



**Rapport van bevindingen en conclusie naar
aanleiding van het onderzoek naar
'informatiebeveiliging in ziekenhuizen' in het
St. Jans Gasthuis te Weert op 9 juli 2007**

Inhoudsopgave

1	Inleiding	3
2	Resultaten inspectiebezoek.....	6
2.1	Inleiding.....	6
2.2	Risicoanalyse	6
2.3	Organisatie	6
2.4	Externe Partijen	8
2.5	Beveiliging ten aanzien van personeel	8
2.6	Toegangsbeveiliging	9
2.7	Naleving	10
2.8	Incidenten.....	10
3	Conclusies	12

Bijlagen

- 1 Overzicht gesprekspartners
- 2 Toelichting scorekwalificaties

1 Inleiding

In het kader van hun toezichthoudende taak hebben de Inspectie voor de Gezondheidszorg (IGZ) en het College Bescherming Persoonsgegevens (CBP) op 9 juli 2007 een bezoek gebracht aan het St. Jans Gasthuis te Weert. Doel van dit bezoek was een onderzoek naar de veilige toepassing van ICT en in het bijzonder de mate waarin de normen voor informatiebeveiliging worden nageleefd. Onder informatiebeveiliging moet worden verstaan dat de informatie toegankelijk, oorspronkelijk en juist is en dat de beoogde hulpverleners er datgene mee kunnen doen wat bedoeld wordt, alsmede dat de toegang tot de gegevens of functionaliteit beperkt is tot diegenen die daartoe bevoegd zijn (vertrouwelijkheid).

De IGZ en het CBP hebben in 2007 een toetsingsronde gehouden bij 20 aselect gekozen ziekenhuizen in Nederland (2 academische ziekenhuizen, 9 grote en 9 kleine ziekenhuizen, ingedeeld op basis van het ziekenhuisbudget) teneinde te controleren of zij voldoen aan de regels die gesteld zijn en aldus een beeld te verkrijgen van de veilige toepassing van ICT in de zorg en in het bijzonder de informatiebeveiliging. IGZ en CBP maakten daarbij gebruik van het Toetsingsinstrument ICT in de Zorg (TICTzorg). Hierin staan de criteria op basis waarvan de IGZ en CBP toetsen. De criteria in dit instrument zijn gebaseerd op de relevante wet- en regelgeving en de daarvan afgeleide veldnormen, die de koepelorganisaties en beroepsverenigingen hebben ontwikkeld. Het gaat hierbij om de volgende wetten: de Wet Bescherming Persoonsgegevens, de Wet op de geneeskundige behandelingsovereenkomst, de Wet op de beroepen in de individuele gezondheidszorg en de Kwaliteitswet zorginstellingen. Artikel 13 Wet bescherming persoonsgegevens (Wbp) 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.”

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 overigens 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.

Het doel van dit onderzoek is het verkrijgen van een beeld van de stand van zaken van de implementatie van de NEN 7510 norm bij ziekenhuizen in het algemeen. Tevens wordt de invulling van de informatiebeveiliging in de gekozen ziekenhuizen onderzocht en gecontroleerd of de getroffen maatregelen voldoen aan de hierboven genoemde wet- en regelgeving. In het onderzoek moet ook duidelijk worden welk beeld ziekenhuizen zelf hebben van de wijze waarop en de mate waarin hun informatiebeveiliging is vormgegeven en in het bijzonder of ziekenhuizen hun risico's op het gebied van informatiebeveiliging kennen. IGZ en CBP hebben zes onderdelen¹ van de NEN 7510 norm gekozen als indicatoren voor de toestand van de informatiebeveiliging. IGZ en 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 niet zeggen dat daarmee de gehele NEN 7510 norm voldoende geïmplementeerd is.

De scores op de zes indicatoren zijn in samenhang bepalend voor het oordeel of al dan niet sprake is van overtreding van art. 13 Wbp.

Gezien het voorgaande is bij deze beoordeling het uitgangspunt, dat een ziekenhuis bij een onvoldoende totaalscore in strijd handelt met art. 13 Wbp, tenzij het ziekenhuis kan aantonen dat (a) de beveiliging (op andere wijze) in orde is, (b) het betrokken risico ontbreekt, (c) invoering van de geveerde maatregelen gezien de stand van de techniek praktisch onmogelijk is of (d) de kosten van tenuitvoerlegging redelijkerwijs niet kunnen worden gedragen door het ziekenhuis.

