



**Rapport van bevindingen en conclusie naar
aanleiding van het onderzoek 'informatiebeveiliging
in ziekenhuizen' in het Erasmus Medisch Centrum
te Rotterdam op 29 maart 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	10
2.8	Incidenten.....	10
3	Conclusies	12

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 29 maart 2007 een bezoek gebracht aan het Erasmus Medisch Centrum (Erasmus MC) te Rotterdam. 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 Erasmus MC te Rotterdam. Achtereenvolgens worden twee vragen beantwoord:

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

2 Resultaten inspectiebezoek

2.1 Inleiding

In dit hoofdstuk leest u hoe het Erasmus 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.

In 2006 is een inventarisatie uitgevoerd van de situatie van de informatiebeveiliging binnen het Erasmus MC. Uit deze inventarisatie zijn risico inschattingen gemaakt. Op basis hiervan zijn aanbevelingen opgesteld voor te nemen maatregelen. De resultaten hiervan zijn geëvalueerd en geprioriteerd.

Het management van het Erasmus MC heeft daardoor voldoende zicht op de risico's die het ziekenhuis op het gebied van informatiebeveiliging loopt.

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

Er is een functionaris (Security Officer SO) met een duidelijke taak- en functie omschrijving, deze wordt geëvalueerd en aangepast. Er is een voor zover te beoordelen adequaat budget voor deze functie. De functionaris wordt ingeschakeld indien dat vanuit oogpunt van informatiebeveiliging wenselijk is. De functionaris heeft voldoende inbedding in de organisatie om in te kunnen signaleren wanneer het wenselijk is om ongevraagd advies te geven. Er is een functionaris gegevensbescherming (FG), deze heeft een organisatorisch vergelijkbare inbedding.

Er is een externe audit, in het kader van de jaarrekening, door de accountant uitgevoerd. Daarnaast wordt de Status Informatiebeveiliging gebruikt en is met instemming van de Raad van Bestuur de houding van het personeel ten aanzien van informatiebeveiliging extern getoetst. Bij die laatste toetsing is duidelijk geworden dat het noodzakelijk is om intensieve aandacht te besteden aan de cultuuraspecten van informatiebeveiliging. Mede op basis daarvan zal met alle academische ziekenhuizen samen een voorlichtingscampagne gestart worden. Het is niet duidelijk in hoeverre de accountant geaccrediteerd is voor het toetsen van de NEN 7510 in de volle breedte (voor zoverre relevant).

De NVZ/NEN monitor is in 2006 toegepast.

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

Het Erasmus MC wisselt op vele manieren informatie uit met externe partijen. Met huisartsen worden laboratoriumgegevens en ontslagbrieven elektronisch uitgewisseld. Het ziekenhuis is zich voldoende bewust van het risico dat externe partijen vormen voor de veiligheid van de aan de organisatie toevertrouwde informatie. Er is een voldoende veilige infrastructuur in ontwikkeling om deze informatie verantwoord aan te bieden. Er zijn voor de uitwisseling van gegevens met derden standaardcontracten opgesteld. Externen moeten een gedragscode tekenen. Het beheer van contracten met externe partijen is echter slechts beperkt ingericht. Op dit moment zijn deze voorwaarden nog niet contractueel vastgelegd met alle relevante partijen. Deze contracten worden thans ontwikkeld. Er wordt een Transmuraal Informatie Platform (TIP) en een patiëntenportaal ontwikkeld. Er wordt tevens een 'etalage' waarin alleen gecontroleerd gegevens beschikbaar worden gesteld ontwikkeld. Toegang tot dat systeem zal alleen via een Uzipas mogelijk worden.

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 aanwezig in het ziekenhuis en aangegeven is dat deze is geïmplementeerd. Tijdens een afdelingsbezoek wordt duidelijk dat deze implementatie nog niet de afdeling heeft bereikt. Alle pc's zijn toegankelijk. Het is zeer eenvoudig toegang te krijgen tot patiënteninformatie. Statussen liggen in stapels op bureaus van medewerkers die zelf niet aanwezig zijn. Ruimten waar veel informatie aanwezig is zijn verlaten, terwijl pc's aanstaan en de afwezige medewerker is ingelogd in een patiëntendossier. Er is een communicatiecampagne in voorbereiding om het bewustzijn op dit gebied te vergroten. Het is ook duidelijk dat de eerdere gepubliceerde inbreuk op de beveiliging van het netwerk in het Erasmus MC² niet heeft geleid tot een minimaal

² Het Erasmus MC heeft meegedaan aan een test of de beveiliging van het netwerk van het ziekenhuis te kraken was.

voldoende bewustzijn. Het is overigens duidelijk dat dit probleem bekend is bij de verantwoordelijken.

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 engineering³ is onderkend en er zijn hiertegen 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 beleid voor de fysieke toegangsbeheersing, gebaseerd op pasjes en camera's. Iedereen heeft een pas, ongeveer de helft van de medewerkers draagt deze pas zichtbaar. De pas geeft toegang tot kritische ruimten. Tijdens het onderzoek blijkt dat het in de praktijk eenvoudig is om met een willekeurige medewerker mee te lopen en zo toegang te krijgen tot een ruimte. Schoonmakers hebben toegang tot ruimten met vertrouwelijke informatie. Het is bij de geïnterviewden niet bekend of deze schoonmakers een geheimhoudingsclausule in het contract hebben. De mate waarin medewerkers zich houden aan de voorgestelde regelingen, blijkt de voornaamste beperkende factor te zijn. Het beleid is geïmplementeerd, echter uit een intern uitgevoerde meting blijkt dat voor de fysieke beveiliging beperkte maatregelen zijn getroffen en uit de risicoanalyse blijkt dat hier verder prioriteit aan moet worden gegeven.

