



**Rapport van bevindingen en conclusie naar  
aanleiding van het onderzoek  
'informatiebeveiliging in ziekenhuizen'  
in het Maasziekenhuis Pantein te Boxmeer  
op 22 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 .....	8
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 22 maart 2007 een bezoek gebracht aan Maasziekenhuis Pantein te Boxmeer. 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 Maasziekenhuis Pantein. Achtereenvolgens worden twee vragen beantwoord:

- Hoe scoort het Maasziekenhuis Pantein op de zes als indicator gekozen onderdelen uit de NEN 7510 norm, als voorwaarden voor verantwoorde zorg? (hoofdstuk 2)
- Wat zijn de conclusies van IGZ en het CBP, alle scores overziende, voor het Maasziekenhuis Pantein? (hoofdstuk 3)

## 2 Resultaten inspectiebezoek

### 2.1 Inleiding

In dit hoofdstuk leest u hoe het Maasziekenhuis Pantein 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.

Door het Maasziekenhuis Pantein is geen risicoanalyse uitgevoerd. Hierdoor loopt het Maasziekenhuis Pantein 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

In het ziekenhuis is geen specifiek beleid gericht op informatiebeveiliging. Uit de gesprekken blijkt wel dat aan diverse aspecten op het gebied van informatiebeveiliging aandacht wordt geschonken. Zo heeft het hoofd receptie een rol gekregen in het bewaken van het gedrag rond de beveiliging van informatie. Tevens wordt door het ziekenhuis aan verschillende onderdelen van de NEN 7510 norm aandacht besteed. Dit gebeurt echter niet systematisch.

De koepel van ziekenhuizen heeft aan de ziekenhuizen een instrument beschikbaar gesteld om na te gaan in hoeverre er tekortkomingen zijn bij de implementatie van de NEN 7510 norm. Dit instrument is binnen het Maasziekenhuis Pantein niet toegepast. In de externe beoordeling van de accountant wordt sinds twee jaar aandacht besteed aan aspecten van ICT en de NEN 7510 norm. Uit de accountantsrapportage blijkt echter dat dit niet de volledigheid heeft die bijvoorbeeld bij een externe audit van de informatiebeveiliging beschikbaar is. Bij de beoordeling is geen risico-inschatting gemaakt.

## 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**

Aan externe hulpverleners wordt alleen via het Edifact protocol op elektronische wijze gegevens verstuurd. Dit betreft het versturen van laboratoriumuitslagen, röntgenrapportages en informatie rondom opname en ontslag van patiënten. Externe hulpverleners kunnen niet de informatiesystemen van het ziekenhuis raadplegen. Medewerkers kunnen van huis uit gebruik maken van inbelmogelijkheden op het netwerk. Hiervoor worden RSA keys gebruikt. Hoewel men tekent voor ontvangst zijn er geen specifieke afspraken gemaakt over beveiligingsaspecten. Ook al is er een gedragsregel dat er over patiënten niet per e-mail wordt gecommuniceerd, blijkt uit de gesprekken dat er toch e-mailverkeer over patiënten plaatsvindt.

**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**

Aan de geheimhoudingsplicht wordt aandacht besteed in de aanstellingscontracten van medewerkers. Ten behoeve van het gebruik van Internet en e-mail is een gedragsreglement opgesteld. Door expliciet aandacht te schenken aan de wijze waarop medewerkers met informatie om (moeten) gaan wordt het mogelijk om daar daadwerkelijk op te sturen en het te beheren. Er is geen gedragscode specifiek voor informatiebeveiliging.

**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.

<sup>2</sup> Bij deze tactiek probeert iemand informatie los te krijgen bij personeel, om zodoende toegang te krijgen tot het ziekenhuis.

### 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 de scores

Er is geen algemeen beleid aanwezig voor de fysieke informatiebeveiliging. Er zijn wel specifieke maatregelen genomen, die apparatuur en informatie fysiek moeten beschermen. Met name is er aandacht geschonken aan het beperken van de toegang tot bepaalde ruimten.

Voor de toegang tot informatie zijn (vele) maatregelen genomen om te voorkomen dat onbevoegden bij informatie kunnen. Het blijkt echter, dat ook deze maatregelen niet op een specifiek beleid berusten. Daarnaast blijkt dat de maatregelen niet compleet zijn. Ondanks een autorisatiestructuur is het mogelijk om op openstaande pc's verder te werken onder iemand anders autorisatie. Voor sommige medewerkers zijn alle patiëntgegevens toegankelijk, terwijl zij met vele patiënten nooit iets te maken zullen hebben. Gegevens zijn hierdoor vrij gemakkelijk voor onbevoegden toegankelijk.