Dezelfde scores op de zes indicatoren zijn in samenhang ook bepalend voor het oordeel van de IGZ, of al dan niet sprake is van verantwoorde zorg zoals gedefinieerd in de

¹ De NEN 7510 norm kent 14 onderdelen. De zes onderdelen waarop in dit onderzoek is getoetst zijn; 1. Organisatie (bestuurlijke verankering), 2. Externe partijen (toegang), 3. Beveiligingseisen ten aanzien van personeel, 4. Toegangsbeveiliging (identificatie en authenticatie), 5. Naleving wetgeving en 6. Beveiligingsincidenten.

kwaliteitswet zorginstellingen. Van bovengenoemde gronden is voor de IGZ alleen uitzondering a van toepassing.

Bij ieder ziekenhuis bestond de toetsing uit een drietal gesprekken: één met een vertegenwoordiger van het bestuur van het ziekenhuis, één met het hoofd van de automatiseringsafdeling en één met een medewerker van het ziekenhuis uit het primair proces (medisch specialist of verpleegkundige). IGZ en CBP verzochten voorafgaande aan het onderzoek de volgende documenten toe te zenden:

- Risicoanalyse(s) met betrekking tot ICT voorzieningen
- Registratie van incidenten met betrekking tot ICT voorzieningen
- Interne en externe auditrapportages met betrekking tot ICT voorzieningen

In dit rapport leest u de resultaten van het onderzoek in het St. Jans Gasthuis.

Achtereenvolgens worden twee vragen beantwoord:

- Hoe scoort het St. Jans Gasthuis op de zes als indicator gekozen onderdelen uit de NEN 7510 norm, als aanwijzing voor het voldoen aan de WBP en als voorwaarden voor verantwoorde zorg? (hoofdstuk 2)
- Wat zijn de conclusies van IGZ en het CBP, alle scores overziende, voor het St. Jans Gasthuis? (hoofdstuk 3)

2 Resultaten inspectiebezoek

2.1 Inleiding

In dit hoofdstuk leest u hoe het St. Jans Gasthuis scoort op de aspecten van informatiebeveiliging zoals vastgelegd in het Toetsingsinstrument ICT in de zorg (TICTzorg). Er zijn zes aandachtsgebieden en per aandachtsgebied vindt u een tabel met scores. Deze scores zijn weergegeven op een vierpuntschaal:

- afwezig
- aanwezig
- operationeel
- geborgd

Zie bijlage 2 voor een toelichting op deze vier kwalificaties.

In dit onderzoek geldt dat voor elk onderdeel een score lager dan “Operationeel” als onvoldoende dient te worden gekwalificeerd. Pas bij de score “operationeel” is de beveiliging immers niet alleen op papier op orde, maar worden de vastgestelde procedures en regels in de praktijk ook daadwerkelijk nageleefd. De score “geborgd” duidt op een hoger niveau van naleving, waarbij de beveiligingsmaatregelen regelmatig worden geëvalueerd en zonodig bijgesteld; pas bij deze score is sprake van een volledig geïmplementeerd beveiligingsbeleid.

Per aandachtsgebied is onder “ijkpunten” een korte beschrijving gegeven van wat op basis van de NEN 7510 norm van ziekenhuizen mag worden verwacht.

2.2 Risicoanalyse

Een risicoanalyse vormt de basis voor het informatiebeveiligingsbeleid van een organisatie. Zonder risicoanalyse is het niet mogelijk om een adequaat informatiebeveiligingsbeleid te formuleren: pas na een risicoanalyse kunnen de prioritaire maatregelen voor informatiebeveiliging worden bepaald.

Door het St. Jans Gasthuis is recentelijk geen risicoanalyse uitgevoerd. Uit nagezonden informatie blijkt dat er wel een procedure voor het uitvoeren van een risicoanalyse in het ziekenhuis beschikbaar is. Doordat het ziekenhuis niet regelmatig een risicoanalyse uitvoert, loopt het St. Jans Gasthuis het gevaar dat er onvoldoende duidelijkheid bestaat over de risico's ten aanzien van informatiebeveiliging en de noodzakelijke maatregelen die moeten worden getroffen om eventuele risico's te beperken.

2.3 Organisatie

IJKpunten functionaris 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. Beleidsaanpassingen zijn voorgenomen / worden doorgevoerd.

