



**Rapport van bevindingen en conclusie naar
aanleiding van het onderzoek 'informatiebeveiliging
in ziekenhuizen' in Alysis Zorggroep, Ziekenhuis
Rijnstate te Arnhem op 6 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	7
2.5	Beveiliging ten aanzien van personeel	8
2.6	Fysieke toegangsbeveiliging	9
2.7	Naleving	9
2.8	Incidenten.....	10
3	Conclusies	11

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 6 juli 2007 een bezoek gebracht aan de Alysis Zorggroep, het Rijnstate Ziekenhuis te Arnhem. 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) 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 Rijnstate Ziekenhuis.

Achtereenvolgens worden twee vragen beantwoord:

- Hoe scoort het Rijnstate 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 Rijnstate Ziekenhuis? (hoofdstuk 3)

2 Resultaten inspectiebezoek

2.1 Inleiding

In dit hoofdstuk leest u hoe het Rijnstate 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 Rijnstate Ziekenhuis heeft in 2005 een beperkte externe risicobeoordeling uit laten voeren en vult deze aan met interne audits, de laatste in 2006. Er is thans geen actueel beeld van de risico's die het ziekenhuis ten aanzien van informatiebeveiliging loopt. Hierdoor loopt het ziekenhuis het gevaar dat er onvoldoende duidelijkheid bestaat over de risico's ten aanzien van informatiebeveiliging en de hiertegen te treffen noodzakelijke maatregelen.

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 scores

De ICT manager is verantwoordelijk voor de informatiebeveiliging. De functie is niet als zodanig aangewezen, maar iedereen beschouwt hem als de verantwoordelijke. Dat kan problemen opleveren omdat de functionaris weliswaar over de ICT voorzieningen gaat maar over de beveiligingsaspecten van papieren dossiers geen zeggenschap heeft.

Een extern bureau heeft in 2005 een onderzoek verricht naar de kwaliteit van de informatiebeveiliging in het ziekenhuis om zodoende een beeld te krijgen over de mate, waarin wordt voldaan aan de NEN 7510 norm. Ook intern worden er audits uitgevoerd naar de kwaliteit van de Informatisering. Informatiebeveiliging speelt daarbij ook een rol. Veel gesignaleerde tekortkomingen hebben geleid tot actieplannen die op hun beurt weer hebben geleid tot aanpassingen en maatregelen. Er is na de Quick Scan NEN 7510 in 2005 een aanzet gegeven tot het opstellen van een informatiebeveiligingsbeleid. De Quick Scan heeft echter niet geleid tot een formeel beleid, waarbij op basis van een risico-inschatting een totaal plan voor de uitvoering van de informatiebeveiliging is gemaakt om uiteindelijk aan de NEN 7510 norm te voldoen.

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 scores

Huisartsen kunnen langs elektronische weg correspondentie ontvangen. Dit vindt plaats via EDIFACT standaarden. Het betreft dus een eenrichtingverkeer van ziekenhuisgegevens. Er zijn binnen het ziekenhuis afspraken over de uitwisseling van gegevens via EDIFACT gemaakt.

Met het Radboud Ziekenhuis in Nijmegen is een VPN verbinding. Voor de uitwisseling van gevoelige gegevens met bijvoorbeeld het Klinisch Genetisch Centrum over pre- en postnatale diagnostiek wordt altijd de VPN verbinding gebruikt. Het is niet bekend of er met huisartsen hierover afspraken zijn gemaakt.

De toegang die leveranciers tot de ziekenhuisinformatiesystemen hebben is afgedekt met een addendum bij de inkoopvoorwaarden. Mutaties die door leveranciers in systemen worden aangebracht, worden gelogd. Technisch doet het ziekenhuis er alles aan om de verbindingen die nodig zijn voor gegevensuitwisseling zo veilig mogelijk te maken. Medewerkers wisselen onderling geen patiëntgegevens uit via standaard e-mailvoorzieningen. Uitzondering hierop is dat specialisten via email mogen communiceren met patiënten. Hier is een protocol voor en patiënten tekenen hiervoor.

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

Door middel van verschillende gedragscodes heeft het ziekenhuis aan de medewerkers duidelijk gemaakt hoe zij met patiëntgegevens en bedrijfsvertrouwelijke zaken moeten omgaan. Er vindt geen systematische controle op de naleving van deze gedragscode plaats. Incidenteel worden overtredingen van deze gedragscodes opgepakt en onderzocht.

2.6 Fysieke 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

Het beleid voor de toegang tot ruimten wordt herzien. Het ziekenhuis wil het elektronisch pasjessysteem uitbreiden met een logging van de toegang. Het ziekenhuis heeft dit voorstel ter goedkeuring voorgelegd aan de OR. Doordat de controle op de afdeling die de pasjes uitgeeft nu niet is geregeld, is het huidige systeem niet waterdicht.

Het informatietoegangsbeleid van het ziekenhuis regelt op basis van functies de toegang tot de informatie. In het huidige ziekenhuisinformatiesysteem (ZIS) kan de toegang tot de patiëntgegevens niet zo verfijnd worden geregeld als het ziekenhuis zou willen. Het ziekenhuis wil dat de toegang tot informatie in het nieuwe ZIS specifieker wordt ingericht. Het is nu niet mogelijk om na te gaan welke medewerker tot welke patiëntgegevens toegang heeft gehad. Het ziekenhuis moet nu met name uitgaan van het goede gedrag van medewerkers.

