

Informatiebeveiliging in de zorg

De Inspectie voor de Gezondheidszorg heeft in het verleden geconstateerd dat ziekenhuizen onvoldoende aandacht schenken aan de risico's die de toepassing van ICT met zich meebrengt. De auteur noemt als een van de hoofdoorzaken hiervan dat informatiebeveiliging nog te veel een zaak is van specialisten die te weinig aandacht hebben voor het geheel. Ook houden vrijwel uitsluitend hoofden informatievoorziening zich bezig met die beveiliging en kunnen ze onvoldoende het lijnmanagement en de directies erbij betrekken. Zorgvuldig handelen en de geheimhoudingsbelofte van medici volstaan bovendien niet meer om te voorkomen dat medische fouten optreden.

Dit boek gaat over het voordeel van beveiliging indien betrokkenen het nut en de noodzaak ervan inzien en beveiliging niet als een hindernis ervaren. Met andere woorden: het gaat over het oplossen van de paradox dat goed bereikbare informatie voorhanden is, terwijl de privacy van een patiënt gewaarborgd blijft.

Na een inventarisatie van betrokkenen en standpunten in de zorg beoordeelt de auteur de diverse wetten en normen en komt hij met voorstellen om de bescherming van informatie en beveiliging op een hoger plan te tillen.

Het boek is in de eerste plaats bedoeld voor hoofden informatievoorziening, projectleiders en andere informatie- en automatiseringsdeskundigen, maar zeker ook voor juridische medewerkers, afdelingsmanagers en directieleden die de beveiliging op een hoger peil willen brengen.

Het boek bevat interessante praktijkverhalen en opiniërende hoofdstukken over de rol van de wet en de informatievoorziening.

J.A. van der Wel is directeur van Comfort Information Architects en lid van de NEN-normcommissie voor informatiebeveiliging in de zorg. Hij publiceert geregeld in vaktijdschriften over beveiliging en informatieuitwisseling in de zorg.

Informatiebeveiliging in de zorg J.A. van der Wel

Informatiebeveiliging in de zorg

ISBN 90 395 2498 X

NUR 981/870



9 789039 524985

www.academicservice.nl



Informatiebeveiliging in de zorg

J.A. van der Wel

Academic Service, 2006

Deel I Overzicht

3	De betrokkenen.....	11
3.1	Inleiding.....	11
3.2	Medici, verplegend personeel als gebruikers van ICT.....	12
3.3	Directies van zorginstellingen	13
3.4	Patiënten.....	13
3.5	Het hoofd ICT	14
3.6	Software leveranciers	16
3.7	Quick Scan van informatiegebruik en - beveiliging.....	16
4	Basisbegrippen.....	18
4.1	Inleiding.....	18
4.2	Informatievoorziening	19
4.3	Bedrijfsorganisatie	21
4.4	Gedrag, attitude, opvattingen.....	22
4.5	Argumentatieschema	23
4.6	Voorkomen of genezen?	25
5	Informatiebeveiliging in regels.....	27
5.1	Inleiding.....	27
5.2	Geschiedenis.....	28
5.3	Wetten en normen in de IM-kaart	29
5.4	Informatiebeveiliging in de wet.....	30
5.5	De norm voor informatiebeveiliging in de zorg	33

Deel II Verbeteren en beheren

6	Voorwaarden voor verbeteren	38
6.1	Inleiding.....	38
6.2	Bouw gelijk goed	38
6.3	Snel op zoek naar oorzaken	39
6.4	Motivatie	40
7	Faseren.....	42
7.1	Inleiding.....	42
7.2	Faseren en informatiebeveiliging.....	43
7.3	Mogelijkheden om te starten	51
7.4	Organiseren van de verandering	52
8	Onderzoeksmethoden.....	55
8.1	Inleiding.....	55
8.2	Informeel onderzoekstechnieken.....	56
8.3	Formele methoden.....	56
8.4	Kwantificeren	62
8.5	Aangifte doen van Cybercrime	64
8.6	Administratie	65

