonder gelden voor de ziekenhuizen, maar ook van toepassing kunnen zijn op andere zorginstellingen.

- Ziekenhuizen moeten zich bij elke applicatie systematisch afvragen wat de specifieke risico's voor de patiënt zijn. Risico's bij uitval, maar ook de risico's voor de betrouwbaarheid van de gegevens moeten in kaart gebracht worden en moeten leidend zijn voor de veiligheidsmaatregelen.
- Ziekenhuizen moeten de NEN 7510 norm voor de informatiebeveiliging in de zorg volgen.
- Bij de introductie van afdelingsspecifieke applicaties zal een strakkere centrale sturing noodzakelijk zijn dan nu in veel instellingen het geval is.
- Uit een duidelijke organisatiestructuur (voor de toepassing van ICT) met heldere verantwoordelijkheids- en bevoegdheidstoedelingen moet blijken dat deze past bij een integrale ondersteuning van het zorgproces.
- Ziekenhuizen die dat nu niet doen, moeten hun voornemens met betrekking tot ICT explicieter in beleidsplannen en werkplannen opnemen.
- (Bijna-)fouten en incidenten bij de toepassing van ICT moeten nauwgezet volgens een vastgestelde procedure geanalyseerd worden, zodat er maximaal van geleerd kan worden.

- Scholing van medewerkers bij de toepassing van ICT moet, net als bij de introductie ervan, systematisch blijven plaatsvinden.
- Instellingen die beheer en onderhoud decentraliseren, moeten centraal voor waarborgen zorgen dat beheer en onderhoud decentraal verantwoord gebeurt.

Voor de overheid is het volgende van belang.

- Standaardisatie bij de toepassing van ICT zal voortvarend ter hand genomen moeten worden. De inspectie is van mening dat door de traagheid waarmee de standaardisatie tot nu toe plaatsvindt, de overheid hierin het initiatief moet nemen.

De inspectie zal in de toekomst bij toezicht in ziekenhuizen aan deze onderwerpen meer aandacht schenken. Daarom zal de inspectie onderzoek instellen naar de mogelijkheid om meer prestatie-indicatoren te gebruiken op het gebied van ICT in de zorg. Niet alleen voor ziekenhuizen, maar ook voor andere instellingen voor de gezondheidszorg.

De inspectie zal in 2005 nagaan of de ziekenhuizen inmiddels de NEN 7510 norm voor informatiebeveiliging in de zorg volgen.

2 Inleiding

Regelmatig ondervinden patiënten risicovolle bijwerkingen door het gebruik van geneesmiddelen. Een belangrijk deel daarvan kan worden voorkomen door het gebruik van een elektronisch patiëntendossier. Maar informatiesystemen veroorzaken ook fouten. Patiënten krijgen de verkeerde medicijnen omdat de verpleegkundigen verkeerde informatie van de computer kregen. Ook is het bekend dat patiënten niet worden geopereerd omdat computers uitvallen.

Enerzijds is het bijna niet meer verantwoord om geen ICT te gebruiken, maar anderzijds kan de patiënt gevaar lopen wanneer er onvoldoende aandacht is voor de veiligheid van het gebruik daarvan.

Er is, zowel van de beleidsmakers als van het veld van de gezondheidszorg zelf, veel aandacht voor het gebruik van ICT. De betrouwbare beschikbaarheid van informatie kan – zo wordt gesteld - veel bijdragen aan de kwaliteit van zorg. Dit rapport bestrijdt dat niet, maar vraagt aandacht voor de risico's.

Waarom aandacht voor ICT?

Omdat er een kans is dat de patiënt schade ondervindt door het gebruik van ICT, besteedt de inspectie aandacht aan het onderwerp.

Voorbeelden van incidenten en problemen bij de toepassing van ICT zijn:
- Onjuist ingevoerde medische gegevens leiden tot herhaling van fouten.
- ICT-producten maken gebruik van verschillende terminologieën en codetabellen, waardoor informatie-uitwisseling onbetrouwbaar is.
- ICT-producten maken gebruik van verouderde codetabellen, waardoor registraties onjuist zijn.
- Verwisseling van gegevens van patiënten leidt tot het geven van medicatie aan een naamgenoot.
- De gebruiksinstructie van ICT-producten sluit niet aan bij de gebruiker(s), waardoor (herhalings-)fouten worden gemaakt.
- ICT-producten bevatten onjuiste of achterhaalde protocollen en/of rekenregels, waardoor uitkomsten onjuist worden geïnterpreteerd.
- Verwisseling van bloedgroepen met dodelijke afloop.
- Verkeerd voorschrijven vanwege het verkeerd aanklikken in een lijst op een computerscherm.
- Systemen met verschillende versies van diagnoseclassificaties.
- Wat wordt ondertekend: hetgeen op het scherm te zien is? Of dat wat in de database staat?
- Diefstal van de identiteit van een ander.
- Vernietigen van dossiers door bijvoorbeeld virussen.
- Problemen bij de bewijsbaarheid van handelen door niet-traceerbare gegevensmutaties.
- Het gebruik van autonome programma's (sofware agents) die zonder directe sturing gegevens zoeken en verwerken. Bijvoorbeeld: Autonomous Decision Support.
- Uitval van ICT-apparatuur veroorzaakt bijvoorbeeld verlies van gegevens, uitval van spreekuren, uitval van OK-programma's en verlies van digitale röntgenfoto's.

Normering[1] en standaardisatie[2] op het gebied van ICT in de zorg kent veel variatie. Normen en standaarden zijn te vinden in drie functionele groepen, te weten: proces-, product- en kwaliteitsnormen en -standaarden. Er is bijvoorbeeld geen duidelijke standaard waaruit blijkt dat bij bepaalde processen en bij bepaalde functies sprake moet zijn van de toepassing van ICT. Ook is niet vastgelegd welke product- en kwaliteitsnormen van toepassing zijn als men eenmaal overgaat tot de implementatie van ICT. Hoewel NICTIZ, (Nationaal ICT Instituut in de zorg), het NEN (Nederlands Normalisatie Instituut), CEN (Comité Européen de Normalisation), ISO (International Organisation for Standardisation) en HL7 (Health Level Seven, een standaard in de gezondheidszorg voor gegevensuitwisseling) vele inspanningen verrichten om tot normering en standaardisatie te komen, zijn deze pas over een zeer beperkt aantal onderwerpen ontwikkeld. Helaas zijn er voor die onderwerpen meer dan één standaard of zijn er standaarden die voor verschillende uitleg vatbaar zijn. ICT-leveranciers zijn bovendien geneigd om eigen productstandaarden te hanteren voor bescherming van intellectueel eigendom en marktaandeel. Dat leidt er toe dat er een grote diversiteit mogelijk is in de toepassing van ICT in de zorg, waardoor mogelijk gegevens niet uitgewisseld kunnen worden, men onvoldoende gebruik kan maken van producten die voldoen aan andere standaarden etc. Er is dan sprake van variatie in de mate waarin het gebruikt wordt als variatie in de wijze waarop.

Waarom NU aandacht voor ICT?

