



**Rapport van bevindingen en conclusie naar  
aanleiding van het onderzoek 'informatiebeveiliging  
in ziekenhuizen' in Medisch Centrum Haaglanden te  
Den Haag op 13 april 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	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 13 april 2007 een bezoek gebracht aan het Medisch Centrum Haaglanden te Den Haag. 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<sup>1</sup> 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 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.

---

<sup>1</sup> 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.

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 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 Medisch Centrum Haaglanden. Achtereenvolgens worden twee vragen beantwoord:

- Hoe scoort het Medisch Centrum Haaglanden 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 Medisch Centrum Haaglanden? (hoofdstuk 3)

## 2 Resultaten inspectiebezoek

### 2.1 Inleiding

In dit hoofdstuk leest u hoe het Medisch Centrum Haaglanden 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.

Van het Medisch Centrum Haaglanden is een procedure voor risico-classificatie ontvangen. Alhoewel er verschillende interne- en externe beoordelingen van de informatievoorzieningen hebben plaatsgevonden, is er geen specifieke risico-analyse uitgevoerd naar de informatiebeveiliging binnen het ziekenhuis. Hierdoor loopt het ziekenhuis het gevaar dat 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 verantwoordelijkheid voor informatiebeveiliging is bij enkele medewerkers ondergebracht. Er is dus niet één specifieke medewerker die verantwoordelijk is voor informatiebeveiliging. De coördinator informatiebeveiliging is verantwoordelijk voor de meeste taken op het gebied van informatiebeveiliging. Het ziekenhuis heeft uitgebreid stilgestaan bij de taken en rollen waar informatiebeveiliging uit bestaat. Het document waarin die rollen en taken beschreven zijn, is echter (nog) niet vastgesteld. In de begroting is ruimte gereserveerd voor informatiebeveiliging.

Het ziekenhuis heeft informatiebeveiliging op meerdere wijzen getoetst en laten toetsen. De quick scan NEN 7510 is uitgevoerd en externe beoordelaars hebben op onderdelen aspecten van de beveiliging getoetst. Uit de toetsen zijn verschillende acties gevolgd en is een informatiebeveiligingsbeleid en –plan opgesteld. Na de uitvoering van de maatregelen ter verbetering van de informatiebeveiliging zullen controles worden uitgevoerd.

## 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**

Met de groep van huisartsen zijn afspraken gemaakt over de het verzenden en ontvangen van patiëntgegevens langs elektronische weg. De huisartsen hebben een contract voor gegevensuitwisseling met de operator van het zorgnetwerk afgesloten. De leverancier van de software van het ziekenhuisinformatiesysteem heeft de mogelijkheid tot elektronische toegang tot de informatiesystemen. Er zijn afspraken gemaakt onder welke voorwaarden onderhoud op de informatiesystemen plaats kan vinden. Dit is niet contractueel vastgelegd. De afspraken zijn wel vastgelegd in een procedure.

Medewerkers kunnen via een beveiligde verbinding (Virtual Private network met een RSA token) van huis uit werken.

**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 geen gedragscode voor de wijze waarop de medewerkers met patiënteninformatie moeten omgaan. Medewerkers tekenen bij in dienst treden wel een geheimhoudingsverklaring. Er is binnen het Medisch Centrum Haaglanden een project gestart, waarin aandacht wordt besteed aan de uitwerking van gedragscodes en regels in het algemeen. Hierin wordt ook de informatiebeveiliging meegenomen. Er is tevens een project gestart om het bewustzijn van medewerkers rond informatiebeveiligingsaspecten te vergroten. Medewerkers worden in dit project actief betrokken bij het definiëren van de 'ideale medewerker'. Hierbij is de omgang met patiëntgegevens een belangrijk aandachtspunt. Er is wel een gedragscode voor het omgaan met Internet en e-mailverkeer. In het ziekenhuis worden regelmatig 'veiligheidsrondes' gelopen. Tijdens deze veiligheidsrondes, waar de leden van de Raad van Bestuur aan deelnemen, wordt aandacht geschonken aan de veiligheid van de informatie. Medewerkers worden erop aangesproken, indien onzorgvuldig met patiëntgegevens wordt omgegaan.

## 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<sup>[2]</sup> 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 zijn regels vastgelegd voor de toegang tot specifieke ruimten. Iedere avond wordt gecontroleerd of deze ruimten afgesloten zijn. Sommige ruimten zijn niet altijd afgesloten. Hierover wordt maandelijks door beveiligingsambtenaren gerapporteerd. Naar aanleiding van deze rapportages worden verbeteringen in de toegangsbeveiliging doorgevoerd.

Er is een procedure voor wat betreft het verlenen van toegang aan medewerkers tot de informatiesystemen. Ondanks de regelingen voor toegang tot informatie zoals de autorisatieregeling, de regeling uitdiensttreding, is het systeem niet sluitend. Er wordt toch gebruik gemaakt van groepsaccounts en men werkt soms door op het account van een ander. Onderkend wordt, dat het gedrag van de medewerkers een sterk bepalende factor is bij dit onderwerp en men is zich ervan bewust dat hier nog veel aan verbeterd moet worden.

