COLLEGE BESCHERMING PERSOONSGEGEVENS

Rapport van bevindingen en conclusie naar aanleiding van het onderzoek 'informatiebeveiliging in ziekenhuizen' in het Rijnland Ziekenhuis te Leiderdorp op 7 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 7 juni 2007 een bezoek gebracht aan het Rijnland Ziekenhuis te Leiderdorp. 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 van het CBP 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 Rijnland Ziekenhuis. Achtereenvolgens worden twee vragen beantwoord:

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

2 Resultaten inspectiebezoek

2.1 Inleiding

In dit hoofdstuk leest u hoe het 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.

In 2005 is een quickscan risicoanalyse uitgevoerd naar de informatiebeveiliging in het Rijnland Ziekenhuis. Als basis voor de quickscan is de NEN 7510 norm gebruikt. Naar aanleiding van deze quickscan zijn de risico´s in kaart gebracht en geprioriteerd. Op basis hiervan zijn aanbevelingen opgesteld voor te nemen maatregelen. Er zijn tussen rapportages opgesteld over de voortgang van de implementatie van aanbevelingen en maatregelen uit de risicoanalyse.
In 2006 is een procedure vastgesteld voor het tweejaarlijks uitvoeren van een risicoanalyse op de informatiebeveiliging.

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 verantwoordelijkheid voor informatiebeveiliging is ondergebracht bij twee medewerkers. De ene medewerker is verantwoordelijk voor de technische infrastructuur en de andere medewerker is verantwoordelijk voor het functioneel beheer. De effectiviteit van de tweedeling staat of valt met een goede verdeling van taken. Er zou een taakomschrijving voor beide functionarissen zijn, maar deze is niet ingezien. Doordat het hoofd ICT de verantwoordelijkheid heeft voor het waarborgen van het ICT deel van de informatiebeveiliging, is de inbreng hiervan in het ICT beleid gewaarborgd. Op dit moment kunnen de inspecteurs onvoldoende beoordelen in hoeverre dit leidt tot een heldere en eenduidige taakstelling. De maatregelen die het ziekenhuis voor verbetering van de beveiliging tot dusverre heeft genomen liggen vooral op het gebied van de ICT infrastructuur. Volgens het ziekenhuis is voorrang gegeven aan de verbetering van de ICT infrastructuur, omdat er sprake was van een achterstand in het treffen van technische voorzieningen.

Er zijn onderzoeken door een externe bureaus uitgevoerd om de stand van zaken van de ICT voorzieningen te beoordelen. Tijdens deze onderzoeken is ook aandacht besteed aan de technische aspecten van de informatiebeveiliging. Op basis van de vastgestelde risico's is een informatiebeveiligingsplan opgesteld. Daarin is een tijdpad opgenomen, waarbinnen de verbeteringen gerealiseerd moeten worden. Prioriteit is gegeven aan de ICT gerelateerde aspecten van informatiebeveiliging. Uit de actielijst is op te maken dat veel maatregelen gericht op de medewerkers (nog) niet worden uitgevoerd.
Het externe bureau heeft een meerjarenplan opgesteld voor EDP audits.

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

In de risicoanalyse is aandacht besteed aan de risico's van het uitwisselen van informatie. Het ziekenhuis wisselt versleuteld patiëntgegevens uit met huisartsen via Edifact. Dit betreft laboratoriumuitslagen en specialistenbrieven. Het ziekenhuizen heeft nog geen contracten afgesloten met huisartsen, waarin concrete afspraken met betrekking tot deze gegevensuitwisseling zijn opgenomen. Met het Diaconessenhuis Leiden en het Leids Universitair Medisch Centrum (LUMC) worden eveneens patiëntgegevens uitgewisseld. Software leveranciers hebben toegang tot de informatiesystemen. In de contracten, die tussen het ziekenhuis en de softwareleveranciers zijn afgesloten, zijn alleen de technische aspecten van de informatiebeveiliging geregeld. Medewerkers kunnen via een 'Citrix' verbinding vanuit huis werken. De toegangsprocedure voor het eigen personeel vindt plaats op basis van wachtwoorden en een pincode.

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

Er is een gedragscode. In de personeelscontracten wordt naar deze gedragscode verwezen. In de gesprekken is ter sprake gekomen dat de code onvoldoende bekend is bij medewerkers of toch onvoldoende 'leeft' bij medewerkers. Er is een communicatieplan opgesteld om de naleving van de gedragscode te verbeteren.

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

	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 beleid voor wat betreft de fysieke toegang aanwezig. Er wordt gewerkt met beheerde passen en sleutels. Het beleid wordt niet/onvoldoende geëvalueerd en herzien. De beveiliging van papieren dossiers is nog onvoldoende. Artsen nemen deze nog steeds mee naar huis.

Er is beleid voor het verlenen van toegang tot patiëntengegevens. Er wordt in sommige gevallen gebruik gemaakt van groepsaccounts. Het ziekenhuis geeft aan dat het de bedoeling is om deze groepsaccounts op termijn om te zetten naar individuele accounts. Het is niet duidelijk hoe de toegang tot de informatiesystemen voor co-assistenten is geregeld. De door de medewerkers verrichtte activiteiten op de informatiesystemen worden gelogd. Applicaties blijven vaak open staan zonder dat een screensaver de toegang tot het informatiesysteem afsluit. In het gesprek met de ICT manager werd aangegeven dat er bij enkele applicaties technische problemen zijn bij het gebruik van een screensaver. Hier worden oplossingen voor gezocht. Ook kunnen artsen / medewerkers op meerdere plaatsen ingelogd zijn. Zodra medewerkers uit dienst treden hebben zij geen toegang meer tot de informatiesystemen. Hiervoor is een procedure vastgesteld.