ICT wordt veel toegepast in de zorg. We staan evenwel aan de vooravond van een uitgebreide introductie van het elektronisch patiëntendossier, die gepaard zal gaan met een enorme toename van het elektronisch informatiebeheer en elektronische informatie-uitwisseling. Dat is niet alleen in ziekenhuizen, maar betreft zorginstellingen in het algemeen. Die toename van het belang van ICT is gekoppeld aan de verwachting dat:

- samenwerking tussen zorgaanbieders gaat toenemen en informatiedeling daarom nog meer noodzakelijk wordt;
- ICT positief bijdraagt aan de doelmatigheid en doeltreffendheid van de zorg wat betreft administratieve en zorginhoudelijke processen.

De ontwikkeling van ICT in ziekenhuizen kent al een lange historie met aanvankelijk meer aandacht voor de producten voor de ondersteuning van financieel beheer en logistiek. Veel meer dan tot nu toe het geval was, worden ICT-producten ontwikkeld, aangeboden en geïmplementeerd voor de ondersteuning van diagnostiek, behandeling en therapie.

De verwachte toename van ICT in de zorg dwingt tot noodzaak van het stellen van heldere toetsingscriteria voor het verantwoord toepassen van de ICT, zodat onacceptabele aantallen patiëntveiligheidsincidenten kunnen worden voorkomen.

Waar kijkt de inspectie naar?

Door de grote mate van variatie van de normen en standaarden op ICT-gebied en de variatie in de toepassing van ICT schenkt de inspectie in eerste instantie aandacht aan de voor-waarden die instellingen hanteren voor een verantwoorde toepassing van ICT.
In 1999 is ter voorbereiding op de millenniumwisseling door de inspectie veel aandacht besteed aan de veiligheid van apparatuur en software in de gezondheidszorg, gericht op het

[1] Norm: manier van handelen waarnaar een categorie van personen zich kan of moet richten, Van Dale, Groot Woordenboek Hedendaags Nederlands, versie 2.0, 2002.

[2] Standaardiseren: brengen tot een standaard of eenheid in afmeting, vorm, inhoud, samenstelling enz. Van Dale, Groot Woordenboek Hedendaags Nederlands, versie 2.0, 2002.

voorkomen van de zogenaamde milleniumbug. Het huidige onderzoek richt zich dus op een ander element van de toepassing van ICT. Dit onderzoek richt zich niet op specifieke problemen of calamiteiten. Indien daar sprake van is, volgt zonodig onderzoek door de inspectie. De *Leidraad onderzoek door de Inspectie voor de Gezondheidszorg naar aanleiding van meldingen* is dan het uitgangspunt.

Bij wie kijkt de inspectie?

Dit onderzoek van de inspectie is gericht geweest op ziekenhuizen. Ziekenhuizen zijn de meest complexe organisaties in de zorg met de meeste risico's voor de veiligheid van de patiënt.[3] Bovendien is de toepassing van ICT in ziekenhuizen ver gevorderd. Het instrument[4] dat in samenwerking met TNO is gebouwd, is evenwel toe te passen in iedere instelling voor de gezondheidszorg, dus ook bij een thuiszorgorganisatie en een instelling voor verstandelijk gehandicapten.

Wat wil de inspectie bereiken?

De inspectie wil een beeld krijgen van de mate waarin instellingen de randvoorwaarden voor verantwoorde toepassing van ICT invullen. Het is de eerste keer dat de inspectie een dergelijk onderzoek uitvoert. De criteria die de inspectie hanteert, zijn de algemene criteria die voortvloeien uit wetgeving zoals de Kwaliteitswet zorginstellingen, de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG) en de Wet op de geneeskundige behandelingsovereenkomst (WGBO). Daarnaast wil de inspectie bereiken dat instellingen deze criteria toepassen. Wat betreft privacywetgeving is deze beoordeeld voor zover deze van belang is in het kader van de Kwaliteitswet zorginstellingen. Voor beveiligingsaspecten wordt gerefereerd aan de concept NEN 7510 Informatiebeveiliging in de zorg norm.

In dit rapport wordt verslag gedaan van een onderzoek bij twintig ziekenhuizen. De gegevens die verkregen zijn bij deze ziekenhuizen, geven aanleiding een aantal conclusies te trekken en daarop aanbevelingen te doen.
Dit rapport is tevens te vinden op www.igz.nl.

---

[3] C.A. Baan, J.P.J.M. Smits, L.C.M. Limburg. *Risico's verkend : naar een risicomodel voor toezichtstrategie van IGZ.* Bilthoven : RIVM, 2001.

[4] A.C.M. Dumay en M. Schoone. *TICTZorg. Toetsing kwaliteit van ICT in de zorg.* TNO-rapport PG/TG/2003-032, 4 juli 2003.

3 Bevindingen

3.1 ICT-beheer : taken en verantwoordelijkheden goed vastleggen is vereist

Alle bezochte ziekenhuizen hebben een centrale ICT-afdeling. Daarnaast is in vrijwel alle ziekenhuizen de verantwoordelijkheid voor ICT-gebruik (het zogenaamde applicatiebeheer) gedelegeerd naar divisies, vakgroepen of afdelingen. Medewerkers met een zorginhoudelijke achtergrond hebben de taak van applicatiebeheerder gekregen. Zij vallen hiërarchisch onder het hoofd van een zorginhoudelijke afdeling. Ook in grote ziekenhuizen zijn de grote, relatief zelfstandige, decentrale organisaties (zorggroepen, divisies, afdelingen) door hun koppeling aan het centrale netwerk afhankelijk van een centraal automatiseringssysteem. Gegevens uit decentrale systemen worden geheel of ten dele getransporteerd, beheerd, verwerkt, bewerkt in de centrale netwerkstructuur. In alle ziekenhuizen is in de centrale organisatie de technologische kant van ICT geconcentreerd en daarmee beter geoutilleerd en gekwalificeerd ('professioneler'). Overigens hebben we ook ziekenhuizen gezien waar - naast de ICT-technici in de centrale organisatie - ook ICT-technici door de afdelingen in de decentrale organisatie werden aangesteld, zonder dat een relatie met de centrale ICT-afdeling geregeld was. Veel ziekenhuizen experimenteren met een elektronisch patiënten-dossier (EPD) als zijnde decentrale systemen. Waar dit gebeurt, komt het voor dat EPD's worden gebruikt zonder dat centrale standaardisatie aanwezig is, of wordt nagestreefd. Een enkele keer werd een ziekenhuis aangetroffen waar tussen de centrale ICT-afdeling en de decentrale applicatiebeheerders een gestructureerd contact was, met voor alle applicatie-beheerders geldende werkafspraken.

Tabel 1
Aspecten van centraal en decentraal beheer van ICT-producten

Centraal	*Decentraal*
Inkoop, beheer en onderhoud van centrale voorzieningen: computer server(s), intern datanetwerk, aansluiting(en) op extern datanetwerk(en).	Inkoop, beheer en onderhoud van specifieke, klinische ICT-producten: Afdelingsspecifiek EPD, zeer afdelingsspecifieke, soms zelf ontwikkelde systemen.
Primair verantwoordelijk voor technische installatie, beheer en onderhoud van de centrale communicatievoorzieningen.	Primair verantwoordelijk voor productkeuze en onderhoud van de zorgafdeling.

Conclusie en beoordeling

In veel ziekenhuizen is het beheer van ICT-toepassingen onvoldoende geborgd, omdat de verantwoordelijkheden niet duidelijk zijn vastgelegd.