Binnen de instelling speelt de beveiligingsfunctionaris een actieve rol bij implementatie van beveiligingsbeleid en bij het proces van bewustwording en handhaving van de afspraken.

IJkpunten externe audit

Er is iemand verantwoordelijk voor het laten uitvoeren van externe audits voor de informatiebeveiliging, er is een externe beoordeling uitgevoerd en er is een rapportage van de bevindingen.

De audit is uitgevoerd door een terzake deskundig (geaccrediteerd) instituut, in de audit zijn alle risicovolle aspecten aan de orde gesteld.

Er is naar aanleiding van de resultaten van de audit actie ondernomen en er is toezicht op implementatie van de aanbevelingen.

De NVZ/NEN monitor is toegepast.

Scores

	<i>Afwezig</i>	<i>Aanwezig</i>	<i>Operationeel</i>	<i>Geborgd</i>
(Hoe) is de verantwoordelijkheid voor de informatiebeveiliging belegd?	√			
(Op welke wijze) wordt informatiebeveiliging beoordeeld?		√		

Toelichting op de scores

Er is geen functionaris aangesteld die verantwoordelijk is voor de informatiebeveiliging. Er is een extern bureau ingeschakeld om de directie te adviseren over de invulling van informatiebeveiliging in het ziekenhuis. Dit heeft geleid tot een beleidsplan en het advies om een Security Officer (SO) aan te stellen. Er ligt inmiddels een voorstel om iemand specifiek aan te stellen voor informatiebeveiliging. De directie heeft hier echter nog geen besluit over genomen. Er wordt nu in het ziekenhuis onderzocht of de verantwoordelijkheid voor informatiebeveiliging bij meerdere functionarissen kan worden ondergebracht. Er is geen duidelijke functieomschrijving. Bij het invullen van de functie zal de speciale positie die de medische staf bij dit onderwerp inneemt (zie gedragscode) aandacht moeten krijgen.

Er zijn externe beoordelingen uitgevoerd. Er hebben NIAZ audits plaatsgevonden en in 2006 is een quickscan op de automatisering uitgevoerd. Bij deze audit en de quickscan lag het accent vooral op technische aspecten van de ICT voorzieningen. Het doel van de quickscan was om voor het ziekenhuis te bepalen, waar het ziekenhuis staat met de implementatie van de NEN 7510 norm. De resultaten van de quickscan hebben geleid tot een honderdtal verbeterpunten voor het ziekenhuis. Dit is vertaald in een informatiebeveiligingsplan, waarin de maatregelen zijn geprioriteerd. In de jaarlijkse accountantscontrole wordt aandacht besteed aan aspecten met betrekking tot ICT en aan aspecten uit de NEN 7510 norm. De resultaten hiervan worden in de managementletter opgenomen. Er is niemand verantwoordelijk voor het laten uitvoeren van audits. De NVZ/NEN monitor is niet toegepast. Er is geen dekkende risicoanalyse uitgevoerd als onderdeel van de beoordeling / beleidsvorming.

2.4 Externe Partijen

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

Scores

	<i>Afwezig</i>	<i>Aanwezig</i>	<i>Operationeel</i>	<i>Geborgd</i>
Wat is de status van de afspraken rondom de uitwisseling van gegevens met derden buiten de instelling?		√		

Toelichting op de scores

Er is uitwisseling van patiëntgegevens met externe partijen. Aan huisartsen wordt via het Edifact protocol op elektronisch wijze gegevens verstuurd. Dit betreft het versturen van laboratoriumuitslagen en informatie rondom opname en ontslag van patiënten. Dit verloopt via een beveiligde verbinding. Voor zover bekend zijn er geen schriftelijke afspraken gemaakt over het gebruik van de data.

Er is een beveiligde directe verbinding met een naburig ziekenhuis, maar deze wordt nog niet gebruikt. Voorafgaand aan het gebruik zullen er nog schriftelijke afspraken worden gemaakt. Externe leveranciers hebben op beperkte schaal toegang tot het systeem.

Er worden voorbereidingen getroffen om een elektronisch voorschrijfsysteem mogelijk te maken. Als dit wordt geïmplementeerd zullen hier schriftelijke afspraken over worden vastgelegd. Medewerkers hebben toegang tot het netwerk via een token. Er is een gedragscode opgesteld voor het gebruik ervan.

Er is geen risicoanalyse uitgevoerd. In de meeste gevallen is evaluatie van afspraken nog niet mogelijk. Dit omdat de afspraken nog niet zijn vastgelegd en omdat logging slechts beperkt of niet wordt uitgevoerd.