## 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.

<sup>[2]</sup> 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**

In het algemeen beleid is aandacht besteed aan de naleving van de Wbp en WGBO. Voor de veranderingen in de Wbp heeft het ziekenhuis drie jaar geleden een project opgestart waarmee de consequenties van die wijzigingen ziekenhuisbreed zijn ingevoerd. Een evaluatie heeft echter niet plaatsgevonden. Aan nieuwe medewerkers wordt bij indiensttreding duidelijk gemaakt welke regels er in het ziekenhuis gelden en daaronder vallen ook de consequenties van wettelijke regelingen. Daarnaast zijn er voor patiënten procedures vastgesteld op welke wijze zij het inzage- en correctierecht kunnen uitoefenen.

**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?			√	

**Toelichtingen op scores**

Er zijn gescheiden registraties van incidenten die betrekking hebben op ICT voorzieningen en die betrekking hebben op directe patiëntenzorg. Wanneer er incidenten zijn waarbij beide aspecten een rol spelen is niet duidelijk door wie het incident afgehandeld, geregistreerd en aan wie gerapporteerd wordt. Er is geen strategische keuze gemaakt voor rapportage van incidenten. Desondanks worden incidenten na melding grondig onderzocht en aangeprezen om verbeteringen te realiseren.

### 3 Conclusies

In dit onderzoek is onderzocht in welke mate bij het Medisch Centrum Haaglanden 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 op het volgende neer.

Ad. 1) Het ziekenhuis heeft de verantwoordelijkheid voor informatiebeveiliging bij verschillende medewerkers ondergebracht. Echter er is niemand benoemd op directieniveau, die verantwoordelijk is voor informatiebeveiliging. De bevoegdheden en taken op het gebied van informatiebeveiliging zijn in een beleidsdocument vastgelegd. Dit document moet nog worden vastgesteld.

De informatiebeveiliging wordt regelmatig, zowel intern als extern getoetst. Uit de beoordelingen volgen acties en ook hierop worden controles uitgevoerd.

Ad. 2) Er is uitwisseling van patiëntgegevens met derden. Met externe zorgverleners zijn afspraken gemaakt en deze zijn in contracten vastgelegd. Medewerkers die thuiswerken, werken via een beveiligde verbinding.

Ad. 3) Er is geen gedragscode voor de wijze waarop medewerkers met patiëntgegevens moeten omgaan. Het ziekenhuis heeft een project gestart om het bewustzijn rond informatiebeveiligingsaspecten bij medewerkers te vergroten.

Ad. 4) Er is beleid voor fysieke toegangsbeveiliging; in het bijzonder waar het gaat om toegang tot speciale ruimten in het ziekenhuis. Dit beleid wordt geëvalueerd en verbeteringen worden doorgevoerd. Er is een procedure voor het verlenen van toegang aan medewerkers tot de informatiesystemen. Beleid is dat medewerkers alleen op eigen naam een toegang tot het systeem krijgen. In de praktijk blijkt echter dat hiervan nog kan worden afgeweken omdat er met groepsaccounts wordt gewerkt.

Ad. 5) In het algemeen beleid is aandacht besteed aan de naleving van de Wbp en WGBO. Medewerkers worden bij indiensttreding over de implicaties van de Wbp en de WGBO geïnformeerd. Patiënten kunnen het inzage- en correctierecht uitoefenen.

Ad. 6). Er zijn gescheiden registraties van incidenten die betrekking hebben op ICT voorzieningen en die betrekking hebben op directe patiëntenzorg. Er zijn gescheiden registraties van incidenten die betrekking hebben op ICT voorzieningen en die betrekking hebben op directe patiëntenzorg. Wanneer er incidenten zijn, waarbij beide aspecten een rol spelen is niet duidelijk door wie het incident wordt afgehandeld, geregistreerd en aan wie gerapporteerd wordt.

Uit het onderzoek blijkt dat binnen MC Haaglanden geen risicoanalyse heeft plaatsgevonden. Het management van MC Haaglanden 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, 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 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 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 MC Haaglanden zijn verkregen uit gesprekken met:

- Dhr. P. van der Meer, voorzitter Raad van Bestuur
- Dhr. R. van Osch, Hoofd Interne Controle
- Dhr. A. Beckers, extern projectleider informatiebeveiliging
- Dhr. O. Jansen, manager automatisering
- Dhr. H. Lubout, senior informatie adviseur
- Dhr. L.C.F. Haans, gynaecoloog

De volgende documenten werden tevoren toegezonden:

- Adviesrapport MCH-ICT infrastructuur (18-12-2006, versie 1.4 definitief)
- Procedure risico-classificatie (ongedateerd)
- Informatiebeveiligingsbeleid (08-05-2006, versie 1.0)
- Bijlage informatiebeveiligingsbeleid (ongedateerd)
- Implementatieplan informatiebeveiliging (25-08-2006, versie 1.0)
- Bijlage planning en capaciteitsbegroting implementatieplan informatiebeveiliging (ongedateerd, versie 1.3)
- Rapport "Rollen / taken en verantwoordelijkheden" van informatiebeveiliging (12-01-2007, versie 1.0)
- Samenvatting informatiebeveiligingsbeleid t.b.v. medewerkers (niet gedateerd)
- Jaarrapportage automatisering 2006 (januari 2007)
- Maandrapportage automatisering januari 2007 (februari 2007)
- Rapportage beoordeling firewall omgeving (19-06-2006, conceptversie)
- Rapportage beoordeling netwerkomgeving (18-01-2007, versie 1.0 definitief)

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.