3.2 Medische apparatuur is steeds vaker ook ICT-apparatuur

In de beginjaren van de automatisering was de verantwoordelijkheid voor ICT-gerelateerde aangelegenheden veelal ondergebracht in de bestaande organisatie bij bijvoorbeeld een instrumentele dienst of technische dienst. In de loop der jaren is in ziekenhuizen een structuur ontstaan waarbij deze verantwoordelijkheid meer en meer terecht is gekomen bij een centrale ICT-afdeling. De verantwoordelijkheid voor ICT-applicaties wordt nu vrijwel altijd verdeeld over deze ICT-afdeling en de instrumentele dienst. De netwerkgerelateerde applicaties vallen dan onder de verantwoordelijkheid van de ICT-afdeling, de medische apparatuur gebonden applicaties onder verantwoordelijkheid van de afdeling medische technologie of afdeling instrumentele dienst.

De verantwoordelijkheid voor ICT-producten in apparatuur die gekoppeld (moeten) worden en data uitwisselen via het centrale computernetwerk, is niet altijd duidelijk. Door de technologische ontwikkeling is de scheiding tussen de centrale ICT-afdeling en de afdeling medische technologie steeds meer aan het verdwijnen. De organisatiestructuur is daar nog niet altijd aan aangepast.

Tabel 2
Aspecten van beheer van het netwerk en medische apparatuur

Netwerkbeheer/centrale ICT-afdeling	*Beheer medische apparatuur/afdeling medische technologie*
Beheer en onderhoud van netwerk(en).	Beheer en onderhoud van medische hulpmiddelen.
Weinig contact met medische afdelingen.	Veel contact met medische afdelingen.
Krijgt te maken met afdelingsspecifieke applicaties.	Krijgt te maken met computernetwerken.
Zwaartepunt techniek	Zwaartepunt inhoud

Conclusie en beoordeling

Het vóórkomen van instrumentele diensten die hulpmiddelen beheren waaraan software gekoppeld is (een groot aantal apparaten kan alleen maar werken met software; de apparatuur wordt door software bestuurd), naast de ICT-afdelingen die netwerken beheren waarop de hulpmiddelen worden aangesloten, is een risico nu niet helder is welke taken en verantwoordelijkheden er zijn voor elk van de afdelingen.

3.3 Optimaal ICT-beheer vraagt uniforme omgang en afstemming tussen inhoud en techniek

ICT-afdelingen hebben over het algemeen geen kennis over de informatiebehoefte van de medewerkers die de applicatie gebruiken. De kennis die zij hebben, gaat voornamelijk over de technische aspecten van ICT. De reden om te automatiseren is vaak ingegeven om informatie te kunnen beheren en deze gemakkelijker toegankelijk te hebben. De keuze voor

automatisering en de keuze van de meest gewenste applicatie is, behalve wanneer het om de technische aspecten gaat, een zaak van de zorginhoudelijke afdelingen. Deskundigheid op het gebied van te automatiseren informatie is om die reden verspreid over afdelingen en slechts bij enkelen aanwezig. De deskundigheid over de techniek daarentegen is geconcentreerd in de ICT-afdeling en vaak bij alle ICT-medewerkers in hoge mate aanwezig. In vrijwel alle ziekenhuizen is een functie gegroeid van applicatiebeheerder die ook wel key-user of super-user wordt genoemd. Deze is verantwoordelijk voor het beheren van de inhoud van 'zijn/haar' applicatie. Deze functionaris is ook verantwoordelijk voor het bewaken dat de applicatie die inhoud bevat die andere gebruikers noodzakelijk achten. De functie van de applicatiebeheerder is niet altijd omschreven. De functie staat onder het management van een zorgeenheid. De ICT-afdeling is vaak niet of alleen informeel betrokken bij het evalueren van het functioneren van de applicatiebeheerder. Als dit niet gebeurt, is het vrijwel altijd de wens van het hoofd ICT om wel bij deze beoordeling betrokken te zijn.

Tabel 3
Aspecten van beheer van inhoud en techniek

Informatiebeheer	*Technisch beheer*
Verantwoordelijkheid applicatiebeheerder.	Organisatorisch geborgd in ICT-afdeling.
Verspreid over afdelingen bij zorginhoudelijke medewerkers met daardoor spreiding van kennis en ervaring. Semi-professioneel op ICT-gebied.	Geconcentreerd in ICT-afdeling met veel kennis en ervaring. Professioneel.
Functieprofiel niet duidelijk.	Functieprofiel wel duidelijk.
Hiërarchisch in zorglijn	Hiërarchisch in facilitaire lijn.

Conclusie en beoordeling

Er is een scheiding aangebracht in het technisch beheer en het inhoudelijk beheer van applicaties, die terug te vinden is in de verantwoordelijkheden daarvoor. Door enerzijds het technisch beheer te concentreren bij de ICT-afdeling en anderzijds het inhoudelijk beheer te spreiden over de zorginhoudelijke afdelingen ontstaan bedreigingen voor optimale afstemming en uniforme omgang met de ICT.

3.4 Zorgondersteunende ICT-toepassingen hebben geen achterstand meer ten opzichte van administratieve ICT-toepassingen

Automatisering van administratieve functies is in ziekenhuizen eerder ter hand genomen dan de automatisering die een directe relatie heeft met het zorginhoudelijke proces. Door de aard van de administratieve applicaties overheersen deze nu nog op het ICT-netwerk. Het betreft veelal patiëntenlogistiek, beheer- en financiële administraties. De risico's die deze applicaties met zich meebrengen voor de veiligheid van de patiënt, zijn gering ingeschat. Daarnaast worden deze functies omdat ze netwerkgebonden zijn over het algemeen professioneler ondersteund. Zorgondersteunende toepassingen krijgen echter in toenemende

mate meer aandacht en zullen in de komende jaren een belangrijke rol gaan spelen. Met name de introductie van het EPD die in bijna alle ziekenhuizen aan de gang is of op het punt staat te beginnen, zal zeer veel veranderingen met zich meebrengen.

Tabel 4
Aspecten van administratieve en zorgondersteunende toepassingen

Administratieve ICT-toepassingen	*Zorgondersteunende ICT-toepassingen*
Lage risicoklasse.	Hoge risicoklasse.
Niet zorggebonden.	Primair zorggebonden.
Professioneel beheer en onderhoud.	Onduidelijker beheer en onderhoud.
Risico's bekend en geborgd.	Risico's vaak niet bekend en dus niet geborgd.
Geen relatie met afdeling medische instrumentele dienst.	Goede relatie met afdeling medische instrumentele dienst.

Conclusie en beoordeling

Er zijn concluderend drie onderdelen zichtbaar in de organisatie van ICT: de centrale ICT-afdeling, de afdeling, divisie c.q. vakgroep en de afdeling medische instrumentele dienst. Samenwerking tussen de drie onderdelen is het meest frequent geborgd tussen ICT-afdeling en afdeling medische Instrumentele dienst. Coördinatie tussen centrale ICT-afdeling en zorgafdeling/divisie/vakgroep ICT ontbreekt soms geheel. Deze verschillen en systematisch andere coördinatie dragen er toe bij dat de veiligheid van het zorgproces onder druk komt te staan wanneer afdelingen/divisie/vakgroep een autonome weg gaan.