2.5 Beveiliging ten aanzien van personeel

IJkpunten geheimhouding

Er is een gedragscode vastgesteld, de gedragscode is bij alle werknemers bekend, men houdt zich aan deze code. Afwijkingen worden gerapporteerd en adequaat afgehandeld.

Scores

	<i>Afwezig</i>	<i>Aanwezig</i>	<i>Operationeel</i>	<i>Geborgd</i>
Hoe wordt omgegaan met geheimhouding?		√		

Toelichting op scores

Er is nog geen algemene gedragscode vastgesteld, waarin beschreven staat hoe medewerkers met ICT middelen en patiëntgegevens dienen om te gaan. Er wordt wel aandacht besteed aan de geheimhoudingsplicht in de aanstellingscontracten van medewerkers. Voor het gebruik van Internet is wel een gedragscode vastgelegd. De mate, waarin medewerkers worden aangesproken op afwijkingen van deze gedragscode hangt af van de prioriteit die individuele leidinggevenden eraan geven.

2.6 Toegangsbeveiliging**IJkpunten 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^[2] is onderkend en hiertegen zijn maatregelen getroffen. Er zijn voorts maatregelen voor het beheer van papieren dossiers getroffen.

IJkpunten toegang tot informatie

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

Scores

	<i>Afwezig</i>	<i>Aanwezig</i>	<i>Operationeel</i>	<i>Geborgd</i>
Wat is de status van maatregelen ten aanzien van fysieke toegangsbeveiliging?		√		
Wat is de status van maatregelen ten aanzien van het verlenen van toegang tot informatie?		√		

Toelichting op scores

Er is geen algemeen beleid vastgesteld voor toegangsbeheersing. De individuele leidinggevende bepaalt tot welke ruimten een medewerker toegang heeft. Er is een goedwerkend elektronisch passysteem, waarmee bepaald wordt wie tot welke ruimten toegang heeft. De toegang tot bepaalde ruimten is extra beveiligd met een toegangscode. De computerruimten zijn dubbel beveiligd met badges. De toegang tot deze ruimten wordt geregistreerd.

^[2] Bij deze tactiek probeert iemand informatie los te krijgen bij personeel, om zodoende toegang te krijgen tot het ziekenhuisnetwerk.

Er is beleid voor het verlenen van toegang tot informatie. Medewerkers krijgen een individueel account en dienen eens per half jaar hun wachtwoord te wijzigen. Het e-mail account is gekoppeld aan het wachtwoord. Hiermee wordt bevorderd dat medewerkers hun eigen account niet onbeheerd open laten staan. Er is één groepsaccount, op de spoedeisende hulp en deze account heeft slechts een beperkte functionaliteit. Er kan op het account van een andere medewerker gewerkt worden. Dit wordt niet gecontroleerd. Logfiles worden, indien aanwezig, niet systematisch nagekeken. Zeer privacy gevoelige medische gegevens worden alleen voor de medisch specialisten toegankelijk gemaakt.

2.7 Naleving

IJKpunten 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. Dit is vertaald in reglementen, procedures en maatregelen. Er is toezicht op de naleving hiervan.

Scores

	<i>Afwezig</i>	<i>Aanwezig</i>	<i>Operationeel</i>	<i>Geborgd</i>
Wat is de status ten aanzien van de naleving van wettelijke voorschriften (WGBO, Wbp en andere relevante wetgeving)?		√		

Toelichting op de scores

Er is geen beleidsstuk waarin staat hoe met deze privacykwesties moet worden omgegaan. Er zijn procedures uitgewerkt voor de WGBO en er is een privacy reglement. Het privacy reglement is op het intranet beschikbaar gesteld. Maar het is niet duidelijk of medewerkers bekend zijn met het privacy reglement. De naleving van de wetgeving wordt niet systematisch getoetst. Er zijn procedures voor het uitoefenen van het inzage- en correctierecht door patiënten.

2.8 Incidenten

IJKpunten 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.

