



**Rapport van bevindingen en conclusie naar
aanleiding van het onderzoek 'informatiebeveiliging
in ziekenhuizen' in het Atrium MC te Heerlen op 10
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	Toegangsbeveiliging	9
2.7	Naleving	9
2.8	Incidenten.....	10
3	Conclusie.....	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 10 juli 2007 een bezoek gebracht aan het Atrium MC te Heerlen. 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 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 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 Atrium MC te Heerlen.

Achtereenvolgens worden twee vragen beantwoord:

- Hoe scoort het Atrium MC 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 Atrium MC? (hoofdstuk 3)

2 Resultaten inspectiebezoek

2.1 Inleiding

In dit hoofdstuk leest u hoe het Atrium MC 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 Atrium MC is in 2003 eveneens door IGZ onderzocht. Op basis van de uitkomsten van dit eerdere onderzoek is een risicoanalyse uitgevoerd. Tevens zijn er acties ondernomen om de ICT voorzieningen in het ziekenhuis te verbeteren. Er is nadien geen risicoanalyse meer uitgevoerd. Doordat het ziekenhuis niet periodiek een risicoanalyse uitvoert heeft het ziekenhuis geen actueel beeld van risico's, waar het ziekenhuis rekening mee dient te houden. Hierdoor loopt het Atrium MC 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 scores

De interim manager ICT is sedert 1 januari 2007 verantwoordelijk voor informatiebeveiliging. De voorzitter van de Raad van Bestuur is eindverantwoordelijk voor ICT. Besloten is om de verantwoordelijkheid voor informatiebeveiliging bij een aparte functionaris (security officer) onder te brengen. Er wordt actief geworven voor een security officer, met vaardigheden zowel in het ICT- technische als op het organisatorische vlak. Dit blijkt niet eenvoudig te zijn. Er is nagedacht over plaats en functie in de organisatie. Tijdens het onderzoek is geen taakomschrijving van de security officer ter beschikking gesteld. Het is op het moment van het onderzoek nog niet mogelijk om te beoordelen hoe de rol van de security officer zal worden ingevuld.

Er zijn enkele externe beoordelingen geweest (ICT audit en NIAZ accreditatie). Tijdens de ICT audit zijn de technische infrastructuur en procedures voor back-up, restore en recovery onderzocht. Het is niet bekend of er een specifieke beoordeling van de informatiebeveiliging heeft plaatsgevonden. De prioriteiten van de ICT organisatie liggen op dit moment bij de hervorming van de ICT structuur. Er zijn geen plannen voor een externe toets van de NEN 7510 norm.

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

Er vindt elektronische gegevensuitwisseling met huisartsen plaats. Huisartsen kunnen via een beveiligde verbinding gegevens van hun eigen patiënten inzien. Huisartsen maken voor de toegang tot het netwerk gebruik van een token. Er zijn met huisartsen afspraken gemaakt over de wijze, waarop de patiëntgegevens mogen worden gebruikt. Het is niet mogelijk om te controleren wie precies welke informatie inziet. De eindverantwoordelijkheid voor het inzien van patiëntgegevens via de token ligt bij de huisarts. Leveranciers hebben geen directe toegang tot de informatiesystemen. Er zijn met leveranciers afspraken gemaakt voor onderhoudswerkzaamheden. Er wordt een inventarisatie van externe data-uitwisselingen gemaakt, maar deze is nog niet afgerond.

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 een gedragscode en deze wordt dagelijks bij het opstarten van de pc onder de aandacht van de medewerkers gebracht. In deze gedragscode is vastgelegd hoe medewerkers met ICT middelen en patiëntgegevens moeten omgaan. Er is steekproefsgewijs toezicht op de naleving van de gedragscode. Vorig jaar is geconstateerd dat de gedragscode door een medewerker is overtreden. Als gevolg daarvan is de betreffende medewerker ontslagen. Sindsdien is het aantal overtredingen minimaal. De noodzaak van het handhaven van een gedragscode wordt onderkend. In het patiënten informatiesysteem kan door de behandelend arts gecontroleerd worden wie een patiëntendossier heeft geraadpleegd. Dit wordt wekelijks steekproefsgewijs gecontroleerd. Het is niet bekend hoe groot de steekproef is. Overtreders worden direct gemeld aan de Raad van Bestuur.

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 een beleid voor fysieke toegang tot ruimten, gebaseerd op een combinatie van passen en sleutels. Met behulp van het loggen van de passen kan nagegaan worden wie tot welke ruimten toegang heeft gehad. Medewerkers spreken elkaar er op aan, indien zij onbevoegd proberen toegang te verkrijgen tot de afgesloten ruimten.