3.5 Medische staf maakt geen deel uit van de stuurgroep ICT, individuele specialisten wel

Vanwege het belang dat ICT inmiddels in ziekenhuizen heeft, zowel vanwege de behoefte om processen, administratief, financieel en nu ook zorginhoudelijk te ondersteunen, maar ook omdat ICT veel investeringen met zich meebrengt, hecht men veel belang aan een breed gedragen oordeelsvorming rond ICT. Om die reden hebben nagenoeg alle ziekenhuizen een stuurgroep ingesteld. Deze is meestal samengesteld uit een vertegenwoordiging vanuit de Raad van Bestuur of directie, vanuit de ICT-afdeling, vanuit de zorgafdelingen en vanuit de afdeling inkoop. De taak van de stuurgroep is doorgaans om de Raad van Bestuur of directie in belangrijke beslissingen te adviseren. In de stuurgroep nemen meestal ook één of twee specialisten deel, echter niet als vertegenwoordiger van de medische staf. Het betreft vrijwel altijd specialisten (specialisten van een specifieke afdeling zoals een apotheker of een klinisch chemicus of een medisch specialist zoals een radioloog of een chirurg) die deskundig zijn in het toepassen van ICT in hun zorgproces. De deelname van deze specialisten garandeert echter geen commitment van de medische staf.
In het onderzoek is gebleken dat de Raad van Bestuur of de directies nauw betrokken zijn bij de ontwikkelingen op het gebied van ICT in hun ziekenhuis. ICT wordt door hen gezien als

een strategisch belangrijk onderdeel. Dit kan inhouden dat voorheen vooral operationeel denkende ICT-afdelingen soms geconfronteerd worden met de noodzaak van het ontwikkelen van een strategische visie.

Conclusie en beoordeling

Centrale stuurgroepen ICT functioneren redelijk tot goed. Inhoudelijke inbreng van de medische staf is evenwel onvoldoende gewaarborgd door het slechts afvaardigen van enthousiaste, individueel geinteresseerde professionals in een stuurgroep ICT zonder een adequaat mandaat.

3.6 Visie en beleidsvorming op het gebied van ICT onvoldoende

In twee van de onderzochte ziekenhuizen was geen beleids- of visiedocument waaruit afgeleid kon worden op basis waarvan men de automatisering in het ziekenhuis ontwikkelt en stuurt. In acht ziekenhuizen was er wel een document, maar betrof dat vaak een verouderd document of bevatte dat slechts in zeer algemene bewoordingen een aantal opmerkingen over ICT. In de andere tien ziekenhuizen was er dus wel een beleid geformuleerd waaruit duidelijk kon worden afgeleid welke plannen er zijn om in het ziekenhuis tot een samenhangend gebruik van ICT te komen.

Conclusie en beoordeling

Op een terrein waar voor de kwaliteit en veiligheid van zorg zoveel essentiële ontwikkelingen plaatsvinden, dient het ziekenhuis expliciet te zijn in de plannen die ze op dat terrein hebben en willen realiseren. Een visie en beleid op dat terrein moet op zijn minst blijken uit een daarover opgesteld document. Door visie en beleid niet te expliciteren, dreigt een ad-hoc beleid met kans op onjuiste beslissingen met negatieve gevolgen voor de kwaliteit en veiligheid van zorg.

3.7 ICT-investeringen: kosten van ICT moeilijk te plaatsen

ICT is kostbaar. De indruk heeft lange tijd bestaan dat ziekenhuizen achterbleven in automatisering omdat de kosten te hoog zijn en deze niet uit het reguliere budget gefinancierd konden worden. In vergelijking met andere dienstverlenende sectoren in de maatschappij zouden ziekenhuizen zeer ver achterlopen. Om een indruk te krijgen in het aandeel van de ICT in het budget van het ziekenhuis is tijdens het interview gevraagd welk percentage van het budget gereserveerd wordt voor ICT. De door de directies geschatte range van percentages loopt van 2,5 tot 4 procent. In alle gevallen wordt gemeld dat een goede definitie van het budgetaandeel ontbreekt. In sommige gevallen is het percentage opgegeven zonder dat bijvoorbeeld de kosten van het in dat jaar geïmplementeerde Picture Archiving and Communication System (PACS) in het getal is betrokken. Op een mediaan ziekenhuisbudget van 76 miljoen euro is een dergelijke investering ongeveer 2,3 miljoen euro per ziekenhuis. Investeringen die plaatsvinden voor nieuwe applicaties brengen vaak extra onderhoud mee aan bestaande applicaties. Een duidelijk onderscheid tussen het aandeel in de investeringsbegroting en het aandeel in de exploitatiebegroting is daardoor niet te geven.

Conclusie en beoordeling

Nadrukkelijk wordt geen oordeel gegeven over de mate waarin ziekenhuizen hun financiële middelen toebedelen aan ICT. Wel moet duidelijk zijn dat de kosten gemaakt worden op

basis van verantwoorde keuzen. Het moet duidelijk zijn waar keuzen toe leiden. Dat kan alleen wanneer er een goed inzicht is in de consequenties van de keuzen. De continuïteit van het zorgproces wordt bedreigd indien dat inzicht er niet is. Door een toename van transmurale inzet van ICT is dat inzicht nog meer noodzakelijk. Zonder inzicht kan er verspilling van middelen ontstaan.

3.8 Applicaties, aard en aantal: ieder voor zich

In het onderzoek is gevraagd welke applicaties in het ziekenhuis in gebruik zijn en welke applicaties binnenkort in gebruik genomen zullen worden. Op dit moment bestaat er geen opsomming (norm, standaard) welke applicaties er wel en niet aanwezig zouden moeten zijn in een ziekenhuis. Er zijn taken (waaronder informatie verzamelen en verwerken) die met ICT sneller, betrouwbaarder, 'reproduceerbaarder', etc. uitgevoerd kunnen worden. Mits goed geïmplementeerd draagt ICT bij aan doeltreffendheid en doelmatigheid van de zorg. Dat zijn belangrijke kenmerken van verantwoorde zorg. Zoals medische beroepsgroepen bepaalde diagnose- en behandelprotocollen niet meer gebruiken omdat er doelmatiger protocollen voorhanden zijn, worden ook bepaalde applicaties en technologie niet meer gebruikt en vervangen door nieuwe. De 'norm' is dan datgene dat 'state of the art' is. Kenmerkend voor de toepassing van ICT is dat bijna ieder ziekenhuis de applicatie heeft toegesneden en aangepast op de eigen situatie. Daardoor is niet één ziekenhuis vergelijkbaar met de ander wat betreft de toepassing van individuele applicaties.

Over het geheel genomen laat het onderzoek een vergroting van de rol van ICT in het zorgproces zien. Die vergroting is het duidelijkst op twee gebieden, de reeds genoemde radiologische PACS-systemen en in mindere mate de Elektronische Patiënten Dossiers (EPD). In beide gevallen gaat het om vervanging van een 'harde' gegevensdrager door een digitale. Daarbij wordt de toegankelijkheid van de informatie nadrukkelijk verbeterd, maar er ontstaan geen nieuwe databronnen. Van belang is eveneens de invloed van alle medische apparatuur die steeds meer door middel van software met elkaar kan communiceren en op den duur ook gekoppeld zal worden aan EPD, bewakingssystemen en dergelijke.