Scores

	<i>Afwezig</i>	<i>Aanwezig</i>	<i>Operationeel</i>	<i>Geborgd</i>
Wat is de status van het beleid rondom beveiligingsincident melding en afhandeling?		√		

Toelichting op scores

Er is geen beleid voor het afhandelen van informatiebeveiligingsincidenten. Er is wel een procedure voor het melden van ICT gerelateerde incidenten. Als er incidenten met betrekking tot informatiebeveiliging worden gedetecteerd, (bijvoorbeeld het aanvallen van de firewall) worden deze onderzocht en worden er maatregelen getroffen. Er wordt gewerkt aan verbetering van de registratie. Het ziekenhuis is voornemens om binnenkort een informatiesysteem aan te schaffen om in dit systeem incidenten te kunnen registreren. Wanneer patiënten bij incidenten zijn betrokken, worden deze volgens de MIP procedure afgehandeld. Het ziekenhuis geeft aan dat medewerkers zich onvoldoende bewust zijn van het belang van het melden van informatiebeveiligingsincidenten. Het is afhankelijk van de medewerker en de leidinggevende wat er met meldingen rond informatiebeveiliging wordt gedaan.

3 Conclusies

In dit onderzoek is onderzocht in welke mate bij het St. Jans Gasthuis sprake is van een veilige toepassing van ICT en in het bijzonder de mate waarin de normen voor informatiebeveiliging worden nageleefd.

Hierbij is met name getoetst aan art. 13 Wbp. 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.

De IGZ heeft met name getoetst aan de Wet Kwaliteit Zorginstellingen waarbij de NEN 7510 geldt als veldnorm en als randvoorwaarde voor verantwoorde zorg.

Het onderzoek is gericht op de volgende zes onderdelen uit de NEN 7510 norm:

1. Organisatie (bestuurlijke verankering), 2. Externe partijen (toegang), 3. Beveiligingseisen ten aanzien van personeel, 4. Toegangsbeveiliging (identificatie en authenticatie), 5. Naleving wetgeving en 6. Beveiligingsincidenten.

Ook is getoetst of een risicoanalyse is uitgevoerd. Een risicoanalyse is belangrijk omdat dit de basis vormt voor het informatiebeveiligingsbeleid van een organisatie.

In hoofdstuk 2 is aangegeven of er een risicoanalyse is uitgevoerd en zijn de scores weergegeven ten aanzien van de onderzochte aspecten uit de NEN 7510 norm.

Aan de hand van deze informatie is aangegeven wat de huidige stand van zaken van informatiebeveiliging binnen het ziekenhuis is, zoals dit bij het inspectiebezoek is waargenomen.

Kort samengevat komen de feitelijke bevindingen met betrekking tot de hiervoor genoemde onderdelen op het volgende neer.

Ad. 1) Er is niemand specifiek verantwoordelijk voor de informatiebeveiliging. Door een extern bureau is geadviseerd om een aparte functionaris voor de informatiebeveiliging aan te stellen. De directie heeft hier nog geen beslissing over genomen. Er zijn verschillende externe audits uitgevoerd. In deze audits zijn vooral technische aspecten van de ICT voorzieningen getoetst. Informatiebeveiliging is hierin beperkt aan de orde geweest.

Ad. 2) Er is elektronisch gegevensuitwisseling met verschillende zorgverleners. De uitwisseling van patiëntgegevens vindt over beveiligde lijnen plaats. Voor zover bekend zijn er geen schriftelijke afspraken gemaakt over het gebruik van de data. Medewerkers kunnen van huis uit werken. Hiervoor is een protocol opgesteld, waarin beschreven staat aan welke regels medewerkers zich hierbij moeten houden. Het ziekenhuis treft voorbereidingen om de gegevensuitwisseling met derden uit te breiden.

Ad. 3) Er is geen specifieke gedragscode opgesteld voor informatiebeveiliging. De geheimhoudingsplicht is standaard opgenomen in het arbeidscontract.

Ad. 4) Er is geen algemeen beleid voor de fysieke toegangsbeveiliging. Er zijn wel maatregelen getroffen, waarmee de toegang tot bepaalde ruimten is beperkt. Voor de toegang tot informatie is beleid opgesteld en zijn eveneens maatregelen getroffen. Er wordt vooral gewerkt met persoonlijke accounts. Medewerkers moeten eens per half jaar het wachtwoord wijzigen, Het e-mail account is gekoppeld aan het wachtwoord. Alleen voor de spoedeisende hulp is een groepsaccount beschikbaar. Zeer vertrouwelijke medische gegevens kunnen extra worden afgeschermd.

Ad. 5) Er zijn procedures voor de WGBO en er is een privacyreglement. Dit reglement is op het intranet beschikbaar. Het is niet duidelijk of medewerkers bekend zijn met het privacy reglement. De naleving van de wetgeving wordt niet systematisch getoetst. Patiënten kunnen het inzage- en correctierecht uitoefenen.