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

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

Er is een privacyreglement aanwezig. Dit reglement is in het ziekenhuis geïmplementeerd. Er zijn procedures vastgesteld voor het kunnen 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

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

Toelichting op scores

Er is een procedure vastgesteld voor het melden van incidenten. Er is ook een procedure vastgesteld voor het melden van informatiebeveiligingsincidenten. Deze laatste procedure is via een nieuwsbrief aan de medewerkers bekend gemaakt. Medewerkers melden weinig incidenten. Medewerkers zijn zich onvoldoende bewust van het belang van het melden van informatiebeveiligingsincidenten.

3 Conclusie

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

Hierbij heeft het CBP 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 en op het volgende neer.

Ad. 1) De verantwoordelijkheid voor informatiebeveiliging is bij twee medewerkers ondergebracht. De ene medewerker is verantwoordelijk voor de technische infrastructuur en de andere medewerker is verantwoordelijk voor het functioneel beheer. Er is onderzoek door een extern bureau uitgevoerd om de stand van zaken van de ICT voorzieningen te beoordelen. Naar aanleiding van dit onderzoek heeft het ziekenhuis een informatiebeveiligingsplan opgesteld. Het ziekenhuis heeft een meerjarenplan voor het uitvoeren van EDP audits laten opstellen.
Ad. 2) Het ziekenhuis wisselt patiëntgegevens uit met huisartsen. Hiervoor zijn echter geen contracten opgesteld. Daarnaast wisselt het ziekenhuis patiëntgegevens uit met twee andere ziekenhuizen in de regio.
Ad. 3) Er is een gedragscode vastgesteld. Echter, deze is onvoldoende bekend bij de medewerkers.
Ad. 4) Er is beleid ten aanzien van de fysieke toegangsbeveiliging. Dit beleid wordt echter nauwelijks geëvalueerd. Er is beleid voor de toegang tot patiëntgegevens. Naast individuele account wordt er gebruik gemaakt van groepsaccounts. Het ziekenhuis geeft aan dat het de bedoeling is om op termijn deze groepsaccount om te zetten naar individuele accounts.
Ad. 5) Er is een privacyreglement aanwezig. Dit reglement is in het ziekenhuis geïmplementeerd.

Ad. 6). Er is een procedure vastgesteld voor het melden van informatiebeveiligingsincidenten. Omdat medewerkers zich onvoldoende bewust zijn van het belang van het melden van beveiligingsincidenten, wordt er weinig gebruik van gemaakt.

Uit het onderzoek blijkt dat het Rijnland Ziekenhuis een risicoanalyse heeft uitgevoerd. Op basis hiervan zijn aanbevelingen opgesteld voor te nemen maatregelen. Er zijn tussenrapportages opgesteld over de voortgang van de implementatie van de maatregelen. Het ziekenhuis heeft een procedure vastgesteld om twee jaarlijks een risicoanalyse uit te voeren.

De scores in samenhang overziend concluderen IGZ en CBP dat er onvoldoende sprake is van een passend beveiligingsniveau zoals bedoeld in art. 13 Wbp en dat evenmin 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 uitzonderingsronden 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 Rijnland ziekenhuis zijn verkregen uit gesprekken met:
- dhr. E.A. van Royen, lid Raad van Bestuur
- dhr. A.C. van den Berg, Hoofd ICT
- dhr. Z.W. Sneller, uroloog, voorzitter Medische Staf

De volgende documenten werden tevoren toegezonden:

- Beleidsplan Informatiebeveiliging Alatus 2005-2008 (mei 2005)
- BIV kwalificatie Rijnland Alatus(ongedateerd)
- Ernst&Young: meerjarenplan EDP audit 2007-2009 (mei 2007)
- Tussenrapportage implementatie risicoanalyse (mei 2007)
- Tussenrapportage t.b.v. Raad van Bestuur (september 2006)
- Rapportage risicoanalyse ICT omgeving (mei 2006)
- Processchema interne audits informatiebeveiliging (januari 2006)
- Processchema incidenten informatiebeveiliging (januari 2006)
- Processchema informatiebeveiliging (februari 2006)
- Processchema interne audits informatiebeveiliging (januari 2006)
- Informatiebeveiligingsplan Alatus 2005 – 2008 (augustus 2005)
- Maatregelen (ongedateerd)
- Quickscan risicoanalyse Alatus rapportage (mei 2005)
- Procedure risicoanalyse (ongedateerd)
- Procedure interne audits (ongedateerd)
- Procedure incidenten afhandeling (ongedateerd)
- Procedure IB (ongedateerd)
- RGB matrix (ongedateerd)
- Procedure interne audits informatiebeveiliging (september 2006)
- Meldingsformulier IB (ongedateerd)
- Procedure risicoanalyse informatiebeveiliging (juni 2006)
- Procedure incidenten informatiebeveiliging: melding en afhandeling (juni 2006)
- Kwaliteitsbeleidsplan ICT afdeling Alatus (februari 2006)
- Procedure informatiebeveiliging (juni 2006)

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. H.M. de Monyé- de Ridder, Toezichtmedewerker 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.