Naast het verder doordringen van ICT in het primaire zorgproces wordt in meerdere ziekenhuizen gemeld dat de noodzaak om een goed registratiesysteem voor Diagnose Behandel Combinaties (DBC) te hebben, heeft geleid tot een duidelijke verhoging van de informatiseringsgraad in het ziekenhuis. Opvallend is dat het bij ontwikkeling van administratieve applicaties vrijwel altijd gaat om het moderniseren van al bestaande applicaties. Zorggerichte applicaties zijn vaak nieuw of ondergaan een zo drastische wijziging of uitbreiding dat zij dé facto nieuw zijn.

Internet- en e-mail-toepassingen zijn gemeengoed geworden in Nederlandse ziekenhuizen. Opmerkelijk genoeg wordt daarvoor in ongeveer 50 procent van de ziekenhuizen de motivatie gegeven dat e-mail een betere waarborg geeft voor veilig dataverkeer tussen huiscomputers en het ziekenhuisnetwerk dan floppy's en datapennen, omdat dan betere virusscanning mogelijk is.

Conclusie en beoordeling

De hoeveelheid, aard en samenstelling van applicaties in ziekenhuizen verschilt enorm. Er wordt veel maatwerk geregeld voor de applicaties. Een benchmark met als onderwerp ICT-applicaties in het ziekenhuis ontbreekt. Een dergelijke benchmark zou helpen te bepalen wat tot 'the state of the art' behoort.

3.9 ICT en transmurale gegevensuitwisseling zeer beperkt

Veel ziekenhuizen hebben contact met omringende zorginstellingen en hulpverleners over communicatie met behulp van ICT. Deze ontwikkeling is al lange tijd geleden in gang gezet en beperkt zich in veel gevallen nog tot communicatie over opname- en ontslaggegevens en over laboratoriumgegevens. Een daadwerkelijke toename zou te verwachten zijn nu koppelingen gemakkelijker worden en internettechnologie geïntroduceerd wordt. Bij de samenwerking op ICT-gebied is bijna altijd sprake van dienstverlening van ziekenhuizen aan die omringende zorgverleners. Deze eenzijdige inzet van mensen en middelen werkt niet bevorderend op de totstandkoming van samenwerking. Een belangrijker belemmerende factor wordt genoemd de diversiteit aan automatisering die buiten het ziekenhuis te vinden is. Huisartsen hebben geen uniform systeem waardoor elektronisch communiceren met hen vele technische maar ook emotionele en politieke hobbels kent. Keuzen hierin komen maar moeizaam tot stand, want de keuze voor de een betekent de uitsluiting (en dus noodzaak tot technische aanpassing) van de ander. Vanuit de ziekenhuizen werd meerdere malen op dit terrein om het afdwingen/forceren van standaardisatie door een onafhankelijke partij als de overheid verzocht.

3.10 Risicomanagement onder de maat

Risicomanagement is het geheel van activiteiten gericht op het in kaart brengen van mogelijke risico's, deze beheersen wanneer ze er zijn en ze wegnemen. De eerste aandacht moet vanzelfsprekend uitgaan naar ontwikkeling van zorgsystemen (zorg plus techniek) die zoveel mogelijk vrij zijn van risico's.

De situatie is dat technische risico's, leidend tot totale uitval van het systeem, over het algemeen goed worden opgevangen. Hiervoor zijn noodprocedures beschikbaar die vaak voldoende geoefend worden, meestal tijdens geplande uitval van een systeem voor groot onderhoud. Op dit gebied zijn goede afspraken gemaakt, ook in de vorm van service level agreements (SLA) als de opvang hiervan deels is uitbesteed. SLA's worden per applicatie afgesloten met de leverancier. Het ziekenhuis kent doorgaans meer dan één leverancier. Een klassiek probleem is dat individuele SLA's voldoen, maar de combinatie van SLA's met meer leveranciers niet. Raakvlakken tussen systemen zijn per definitie zwakke plakken. In kritische situaties kan daardoor verantwoordelijkheid worden afgeschoven.

Op sommige plaatsen bestaat ongerustheid over de opvang van de uitval van stroom. Dit betreft dan vooral de kleinere, vaak afdelingsgebonden informatiesystemen. Afdelingssystemen bevatten doorgaans vooral de medische informatie. De risico's verbonden aan dit soort systemen zijn bij acute uitval veel groter dan de risico's van beschikbaarheid van logistieke of financiële informatie die meestal centraal is opgeslagen. Sommige centrale systemen kennen een onzekerheid omdat de noodstroomvoorziening bestaat uit een centrale die zelf stroom levert aan het elektriciteitsnet. Het is dan namelijk niet duidelijk of deze bestand is tegen een energiecrisis zoals zich recent voordeed in de Verenigde Staten.

Als het terugvallen op papier niet mogelijk is, worden systemen meervoudig uitgevoerd, in gescheiden ruimtes ondergebracht en wordt continuïteit van verbindingen zo goed als mogelijk is gewaarborgd. Criteria voor redundantie ontbreken. Dit leidt soms tot problemen bij het rechtvaardigen van de grote investeringen die met het redundant uitvoeren gepaard gaan. Continuïteit van ondersteuning bij het uitvallen van het systeem zijn voldoende gewaarborgd gebleken. Van de instabiele systeemdelen waarvan de effecten niet direct bij gebruik merkbaar zijn, kan dat niet gezegd worden omdat men niet weet wat moet worden

gecontinueerd of op welke wijze fouten doorwerken. Het is dus belangrijk dat er een risicoanalyse is om risico's te beperken van uitval en keuzes te maken voor vitale systemen die moeten blijven werken.

Een lacune is het ontbreken van analyses van risico's in het softwarematige/inhoudelijke deel van het systeem. Als er al risico's worden geïdentificeerd, wordt er vanuit gegaan dat deze voldoende te ondervangen zijn tijdens de testfase van het systeem. Een permanente aandacht voor de mogelijkheid dat gegevensbestanden niet met elkaar overeen zouden kunnen komen, ontbreekt.

Problemen die ontstaan bij het werken met ICT-applicaties worden doorgaans neergelegd bij een helpdesk. Ieder ziekenhuis beschikt over een helpdeskfunctie. Ze verschillen wel in de mate waarin de informatie bij een helpdesk wordt verzameld en geanalyseerd ten behoeve van de sturing van activiteiten. Het systematisch verzamelen, aggregeren en analyseren van de meldingen vindt slechts bij een enkel ziekenhuis plaats. Alle ziekenhuizen geven aan dat alleen wanneer patiënten schade hebben ondervonden van het probleem in de ICT-applicatie een melding zal plaatsvinden bij de zogenaamde commissie Melding Incidenten Patiëntenzorg. Deze commissie wordt geacht de melding te onderzoeken en aanbevelingen te doen aan de directie/Raad van Bestuur. Zelden krijgen applicatiebeheerders een overzicht van de over hun systeem gedane meldingen.

Conclusie en beoordeling

Doordat er vrijwel geen systematische risicoanalyse van de ICT-applicaties is gedaan gericht op de veiligheid voor de patiënt bestaat het gevaar dat risico's niet worden herkend, met alle mogelijke gevolgen voor de patiënt.
Omdat steeds meer ICT-applicaties rechtstreeks met de zorg voor de patiënt te maken zullen hebben, zullen ziekenhuizen zich bij elke applicatie af moeten vragen wat de specifieke risico's voor de patiënt zijn. Risico's bij uitval, maar ook de risico's voor de betrouwbaarheid van de gegevens moeten in kaart gebracht worden en moeten leidend zijn voor de veiligheidsmaatregelen.