Er is geen formeel beleid rond het voorkomen van toegang tot informatie door onbekenden. Er wordt wel gewerkt met een matrix waarin bepaald is welke functies tot welke informatiesystemen toegang hebben. Er zijn regelmatige tests om medewerkers scherp te houden. Hierbij wordt gebruik gemaakt van maatregelen om social engineering te voorkomen. Bij bezoek aan de afdeling blijkt echter duidelijk dat de praktische uitwerking onvoldoende is om ongewenste toegang te voorkomen. Er zijn

³ Bij deze tactiek probeert iemand informatie los te krijgen bij personeel, om zodoende toegang te krijgen tot het ziekenhuisnetwerk.

groepsaccounts en pc's staan open. Noodprocedures zijn onderdeel van de reguliere bedrijfsvoering en worden niet merkbaar gecontroleerd. Tijdens het bezoek aan de afdeling blijkt dat er geen merkbare beveiliging aanwezig is van patiënteninformatie die op papier is opgeslagen.

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

	<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 beleid opgesteld over het behandelen van patiënteninformatie. Er zijn procedures rond het inzien van patiënteninformatie. Een procedure voor het wijzigen van informatie is bij de geïnterviewde medewerkers niet bekend. Er is een geïmplementeerd privacy reglement.

Er is binnen Erasmus MC een Functionaris Gegevensbescherming (FG) benoemd. Taken van de FG zijn ingevuld. Uit het onderzoek blijkt dat de invulling als adviseur voor privacy aspecten binnen het ziekenhuis geïmplementeerd is. De taak van de FG als toezichthouder op naleving van de Wbp is formeel geregeld, maar het wordt niet in de praktijk toegepast.

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 systematische aanpak van incidenten, waarbij er aandacht is voor opschaling bij ernstige incidenten. Indien noodzakelijk kan er een Computer Emergency Response Team worden opgeroepen, dat ook problemen die zeer ernstig zijn kan aanpakken. Er is nog een beperkte scheiding in het systeem tussen type meldingen. Om het bewustzijn van het belang van informatiebeveiliging te vergroten is een '10-geboden kaart' ontwikkeld waarin de belangrijkste aandachtspunten voor informatiebeveiliging en het melden van beveiligingsincidenten zijn opgenomen.

Er is echter nog een beperkt bewustzijn van de noodzaak tot melden van informatiebeveiligingsincidenten.

3 Conclusies

In dit onderzoek is onderzocht in welke mate bij het Erasmus MC 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) Er is een functionaris aangesteld voor informatiebeveiliging. Voor deze functie is een duidelijke taak functieomschrijving opgesteld. Er worden externe audits op de informatiebeveiliging uitgevoerd.

Ad. 2) Men is zich bewust van de risico's van gegevensuitwisseling met derden. Er wordt mede gezien ontwikkelingen op ICT gebied een verdere invulling gegeven aan een veilige infrastructuur. De invulling van contracten met derden is hierbij echter nog onvoldoende gerealiseerd.

Ad. 3) Er is een gedragscode, de naleving hiervan is echter onvoldoende in praktijk gebracht.

Ad. 4) Er is beleid voor fysieke toegangsbeheersing; in het bijzonder waar het gaat om toegang tot speciale ruimten in het ziekenhuis. Uit interne controles blijkt dat de naleving hiervan in de praktijk onvoldoende is. Wat betreft de toegang tot informatie, heeft het ziekenhuis maatregelen getroffen. Deze maatregelen blijken in de praktijk echter onvoldoende te worden nageleefd.

Ad. 5) Er is beleid opgesteld voor de omgang met patiëntengegevens en er is een privacy reglement. In het ziekenhuis is een functionaris gegevensbescherming (FG) aangesteld. Echter het is onduidelijk hoe deze functie wordt ingevuld met betrekking tot de naleving van de Wbp.

Ad. 6) Er is een systematische aanpak voor het melden van incidenten. In de praktijk blijkt dat er onvoldoende besef voor de noodzaak van het melden van informatiebeveiligingsincidenten binnen het ziekenhuis bestaat.

Uit het onderzoek blijkt dat het Erasmus MC in 2006 een inventarisatie van de situatie van de informatiebeveiliging heeft uitgevoerd. Uit deze inventarisatie zijn risico inschattingen gemaakt. Op basis hiervan zijn aanbevelingen opgesteld voor te nemen maatregelen. De resultaten hiervan zijn geclassificeerd en geprioriteerd. Het management van het Erasmus MC heeft daardoor voldoende 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 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 Erasmus MC zijn verkregen uit gesprekken met:

- dhr. N. Bruens, Directeur ICT
- dhr. J.W. Schoemaker, Security officer
- mevr. C. Insinger, Lid Raad van Bestuur
- dhr. J. Kerrebijn, Medisch specialist
- dhr. P. van Hoogdalem, Functionaris gegevensbescherming

De volgende documenten werden tevoren toegezonden:

- Status informatiebeveiliging
- Risicoanalysemethode
- Informatiebeveiligingsbeleid
- Managementletter PricewaterhouseCoopers
- Classificatie van bedrijfsprocessen, informatiesystemen en informatie

Documenten ingezien/ meegekregen op de bezoekdatum:

- Conceptmanagementletter 2006 PricewaterhouseCoopers
- Profielschets Security Officer
- Classificatie Noshowsysteem cluster 8
- Continuïteitsplan thoraxcentrum
- Gedragscode voor het gebruik van computerfaciliteiten van het Erasmus MC
- Memo aan commissie patiëntengegevens
- Perspectief 2007
- Tien geboden voor informatiebeveiliging
- Surfnets uitdraai

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.