Er is een beleid voor het verlenen van toegang tot informatie. Er zijn functionele autorisaties opgesteld en procedures voor het verkrijgen van toegang tot de informatiesystemen. Dit beleid omvat ook adequate regelingen voor co-assistenten en assistenten en het vermijden van groepsaccounts. Er wordt gewerkt met meerdere passwords voor toegang tot informatiesystemen. Dit wordt door medewerkers als gebruikersvriendelijk ervaren. Er zijn geen groepsaccounts. Bepaalde gevoelige informatie kan worden afgeschermd. Door de combinatie met het EPD wordt het door de medewerkers als onwenselijk gezien om gebruik te maken van andermans accounts, ook als die openstaan.

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

Er is een gedragscode. De in deze gedragscode relevante wetgeving wordt geactualiseerd. De privacycommissie en de patiëntenraad worden betrokken bij de actualisatie van de gedragscode. Afwijkingen van de gedragscode worden bij de Raad van Bestuur gemeld. Er wordt niet stelselmatig getoetst of regels nog goed worden toegepast. Er is een procedure voor het uitoefenen van 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 een incidentmanagementsysteem. Voor het melden van incidenten is een protocol. Incidenten met patiënten worden volgens de Meldingen Incidenten Patiënten (MIP) procedure afgehandeld. Er is geen specifieke procedure voor informatiebeveiligingsincidenten. Er is een procedure voor het behandelen van ICT calamiteiten, waarbij onder andere gebruik wordt gemaakt van incidentmanagers per type incident. Beveiligingsincidenten worden niet apart gelabeld. Er zijn nog weinig meldingen van incidenten met betrekking tot informatiebeveiliging.

3 Conclusie

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

Hierbij is door 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 op het volgende neer.

Ad. 1) De interim ICT manager is verantwoordelijk voor de informatiebeveiliging. De voorzitter van de Raad van Bestuur heeft ICT in zijn portefeuille. Er is besloten om voor informatiebeveiliging een aparte functionaris aan te stellen. Het ziekenhuis geeft aan dat het echter moeilijk is om de juiste persoon hiervoor aan te trekken. De ICT voorzieningen zijn door een extern bureau beoordeeld. De beoordelingen zijn vooral technisch van aard geweest. Het is onduidelijk of er aandacht besteed is aan informatiebeveiliging.

Ad. 2) Er is gegevensuitwisseling met huisartsen. Dit vindt via een beveiligde verbinding plaats. Met huisartsen zijn afspraken gemaakt over de wijze waarop gegevens mogen worden ingezien. Door het ziekenhuis wordt geïnventariseerd welke externe dataverbindingen er zijn.

Ad. 3) Er is een gedragscode opgesteld voor het gebruik van ICT middelen en hoe medewerkers met patiëntgegevens moeten omgaan. De naleving van de gedragscode wordt steekproefsgewijs gecontroleerd. Indien nodig worden er disciplinaire maatregelen getroffen.

Ad. 4) Er is een beleid voor de fysieke toegang tot specifieke ruimten gedefinieerd. In de praktijk wordt de naleving hiervan gecontroleerd. De cultuur binnen het ziekenhuis is dat medewerkers elkaar aanspreken, indien collega's onbevoegd toegang proberen te krijgen tot specifieke ruimten die niet voor iedereen toegankelijk zijn. Er is een beleid voor het verlenen van toegang tot informatie. Er zijn functionele autorisaties opgesteld en procedures voor het verkrijgen van toegang tot de informatiesystemen. Er wordt gewerkt met meerdere passwords voor toegang tot informatiesystemen.

Ad. 5) Er is een gedragscode. Bij overtreden van de gedragscode kunnen disciplinaire maatregelen volgen. De gedragscode wordt geactualiseerd. De privacycommissie en de patiëntenraad zijn hierbij betrokken.

Ad. 6). Er is een procedure voor het melden van ICT incidenten en incidenten met patiënten. Informatiebeveiligingsincidenten worden niet apart geregistreerd.

Uit het onderzoek blijkt dat het Atrium MC niet periodiek een risicoanalyse uitvoert. Het management van het Atrium MC 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 nog niet in voldoende mate sprake is van een passend beveiligingsniveau zoals bedoeld in art. 13 Wbp, evenmin is voldaan aan de voorwaarden om verantwoorde zorg te leveren, zoals bedoeld in artikel 2 van de kwaliteitwet 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 gevestigde 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 kwaliteitwet 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 Atrium MC zijn verkregen uit gesprekken met:

- dhr. E. Zijlstra, voorzitter Raad van Bestuur
- dhr. W. van Halteren, ICT manager interim
- dhr. T. van Diepen, neuroloog

De volgende documenten werden tevoren toegezonden:

- geen documenten ontvangen

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.