Noodprocedures voldoen over het algemeen wel omdat er op dit moment vrij gemakkelijk overgegaan kan worden op de (oude) papieren situatie. In de toekomst zal bij iedere nieuwe applicatie nadrukkelijk de te hanteren noodprocedure onderdeel moeten zijn van de implementatie.

Ziekenhuizen maken onvoldoende gebruik van signalen die er op wijzen dat systemen niet goed functioneren. Dat komt niet omdat de helpdesk niet goed zou functioneren, maar omdat de informatie die de helpdesk verzamelt niet systematisch gebruikt wordt als informatie voor het management om beleid en operationeel functioneren bij te stellen. Dit is des te meer van belang omdat alleen wanneer er echt patiëntschade is de MIP-commissie wordt ingezet en een analyse van de oorzaak (root cause analysis) plaatsvindt. Veel problemen of fouten in het gebruik kunnen potentieel schade voor de patiënt betekenen, maar worden omdat ze die schade niet veroorzaakten, alleen aan de helpdesk gemeld. Een gedegen analyse blijft dan uit. Veel van die fouten worden vervolgens niet aan de applicatiebeheerder doorgegeven. De helpdesk-medewerker kan niet altijd inschatten of de fout behalve technische kanten ook gevolgen voor een patiënt gehad heeft.
Ziekenhuizen moeten incidenten en fouten systematisch analyseren om risico's voor de veiligheid van de patiënt in kaart te brengen, te analyseren en om ze weg te kunnen nemen.

3.11 Aanschafbeleid: kwetsbaar op een kleine markt

Wanneer een ziekenhuis een nieuwe applicatie aanschaft, handelt men in het overgrote deel van de gevallen zorgvuldig. Nieuwe automatiseringssystemen zijn erg kostbaar en nemen een steeds groter aandeel in van de investeringsbegroting. Op dit moment staat de aanschaf van ICT-applicaties zo hoog op de agenda, dat ze soms voor investeringen in apparatuur voor specifieke medische verrichtingen gaan. In nagenoeg ieder ziekenhuis werkt men ten behoeve van de aanschaf van nieuwe systemen met projectteams. Er zijn verschillende standaard projectmethoden die worden ingezet. De projectteams kennen een logische samenstelling van gebruikers en technici. Ervaren werd dat de technici altijd het voordeel hebben van een continue betrokkenheid bij automatisering, terwijl de gebruikers maar een enkele keer betrokken zijn bij de aanschaf van een nieuw systeem en zich geheel in de materie moet inleven. Het gevaar hiervan is dat de inhoud van de applicatie, eigenlijk daar waar het om gaat, ondergesneeuwd raakt onder de techniek.
Ook is nagenoeg standaard dat men in de afwegingen om tot een nieuwe aanschaffing over te gaan, nagaat wat de betrouwbaarheid van de leverancier is. Zonder uitzondering gaf men aan moeite te hebben met de keuzemogelijkheden die er zijn. Ze zijn beperkt en men voelt zich al snel gedwongen tot de keuze voor een bepaald systeem omdat de markt niet veel meer te bieden heeft. Steeds meer zoekt men contact met andere instellingen om gezamenlijke keuzen te maken of om als gebruikers meer gewicht te kunnen bieden tegen de leveranciers. Ook werd als een beperking ervaren dat de keuze voor één bepaald systeem veelal inhoudt dat men niet meer kan wijzigen en voor vele jaren aan dat systeem of de leverancier vastzit.
Als beperkende factor bij de keuze voor een bepaald systeem is het ontbreken van standaarden vaak genoemd. Meerdere malen werd uitgesproken dat er van overheidswege standaarden gesteld zouden moeten worden voor de automatisering of voor de leveranciers in de gezondheidszorg.
Een gunstige uitzondering is de ontwikkeling bij de PACS-systemen. Hierbij is er wel een duidelijke standaard, namelijk DICOM (Digital Imaging and Communications in Medicine, ooit een initiatief van the American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA)).

Conclusie en beoordeling

Ziekenhuizen zijn zorgvuldig in hun aanschafbeleid van ICT-producten, maar zijn overgeleverd aan een zeer monopolistische en zeer kleine markt. Daardoor zijn de afnemers kwetsbaar. Door het ontbreken van standaarden in techniek en inhoud is die kwetsbaarheid eigenlijk onaanvaardbaar groot. Instellingen kunnen buiten hun schuld om met een uiteindelijk onacceptabel product komen te zitten. De veiligheid van de patiënt loopt hierdoor gevaar. Immers, de afhankelijkheid van de ICT in de zorgprocessen neemt toe en daarmee de zekerheid dat de continuïteit gegarandeerd is ook.
Behalve dat ziekenhuizen actief moeten zijn in het zoeken van informatie, steun en begeleiding bij andere instellingen bijvoorbeeld in de vorm van gebruikersgroepen of verenigingen, moet meer aandacht uitgaan naar de totstandkoming van standaarden. Het NICTIZ kan daar een belangrijke rol in spelen.

3.12 Installatiebeleid: goed, scholing kan beter

Risico-analyse, acceptatietests, -protocollen, testverslagen, gebruikersopleiding en -training, gebruikerstevredenheidsonderzoek zouden alle deel uit moeten maken van een zorgvuldig installatie- en beheersbeleid. Slechts een enkel ziekenhuis doet dat systematisch,

consequent en geprotocolleerd. Vanwege financiële beperkingen kan het niet altijd en overal gerealiseerd worden. Meerdere ziekenhuizen voeren een test van een nieuwe applicatie uit in een zo goed mogelijk nagebootste reële situatie alvorens de applicatie geoperationaliseerd wordt. Dat is nodig ook. Gebleken is dat, zelfs bij applicaties die elders al in gebruik zijn, in nieuwe omgevingen andere ernstige problemen op kunnen treden met gevaren voor de patiënt. De implementatie van de applicatie onder de gebruikers is weer iets dat men overlaat aan de applicatiebeheerders. Omdat deze niet onder de ICT-afdeling vallen, zijn verschillen in de wijze van implementeren waar te nemen. Zo is scholing bij een nieuwe applicatie niet een systematische activiteit die gestandaardiseerd en verplicht gesteld is.

Conclusie en beoordeling

Alhoewel er tekortkomingen zijn geconstateerd, gebeurt het technisch installeren van nieuwe systemen en applicaties in het algemeen verantwoord. Aan een systematische scholing van medewerkers op de afdeling in de gehele levenscyclus van de applicatie moet echter meer aandacht worden geschonken. Vanwege diversiteit in de scholing van de verschillende applicaties die daardoor voor sommige applicaties lacunair is, is centrale sturing vanuit het ziekenhuismanagement noodzakelijk.