## 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**

Het ziekenhuis geeft aan dat met bepaalde aspecten uit de hiervoor genoemde regelgeving rekening wordt gehouden. Er zijn geen structurele voorzieningen in het ziekenhuis getroffen, die ervoor zorgen dat deze regelgeving in het ziekenhuis is geïmplementeerd.

Er zijn bijvoorbeeld geen ziekenhuisbrede instructies hoe medewerkers om moeten gaan met verzoeken van patiënten of van familieleden om inzage van gegevens.

**2.8 Incidenten****IJKpunten incidenten**

Er is beleid voor het melden, registreren en afhandelen van incidenten vastgesteld. Deze afspraken zijn bij alle medewerkers bekend. Men houdt zich aan deze afspraken.

Afwijkingen van deze afspraken worden gerapporteerd en adequaat afgehandeld.

**Scores**

	<i>Afwezig</i>	<i>Aanwezig</i>	<i>Operationeel</i>	<i>Geborgd</i>
Wat is de status van het beleid rondom beveiligingsincident melding en afhandeling?		√		

**Toelichting op scores**

Er is een procedure om incidenten te melden en te registreren. Wanneer patiënten betrokken zijn bij het incident heeft men de neiging om de melding in te brengen bij de MIP commissie. Onder MIP commissie wordt verstaan: meld incidenten met patiënten. Incidenten over informatiebeveiliging worden alleen bij de helpdesk gemeld. Er vindt geen periodieke rapportage van de incidenten aan de directie van de instelling plaats.

### 3 Conclusies

In dit onderzoek is onderzocht in welke mate bij het Maasziekenhuis Pantein 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 daarbij 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 is onvoldoende duidelijk binnen het ziekenhuis wie verantwoordelijk is voor de informatiebeveiliging. In de accountantsbeoordeling wordt in beperkte mate aandacht besteed aan de beoordeling van de informatiebeveiliging.

Ad. 2) Men is zich bewust van de risico's van gegevensuitwisseling met derden. Indien medewerkers van huis uit toegang krijgen tot het netwerk moeten zij tekenen voor ontvangst van de RSA key. Er zijn echter geen specifieke afspraken gemaakt over veiligheidsaspecten.

Ad. 3) Er is geen specifieke gedragscode opgesteld voor informatiebeveiliging.

Ad. 4) Er zijn maatregelen getroffen voor de fysieke toegangsbeveiliging. Deze maatregelen berusten echter niet op een duidelijk beleid.

Voor wat betreft de toegang tot patiënteninformatie zijn eveneens maatregelen getroffen. Deze maatregelen berusten echter evenmin op een specifiek beleid.

Ad. 5) Er is voor de naleving van relevante wetgeving geen beleid. Er is geen privacy gedragscode en er zijn geen procedures voor patiënten, die inzage in hun medische gegevens willen hebben.

Ad. 6) Er is een structuur voor het melden van incidenten. Er wordt echter niet in voorzien dat incidenten worden gerapporteerd aan het management. Hierdoor heeft het ziekenhuis geen maatregelen getroffen waarmee op directieniveau op incidenten gestuurd kan worden.

Uit het onderzoek blijkt dat het Maasziekenhuis Pantein geen risicoanalyse heeft uitgevoerd. Het management van het Maasziekenhuis Pantein 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 geen 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 Maasziekenhuis Pantein zijn verkregen uit gesprekken met:

- Dhr. R. Verreussel, directeur Maasziekenhuis Pantein
- Dhr. T. Jacobs, directeur Service Bedrijf
- Dhr. J. Farla, unithoofd ICT
- Dhr. G. de Wildt, coördinator Automatisering
- Dhr. P. van Rijssel, kinderarts

De volgende documenten werden tevoren toegezonden:

- Memo naar aanleiding van accountantsrapport 2006, d.d. 14-7-2006
- Voorbeeld van een risico-analyse, waarlangs alle systemen beoordeeld zullen worden, versie 1.4 d.d. 13-03-2007
- Beveiligingstructuur extern netwerk, internetverkeer en VPN-verkeer, ongedateerd
- Back-up procedure, ongedateerd
- Conceptnotitie beschikbaarheid van de infrastructuur in relatie tot NEN 7510 norm, versie V3.0, d.d. 26-02-2007

Tijdens het bezoek is ingezien:

- Concept informatiseringsbeleid 2006-2011, d.d. 31-01-2007.
- Accountantsrapport

Namens IGZ en CBP werden de gesprekken gevoerd door,

- Mw. A.C. Gräve, privacy auditor CBP
- Mw. S. Riezebos, programmamedewerker/notulist IGZ
- 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.