Ad. 6). Voor het melden van incidenten op ICT gebied of op het gebied van patiëntenzorg zijn procedures vastgesteld. Medewerkers zijn zich nog onvoldoende bewust van het belang om informatiebeveiligingsincidenten te melden.

Uit het onderzoek blijkt dat het St. Jans Gasthuis recentelijk geen risicoanalyse heeft uitgevoerd. Het management van het St. Jans Gasthuis heeft daardoor onvoldoende zicht op de risico's die het ziekenhuis op het gebied van informatiebeveiliging loopt.

De scores in samenhang overziend concluderen IGZ en CBP dat er geen sprake is van een passend beveiligingsniveau zoals bedoeld in art. 13 Wbp, dan wel dat is voldaan aan de voorwaarden om verantwoorde zorg te leveren, zoals bedoeld in artikel 2 van de kwaliteitswet zorginstellingen.

Het ziekenhuis kan alsnog aan artikel 13 Wbp voldoen door aan te tonen dat een van de volgende uitzonderingsgronden van toepassing is: (a) de beveiliging (op andere wijze) in orde is, (b) het betrokken risico ontbreekt, (c) invoering van de gevergde maatregelen gezien de stand van de techniek praktisch onmogelijk is of (d) de kosten van tenuitvoerlegging redelijkerwijs niet kunnen worden gedragen door het ziekenhuis.

Voor het oordeel van IGZ ten aanzien van verantwoorde zorg, zoals bedoeld in artikel 2 van de kwaliteitswet zorginstellingen is het alleen relevant dat het ziekenhuis kan aantonen op een andere wijze te komen tot een voldoende informatiebeveiliging. De andere uitzonderingsgronden zijn voor het oordeel van de IGZ niet relevant.

BIJLAGE 1

De gegevens over het St. Jans Gasthuis zijn verkregen uit gesprekken met:

- dhr. F. Kroeze, Voorzitter stuurgroep informatica, namens de directie
- mevr. B. van Dijke, Arts-microbioloog
- dhr. P. Kuepers, Hoofd automatisering

De volgende documenten werden tevoren toegezonden:

- Rapportage Quickscan NEN 7510 norm door Infoland (20 september 2006)
- Werkwijze registratie incidenten ontvangen door helpdesk ICT (februari tot maart 2007)
- Meldingen eenvoudige incidenten Helpdesk maart 2007

Ontvangen na afloop van bezoek:

- Cd-rom met documenten met betrekking tot de NEN 7510 norm
- Projectplan Beleid & uitvoering informatiebeveiliging (4 januari 2006) en projectplanning
- Informatiebeveiligingsbeleid Infoland 2006-2008 (12 oktober 2006)
- Informatievoorzieningen BIV (ongedateerd)
- Profielschets informatiebeveiligingsfunctionaris (ongedateerd)
- RGB matrix (ongedateerd)
- Communicatieplan informatiebeveiliging Infoland (maart 2007)
- Informatiebeveiliging monitor Infoland (maart 2007)
- Rapportage quickscan NEN 7510 norm (20 september 2006)
- Maatregelen voorstel (ongedateerd)
- Informatiebeveiligingsplan 2007 Infoland (20 november 2006)
- Het informatiebeveiligingsproces Infoland (ongedateerd)
- Procedure IB (8 november 2004)
- Procedure incidentenafhandeling (8 november 2004)
- Procedure interne audits (8 november 2004)
- Procedure risicoanalyse (8 november 2004)

Namens IGZ en CBP werden de gesprekken gevoerd door,

- mevr. A.C. Gräve, privacy auditor CBP
- dhr. J.M.J. van den Berg, inspecteur IGZ
- mevr. S. Riezebos, programmamedewerker IGZ

BIJLAGE 2 Toelichting scorekwalificaties

<i>Afwezig</i>	Afwezigheid van de invulling van het criterium.
<i>Aanwezig</i>	Dit criterium is op papier ingevuld maar wordt niet consequent gebruikt.
<i>Operationeel</i>	Dit criterium is operationeel en wordt consequent gebruikt conform de beschikbare documentatie.
<i>Geborgd</i>	Dit criterium is operationeel en wordt consequent gebruikt conform de beschikbare documentatie. Bovendien is er sprake van regelmatige evaluatie en zonodig bijstelling.