3.13 Beheers- en onderhoudsbeleid: versnipperd

Ook op dit aspect is het verschil tussen centraal en decentraal goed te zien. De centrale ICT-afdeling heeft doorgaans een goed beleid met betrekking tot beheer en onderhoud. Zij zijn precies op de hoogte van wat er op netwerken aanwezig is. Het is anders gesteld met kleinere systemen of stand alone situaties. (stand alone applicaties gekoppeld aan medische apparatuur is onderdeel van het beheerssysteem van de instrumentele diensten en vaak uitbesteed aan de fabrikant). Daarbij kom het voor dat de ICT-afdeling deze niet kent. Het betreft hier vooral de technische aspecten. De applicaties op zich en zeker wanneer het zorgafdelingsspecifieke applicaties betreft, hebben hun beheer en onderhoud buiten de automatiseringsafdeling. Per applicatie zijn er vrijwel overal applicatiebeheerders. Zij zijn meestal belast met het applicatiebeheer naast hun reguliere zorginhoudelijke of administratieve functie. De applicatiebeheerder op een zorgafdeling is meestal een verpleegkundige. Zo systematisch als het beheer en onderhoud op technisch vlak is, zo vrijblijvend is dat met het applicatiebeheer en onderhoud op inhoudelijk vlak het geval. Het wordt aan de gebruikers van de applicatie overgelaten wat zij aan onderhoud willen. Aan het gegeven dat lokale applicaties die op het netwerk draaien ook effecten op het functioneren van het hele netwerk kunnen hebben, werd geen aandacht geschonken.

Conclusie en beoordeling

Door het onderhoud van applicaties te decentraliseren naar afdelingen ontstaat het risico dat deze applicaties niet systematisch worden onderhouden. Het netwerk waar deze applicaties op draaien, loopt daardoor het gevaar niet te kunnen functioneren waardoor patiënten op hun beurt het risico lopen in hun veiligheid bedreigd te zijn. Wanneer instellingen beheer en onderhoud decentraliseren, moet er centraal een waarborg zijn dat beheer en onderhoud decentraal verantwoord gebeurt. De centrale ICT-afdeling zou hiervoor eisen kunnen stellen.

3.14 Beveiliging: heeft veel aandacht nodig

Zowel de apparatuur als de informatie in ziekenhuizen moet beveiligd zijn. Beveiligd tegen uitval, maar ook tegen verkeerd gebruik, onjuiste weergave en opslag. De gegevens die opgeslagen zijn, moeten betrouwbaar en op het juiste moment in de goede vorm beschikbaar zijn. Ook mogen geen mensen bij de gegevens kunnen komen die niet voor hen bestemd zijn. Om dat te bewerkstelligen moeten ziekenhuizen een plan hebben hoe ze dat willen verwezenlijken. Er zijn, specifiek voor de zorg, normen ontwikkeld voor beveiliging van informatie, de NEN 7510 Informatiebeveiliging in de Zorg[5]. De norm is nog niet formeel vastgesteld maar in conceptvorm in 2002 ruim gepresenteerd aan het veld. Daarmee is de NEN 7510 norm het houvast voor ziekenhuizen om het beveiligingsbeleid vorm te geven. In het onderzoek is dan ook gevraagd naar een norm die gehanteerd wordt bij het beveiligingsbeleid. Niet één ziekenhuis had de NEN 7510 norm als norm al volledig geïmplementeerd in het beveiligingsbeleid. Hoewel ieder ziekenhuis had nagedacht over beveiliging was opvallend hoe weinig systematisch en hoe onsamenhangend dat gebeurde. Men kon de NEN 7510 norm wel noemen, maar deze was slechts in een enkel geval het richtsnoer om de beveiliging vorm te gaan geven. Dat leidt er toe dat in sommige ziekenhuizen veel aandacht uitgaat naar de fysieke beveiliging van apparatuur en middelen om te voorkomen dat deze gestolen wordt, terwijl andere weer veel aandacht schenken aan het voorkomen van onbevoegd raadplegen van gegevens. Een enkel ziekenhuis laat zijn externe beveiliging toetsen door legal hackers of laat een electronic data protection (EDP) audit uitvoeren.

Conclusie en beoordeling

Het informatiebeveiligingsbeleid in ziekenhuizen kan veel beter nu er een norm voor de informatiebeveiliging in de zorg is geformuleerd. Ziekenhuizen moeten daarom alle deze norm volgen.

3.15 Privacybescherming nodig, maar lastig te realiseren

De beveiliging van de persoons- en persoonlijke gegevens van patiënten moet in een ziekenhuis natuurlijk veel aandacht krijgen. De gegevens mogen niet zomaar door anderen worden ingezien en er moeten garanties gegeven kunnen worden aan patiënten dat de gegevens alleen maar gebruikt worden voor het doel waarvoor ze zijn opgeslagen. In veel ziekenhuizen kwam als reactie op vragen over privacy dat de huidige wetgeving over de persoonsregistratie belemmerende effecten heeft op een goed toegankelijk zijn van die gegevens. De ziekenhuizen gaven aan dat artsen en verpleegkundigen op vele plaatsen over de gegevens van de patiënten, die zij in zorg hebben, moeten kunnen beschikken. Dat geeft problemen wanneer voor het raadplegen van die gegevens telkens kenbaar gemaakt moet worden wie de raadpleger is en waarom hij de gegevens wil raadplegen. Veel ziekenhuizen gaan om die reden wisselend om met het daadwerkelijk afsluiten van gegevensbestanden voor onbevoegden. Hoewel het gebruik van log-in codes algemeen is, wordt - een uitzondering daargelaten - het gegevensbestand niet direct afgesloten wanneer de raadpleger er een aantal minuten geen gebruik van maakt. Groepsaccounts komen frequent voor, juist op verpleegafdelingen, waardoor geautoriseerde toegang tot gegevens een farce is. Ook wordt niet systematisch het raadplegen van gegevens geregistreerd (het zogenaamde log-filing). Als excuus dan wel verklaring voor de beperkte regelingen werd nog al eens genoemd dat in de papieren situatie de privacy zeker ook niet gegarandeerd kon worden.

---

[5] De NEN 7510 Informatiebeveiliging in de Zorg is gebaseerd op en afgeleid van de ISO/IEC 17799 en de Code voor Informatiebeveiliging, en vanzelfsprekend toegespitst op de gezondheidszorg.

Rekening houden met de privacy van de patiënt doet ieder ziekenhuis. Daadwerkelijk een systematisch beleid hierop voeren en dat ook controleren is bepaald geen gemeengoed. Een enkel ziekenhuis gaat daadwerkelijk steekproefsgewijs na of er medewerkers zijn die onbevoegd bij gegevens gekeken hebben. Sancties zijn dan het gevolg.

Conclusie en beoordeling

De bescherming van de privacy van de patiënt in ziekenhuizen is met het gebruik van ICT niet in orde. Er bestaan teveel mogelijkheden dat onbevoegden kennis nemen van patiënteninformatie. De vigerende privacywetgeving moet daarom in de ziekenhuizen beter geïmplementeerd worden dan nu het geval is.

4 Methode van onderzoek

Het onderzoek 'ICT in de zorg' is een zogenaamd thematisch toezichtonderzoek. Er is een onderzoek uitgevoerd bij een steekproef van instellingen. Op basis van de geaggregeerde gegevens uit het onderzoek wordt een uitspraak gedaan over de stand van zaken met betrekking tot ICT in de zorg. Speciaal voor dit thematisch toezichtonderzoek is in nauwe samenwerking tussen TNO Preventie en Gezondheid, divisie Technologie in de Gezondheidszorg en de Inspectie voor de Gezondheidszorg het TICTzorg instrument tot stand gekomen. TICTzorg staat voor Toetsing Kwaliteit van ICT in de zorg. TICTzorg is een toetsingsinstrument op waarborgen voor kwaliteit en veiligheid van ICT-producten in een zorginstelling.