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.

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

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 scores

Via de privacycommissie worden consequenties van de hiervoor genoemde wet- en regelgeving verwerkt in ziekenhuisprocedures en voorschriften. De informatiseringsafdeling is daar systematisch bij betrokken. Er is geen algemeen ziekenhuisbrede aandacht voor privacy. De privacycommissie is niet duidelijk in de organisatie aanwezig, men merkt hier op de werkvloer niets van.

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 een procedure voor het melden van incidenten ten aanzien van patiëntenzorg. Daarnaast is er een procedure voor het melden van ICT gerelateerde incidenten. De MIP (Meldingen Incidenten Patiëntenzorg) procedure is goed bekend in het ziekenhuis. Incidenten worden geregistreerd en er vindt systematische rapportage plaats. Incidentenrapportages worden gebruikt ter verantwoording maar ook om trends te signaleren. Het ziekenhuis kan niet aangeven welke specifieke informatiebeveiligingsincidenten hebben plaatsgevonden.

3 Conclusies

In dit onderzoek is onderzocht in welke mate bij het Rijnstate 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 met betrekking tot de hiervoor genoemde onderdelen op het volgende neer.

Ad. 1) De ICT manager is verantwoordelijk voor de informatiebeveiliging. Dit is echter niet formeel vastgelegd. Een extern bureau heeft in 2005 een onderzoek verricht naar de kwaliteit van de informatiebeveiliging binnen het ziekenhuis om een beeld te krijgen over de mate, waarin wordt voldaan aan de NEN 7510 norm.

Ad. 2) Huisartsen kunnen langs elektronisch weg correspondentie ontvangen. Technisch doet het ziekenhuis er alles aan om de verbindingen die nodig zijn voor gegevensuitwisseling zo veilig mogelijk te maken. Specialisten kunnen elektronisch gegevens met patiënten uitwisselen. Hiervoor is een protocol opgesteld.

Ad. 3) Door middel van verschillende gedragscodes heeft het ziekenhuis aan de medewerkers duidelijk gemaakt hoe zij met patiëntgegevens moeten omgaan. Echter, er vindt geen systematisch controle plaats op de naleving van deze gedragscodes.

Ad. 4) Het beleid voor de toegang tot ruimten wordt momenteel herzien. In het huidige ZIS kan de toegang tot patiëntgegevens niet zo verfijnd worden geregeld als het ziekenhuis zou willen.

In het huidige systeem is het niet mogelijk om na te gaan welke medewerker tot welke patiëntgegevens toegang heeft gehad.

Ad. 5) Via de privacycommissie worden de consequenties van de privacy wet en regelgeving verwerkt in ziekenhuis procedures en voorschriften. Echter, er is geen algemeen ziekenhuisbrede aandacht voor privacy en geen systematisch toezicht op de naleving hiervan.

Ad. 6). Er is een procedure voor het melden van incidenten ten aanzien van patiëntenzorg. Daarnaast is er een procedure voor het melden van ICT gerelateerde incidenten. Het ziekenhuis kan niet aangeven welke specifieke informatiebeveiligingsincidenten hebben plaatsgevonden.

Uit het onderzoek blijkt dat er in het Rijnstate Ziekenhuis in 2005 een beperkte externe risicobeoordeling is uitgevoerd. Deze wordt aangevuld met interne audits, de laatste in 2006. Er is thans geen actueel beeld van de risico's die het ziekenhuis ten aanzien van informatiebeveiliging loopt. Hierdoor loopt het Rijnstate Ziekenhuis het gevaar dat er onvoldoende duidelijkheid bestaat over de risico's ten aanzien van informatiebeveiliging en de hiertegen te treffen noodzakelijke maatregelen.

De scores in samenhang overziend concluderen IGZ en CBP dat er onvoldoende 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 Ziekenhuis Rijnstate zijn verkregen uit gesprekken met:

- Dhr. G. de Bey, lid Raad van Bestuur
- Mevr. M. Janssen, secretaris Raad van Bestuur
- Dhr. F. Smolders, manager informatisering
- Dhr. A. de Jong, reumatoloog

De volgende documenten werden tevoren toegezonden:

- Risicomatrix: domein ICT (6 november 2001)
- Status quo rapportage per 31 maart (4 juni 2007)
- Status quo rapportage per 31 december (26 maart 2006)
- Uitdraai storingslogging (31 maart tot 5 april)
- Analyse problemen (18 februari 2007)
- Evaluatie uitval telefonie (20 november 2006 tot 4 januari 2007)
- Risicobeheersing energievoorziening (16 april 2004)
- Verbeteren van beschikbaarheid en performance van de elektronische informatievoorziening (20 april 2005)
- Toegangsbeveiliging van het netwerk (2 oktober 2006)
- Project voorstel: Inrichting informatiebeveiliging (concept, 28 maart 2006)
- Informatiebeveiligingsbeleid (concept, 24 mei 2005)
- Concept rapportage interne audit informatisering (8 juni 2007)
- Quick scan ICT door CapGemini (8 april 2005)
- Quick scan rapport NEN 7510 norm door Getronics (9 maart 2005)

Op locatie ontvangen:

- Eindrapportage Project Mozaïek (december 2006)

Namens IGZ en CBP werden de gesprekken gevoerd door,

- Mw. T. Gräve, privacy auditor CBP
- Mw. S. Riezebos, programmamedewerker / notulist IGZ
- Dhr. J. Vesseur, inspecteur 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.