COLLEGE BESCHERMING PERSOONSGEGEVENS

STAATSTOEZICHT OP DE VOLKSGEZONDHEID
INSPECTIE VOOR DE GEZONDHEIDSZORG

Rapport van bevindingen en conclusie naar aanleiding van het onderzoek 'informatiebeveiliging in ziekenhuizen' in het St. Lucas Ziekenhuis te Winschoten op 1 juni 2007

Juli 2008

Inhoudsopgave

Bijlagen

1 Inleiding

In het kader van hun toezichthoudende taak hebben de Inspectie voor de Gezondheidszorg (IGZ) en het College Bescherming Persoonsgegevens (CBP) op 1 juni 2007 een bezoek gebracht aan het St. Lucas Ziekenhuis te Winschoten. 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 onderdelen[1] 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 níet 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 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.

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. Lucas Ziekenhuis. Achtereenvolgens worden twee vragen beantwoord:

- Hoe scoort het St. Lucas Ziekenhuis 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. Lucas Ziekenhuis? (hoofdstuk 3)

2 Resultaten inspectiebezoek

2.1 Inleiding

In dit hoofdstuk leest u hoe het St. Lucas Ziekenhuis 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.

Het ziekenhuis heeft een risicoanalyse uitgevoerd.

2.3 Organisatie

IJkpunten functionaris informatiebeveiliging

Er is iemand benoemd op directieniveau, die verantwoordelijk is voor informatie-beveiliging. 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

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

Toelichting op scores
De beveiliging van informatie in het St. Lucas Ziekenhuis is niet specifiek belegd bij één persoon. De verantwoordelijkheden en taken rond de beveiliging van informatie zijn niet benoemd. Informatiebeveiliging wordt tot het werkdomein van de manager ICT gerekend voor wat betreft het ICT deel, van de manager zorg voor wat betreft het papieren dossier en van de 'beveiliging' voor de gebouw aspecten. Beveiliging van informatie is een cruciaal onderwerp voor een ziekenhuis. De verantwoordelijkheid daarvoor dient ondubbelzinnig te zijn geregeld. Door dat niet te doen loopt het ziekenhuis het risico dat noodzakelijke maatregelen niet worden genomen.

Het ziekenhuis heeft meerdere audits laten uitvoeren. Het betreft zowel (beperkte) risicoanalyses van hardware/netwerk, als een uitgebreide beoordeling in hoeverre de NEN 7510 norm wordt gevolgd. Met de vaststellingen en de aanbevelingen uit die analyses is zeer pragmatisch omgegaan. Er is geen specifiek beveiligingsbeleid uit naar voren gekomen waarbij systematisch tekortkomingen voorzien zijn van een plan om verholpen te worden. De analyses hebben slechts op beperkte schaal en dus zonder duidelijk herleidbare prioritering tot maatregelen geleid.

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

	Afwezig	*Aanwezig*	*Operationeel*	*Geborgd*
Wat is de status van de afspraken rondom de uitwisseling van gegevens met derden buiten de instelling?		√		

Toelichting op scores

Op dit moment worden op beperkte schaal elektronisch gegevens verzonden naar andere zorgleveranciers. Het betreft voornamelijk laboratoriumgegevens en brieven aan huisartsen. Er zijn wel overeenkomsten gesloten voor de uitvoering van dit gegevensverkeer, maar daar is geen duidelijke risicoanalyse aan vooraf gegaan. Overeenkomsten worden niet periodiek herbeoordeeld.

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

	Afwezig	*Aanwezig*	*Operationeel*	*Geborgd*
Hoe wordt omgegaan met geheimhouding	√			

Toelichting op scores

De wijze waarop medewerkers van het ziekenhuis om moeten gaan met informatie, zoals de plicht gegevens geheim te houden, wordt geacht volledig te zijn geregeld in de CAO. Het ziekenhuis heeft alleen voor internetgebruik en e-mailverkeer een gedragscode opgelegd die zij moeten ondertekenen en waar een consistente controle op plaats vindt. Deze gedragscode heeft echter geen betrekking op de geheimhouding van patiëntgegevens. Door alleen maar naar de CAO te verwijzen laat het ziekenhuis na specifiek op de functie gerichte voorwaarden te stellen over de omgang met de aan hen toe vertrouwde gegevens en apparatuur.

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[12] is onderkend en er zijn hiertegen maatregelen getroffen. Er zijn voorts maatregelen voor het beheer van papieren dossiers getroffen.

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

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

	Afwezig	*Aanwezig*	*Operationeel*	*Geborgd*
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 document waarin staat beschreven hoe de toegang tot ruimten is geregeld Feitelijk zijn sommige ruimten niet toegankelijk voor iedereen (bijvoorbeeld serverruimte, OK). Er is echter geen beleid waar in is opgenomen wie (in welke functie) waar toegang toe heeft, welke procedure wordt gehanteerd om die toegang te verkrijgen en wat er gebeurt als iemand de organisatie verlaat. Door daar geen expliciete regeling voor te hebben loopt het ziekenhuis de kans dat onbevoegde ruimten betreden en een gevaar vormen voor het ziekenhuis en de patiënt. Daarnaast bestaat het risico dat vertrouwelijke gegevens worden ingezien door onbevoegden.