De Inspectie voor de Gezondheidszorg hanteert bij het algemeen toezicht een gefaseerd onderzoekssysteem. In een, eerste, administratieve fase wordt informatie verzameld op basis waarvan wordt beoordeeld of een toezichtsfase noodzakelijk is. Afhankelijk van de bevindingen uit de toezichtsfase kan de inspecteur besluiten of maatregelen in de instelling noodzakelijk zijn (de handhavings- of repressieve fase). Bij dit thematisch toezichtonderzoek is het toetsingsinstrument zodanig opgezet dat het in de toekomst ook inzetbaar is bij algemeen toezicht.

TICTzorg ondersteunt de administratieve en de toezichtfase. Het onderscheid in de toepassing van TICTzorg in de twee verschillende fasen wordt uitgedrukt in:
- TICTzorg Scan (de administratieve fase).
- TICTzorg Scorewijzer (werkversie toezichtsfase).

De TICTzorg Scan bestaat uit twee delen. Deel 1 inventariseert de risico's van ICT-producten binnen de instelling. Deel 2 gaat in op de kwaliteitsborging rond die ICT-producten. Deze versie maakt gebruik van open vragen met als doel de variëteit in mogelijke interpretaties van vragen en antwoorden vast te stellen.

De TICTzorg Scan (de administratieve fase van het toezicht)
TICTzorg scan bestaat uit schriftelijke vragenformulieren in te vullen door de zorginstelling, en wel door management/beleid en door het hoofd ICT samen met het hoofd van de instrumentele dienst. Dit past binnen fase 1 van het gefaseerd toezicht. Ingevulde formulieren worden toegezonden aan de inspectie en beoordeeld door een inspecteur. Aan de hand van de gegevens stelt de inspecteur vast welke vervolgactie gewenst is.

De TICTzorg Scorewijzer (de inspectiefase)
De TICTzorg Scorewijzer heeft tot doel de mate van waarborgen rond verantwoord gebruik van ICT vast te stellen. De scorewijzer wordt ingevuld door de inspecteur/interviewer in dialoog met de gesprekspartner(s) van de instelling.

In dit thematisch onderzoek zijn zowel de administratieve fase, dus de TICTzorg Scan als de inspectiefase, de TICTzorg Scorewijzer toegepast.

De gesprekspartners in de instelling waren één persoon van management/beleid, het hoofd van de ICT-afdeling en twee zorgmedewerkers die als gebruiker zijn betrokken bij de ICT. De drie interviews vonden na elkaar plaats.

De scorewijzer geeft vijf aspecten aan, die zijn onderverdeeld in deelaspecten. De vijf aspecten zijn:
- Organisatie en beleid.
- Communicatie en besluitvorming.
- Risicomanagement.
- Procesbeheersing.
- Beveiligingsbeleid.

Bij elk deelaspect is een norm aangegeven met de gewenste score.

De inspecteur/interviewer geeft bij elk aspect zijn eigen score. De totale score per aspect bestaat uit de som van de scores op de deelaspecten. Per bezochte instelling is een rapportage gemaakt. In het inspectierapport worden de scores opgenomen en wordt zonodig aangegeven wat het oordeel van de inspecteur daarbij is.
De inspecteur/interviewer hanteert de volgende scoreschaal voor eenduidigheid en reproduceerbaarheid.

Toelichting scorekwalificaties

1	Afwezigheid van de invulling van het criterium.
2	Dit criterium is op papier ingevuld maar wordt niet consequent gebruikt.
3	Dit criterium is operationeel en wordt consequent gebruikt conform de beschikbare documentatie.
4	Dit criterium is operationeel en wordt consequent gebruikt conform de beschikbare documentatie. Bovendien is er sprake van regelmatige evaluatie en zonodig bijstelling.

De instellingen worden verzocht binnen een bepaalde termijn aan de hand van de rapportage aan de inspectie te laten weten wat de gevolgde acties op de bevindingen in de rapportage zijn geweest.

Ten behoeve van een test van het instrument zijn in pilot drie ziekenhuizen (twee grote en een kleinere), een verpleeghuis en een thuiszorgorganisatie onderzocht met het instrument. Na de test is het instrument op onderdelen bijgesteld.

Het onderzoek is beperkt tot een onderzoek in ziekenhuizen. Hoewel het TICTzorg instrument geschikt is om in elke zorginstelling toegepast te kunnen worden, is allereerst aandacht geschonken aan de situatie in ziekenhuizen. Ziekenhuizen zijn complexe organisaties met in toenemende mate complexe automatiseringstoepassingen die ook in toenemende mate rechtstreeks de veiligheid van de patiënt kunnen raken.

Door middel van een steekproef zijn twintig ziekenhuizen geselecteerd. Er is bij de selectie een onderscheid gemaakt in grotere ziekenhuizen en kleinere ziekenhuizen. Tien ziekenhuizen zijn geselecteerd uit de groep van vijftig ziekenhuizen met het grootste exploitatiebedrag en tien ziekenhuizen zijn geselecteerd uit de vijftig ziekenhuizen met het kleinste exploitatiebedrag. In juli 2003 hebben de ziekenhuizen de TICTzorg Scan toegezonden gekregen. Vanaf augustus 2003 tot en met januari 2004 hebben de bezoeken aan de ziekenhuizen met de TICTzorg Scorewijzer plaatsgevonden. De ziekenhuizen hebben alle een verslag ontvangen dat is opgesteld aan de hand van de gegevens uit de TICTzorg Scan en de TICTzorg Scorewijzer.

5 Summary

Because improper or inexpert use of Information and Communication Technology (ICT) can place patient safety at risk, the Health Care Inspectorate has conducted a study of the conditions under which ICT is introduced, applied and managed in the health care sector.

The study involved a survey of twenty Dutch hospitals, ten of which were selected at random from the group of fifty hospitals having the highest operational budget, and ten from the group with the lowest budget. Various aspects of ICT use were considered in each.

The study reveals that hospitals are not devoting adequate attention to the hazards that ICT use can present. This results in actual risk to the patient. Important information can be lost or can fall into the wrong hands, while treatment and medical interventions may be disrupted by equipment which is not functioning as it should. The introduction of the 'electronic patient file', which has now been implemented in almost all hospitals, demands that greater attention should be devoted to ensuring that information is made fully accessible in a reliable manner. The standards laid down with respect to information security measures must be followed to the letter. If this is not the case, the use of ICT can no longer be regarded as safe. The study found no significant differences between the larger hospitals and their smaller counterparts.

In future, the Health Care Inspectorate will devote increased attention to the safety aspects of ICT use in the health care sector, incorporating this topic into its general supervisory activities. Further performance indicators are therefore to be developed. In addition to overseeing ICT use in hospitals, the Inspectorate will also consider the situation in other health care institutions. In 2005, steps will be taken to ascertain whether the national NEN 7510 norm (covering information security in the health care sector) is being adequately observed.

IGZ 04-67; 500 exemplaren