Alhoewel er voor het Xcare-systeem een concept-autorisatieregeling is, heeft het ziekenhuis geen beleid geformuleerd over de toegang van de medewerker tot de informatie die in het ziekenhuis aanwezig is. De regeling is beschikbaar via het DKS op het intranet. De raadplegingen binnen het ziekenhuisinformatiesysteem worden gelogd. Deze loggingen worden echter niet systematisch of volgens een bepaalde procedure beoordeeld, hetgeen bijvoorbeeld wel het geval is voor de loggingen van het Internet en e-mailgebruik.

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

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

Toelichting op scores

De consequenties van de regelgeving zijn hier en daar in ziekenhuisprocedures verwerkt. Het inzagerecht is bijvoorbeeld na een besluit door het MT vastgelegd in een procedure die beschikbaar is voor alle medewerkers. De bewaartermijnen zoals in wettelijke regelingen is vastgelegd worden niet gevolgd. Gegevens worden onbeperkt bewaard.

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

	Afwezig	*Aanwezig*	*Operationeel*	*Geborgd*
Wat is de status van het beleid rondom beveiligingsincident melding en afhandeling?		√		

Toelichting op scores

ICT gerelateerde meldingen van incidenten worden apart behandeld en geregistreerd van meldingen die gerelateerd zijn aan de patiëntenzorg. De procedure voor de patiëntenzorg gerelateerde meldingen is in concept vastgelegd en functioneert naar tevredenheid. Dat geldt minder voor de ICT gerelateerde meldingen van incidenten. Informatiebeveiligingsincidenten zijn niet als zodanig te herleiden omdat ze niet apart worden geregistreerd.

3 Conclusies

In dit onderzoek is onderzocht in welke mate bij het St. Lucas Ziekenhuis 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 per hiervoor genoemd onderdeel op het volgende neer.

Ad. 1) De beveiliging van informatie in het St. Lucas Ziekenhuis is niet specifiek belegd bij één persoon. De verantwoordelijkheden en taken rond de beveiliging van informatie zijn niet benoemd.
Het ziekenhuis heeft meerdere audits uit laten voeren, waaronder een beoordeling in hoeverre de NEN 7510 wordt gevolgd. Met de vaststellingen en de aanbevelingen is echter zeer pragmatisch omgegaan: er is geen specifiek beveiligingsbeleid uit naar voren gekomen waarbij systematisch tekortkomingen zijn voorzien van een plan om verholpen te worden.
Ad. 2) Op dit moment worden slechts op beperkte schaal elektronisch gegevens verzonden naar andere zorgleveranciers. Er zijn wel overeenkomsten gesloten voor de uitvoering van dit gegevensverkeer, maar daar is geen duidelijke risicoanalyse aan vooraf gegaan. Deze overeenkomsten worden niet periodiek herbeoordeeld.
Ad. 3) De wijze waarop medewerkers van het ziekenhuis om moeten gaan met informatie, zoals de plicht gegevens geheim te houden, wordt geacht volledig te zijn geregeld in de CAO. Een geheimhoudingsverklaring in een CAO kan echter niet worden gelijkgesteld aan een gedragscode.
Ad. 4) Feitelijk zijn sommige ruimten niet toegankelijk voor iedereen (bijvoorbeeld serverruimte, OK). Er is echter geen beleid waarin is opgenomen wie (in welke functie) waar toegang toe heeft.
Het ziekenhuis heeft geen beleid geformuleerd over de toegang van de medewerker tot de informatie die in het ziekenhuis aanwezig is.

Ad. 5) De consequenties van de regelgeving zijn slechts hier en daar in ziekenhuisprocedures verwerkt.
Ad. 6) De procedure voor de patiëntenzorg gerelateerde meldingen is in concept vastgelegd en functioneert naar tevredenheid. Dat geldt minder voor de ICT gerelateerde meldingen van incidenten. Informatiebeveiligingsincidenten zijn niet als zodanig te herleiden omdat ze niet apart worden geregistreerd.

Uit het onderzoek blijkt dat het St. Lucas Ziekenhuis een risicoanalyse heeft uitgevoerd.

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. Lucas Ziekenhuis zijn verkregen uit gesprekken met:
- Dhr. F. Kremer, manager zorg
- Dhr. J. Olthof, manager ICT
- Dhr. T.R. Bouwmeester, cardioloog

De volgende documenten werden tevoren toegezonden:
- Rapportage incidenten automatiseringsdienst St. Lucas (2006)
- Rapportage incidenten automatiseringsdienst St. Lucas (2007)
- Risicoanalyse automatisering (2007)
- Bevindingen St. Lucas: kwaliteitsaspecten (2006)

Op dag van bezoek ingezien en meegekregen
- Informatiebeveiliging in het St. Lucas ziekenhuis (12-07-2006)

Namens IGZ en CBP werden de gesprekken gevoerd door,
- Dhr. J. Vlug, technoloog CBP
- Dhr. J. Vesseur, inspecteur IGZ
- Mw. S. Riezebos, programmamedewerker IGZ/ notulist

BIJLAGE 2 Toelichting scorekwalificaties

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