Deel III Regels, normen, methoden

9	Inhoud van medische registraties.....	68
9.1	Inleiding.....	68
9.2	Bevoegdheid.....	69
9.3	Registratieplicht	71
9.4	Vernietigingsbevoegdheid en –plicht.....	71
10	Gegevensuitwisseling binnen de zorg.....	74
10.1	Inleiding.....	74
10.2	De wettelijke regeling.....	74
10.3	De praktijk van ICT.....	77
10.4	Raadplegen van het dossier door de patiënt	79
11	Verantwoordelijkheden.....	80
11.1	Inleiding.....	80
11.2	Verantwoordelijkheden volgens de wet	81
11.3	Verantwoordelijkheden - bedrijfsorganisatie	84
12	Procedures informatiefunctie	89
12.1	Inleiding.....	89
12.2	Beleid	89
12.3	Classificatie	90
12.4	Personeel	92
12.5	Fysieke beveiliging en beveiliging van de omgeving	93
12.6	Continuïteitsbeheer.....	94
12.7	Transparantie.....	95
13	Naleving.....	97
13.1	Inleiding.....	97
13.2	Naleving in de NEN7510	97
13.3	Toezicht op handelen van leveranciers	98
14	ICT-procedures	99
14.1	Inleiding.....	99
14.2	Operationeel beheer informatie - en communicatievoorzieningen.....	99
14.3	Toegangsbeveiliging.....	101
14.4	Aanschaf, ontwikkeling en onderhoud van informatiesystemen.....	103
14.5	Beveiligingsincidenten	104
14.6	Acceptatietesten.....	105

Deel IV Opinies

15	Groei-model voor informatiebeveiliging	108
16	Geeft de wet voldoende richting?	114
16.1	Kernpunten voor uitwerking	115
16.2	Wat recht is, dat bepaalt de software	116
16.3	Klaar?.....	116
17	Bijlage 1 Woordenlijst	117
18	Bijlage 2 Samenvatting wetsartikelen	119
18.1	Wbp	119
18.2	Wgbo.....	122
18.3	Wet op de jeugdzorg.....	123
18.4	Wet Bopz.....	124

18.5 Wet BIG	124
18.6 Strafrecht.....	125
19 Bijlage 3 Index.....	126

1 Inleiding

Allerlei theorieën¹ ten spijt, zijn er grote hiaten te constateren in procedures voor IT-beheer. Sterke punten van de bestaande benaderingen zijn het overzicht en de theoretische compleetheid. De zwakke kant is dat wanneer alles van die theorieën wordt toegepast, in veel gevallen de boel vastloopt. Informatiebeveiliging ontstaat niet door het kopiëren van richtlijnen en normen; dat leidt tot een beveiliging waarvan het doel onduidelijk is bij betrokkenen.

Een risicobenadering is nuttiger, dan wordt duidelijk wat volledig, wat deels en wat heel informeel hoeft te worden geïmplementeerd. Informatiebeveiliging moet worden ontworpen, met richtlijnen en normen als hulp; daarvoor is het nodig de belangen van betrokkenen als uitgangspunt te nemen. De probleemstelling van dit boek luidt dan ook: *Welke kritieke factoren zijn van invloed op het verbeteren van dienstverlening en welke condities moeten daarbij zijn vervuld?*

Dit boek gaat over het beschermen van persoonsinformatie en beveiligen van informatievoorziening in de zorg. Bescherming en beveiliging werken alleen maar als de mensen, de hulpverleners in gezondheidszorg, jeugdzorg en psychiatrie en de patiënten en cliënten die beveiliging als prettig ervaren omdat nut en noodzaak van de procedures duidelijk zijn.

Het is een misvatting te denken dat informatiebeveiliging een taak is van de IT. Het is een taak van iedereen; ook het opruimen van het bureau hoort ertoe. Dit boek gaat *niet* over de kettingen en sloten die nog te vaak de boeken en congresfolders over dit onderwerp ontsieren. Daarmee wordt informatie moeilijk bereikbaar gemaakt, terwijl de zorg juist vraagt om goed bereikbare en liefst nog béter bereikbare informatie, met behoud van privacy van de patiënt en niet te vergeten de hulpverlener.

Dit boek gaat *wel* over een leer- en investeringsproces voor organisaties en maatschappij. De hulpmiddelen daarbij zijn praktische risicoanalyses, juridische, organisatorische en technische checklisten, concrete plannings. Transparante organisaties zijn nodig, waarin de vele disciplines – medici, juristen, managers, directieleden en vanzelfsprekend ook de informatie- en automatiseringsspecialisten – nauw samenwerken.

Beveiliging heeft altijd een paradox in zich: informatie beter bereikbaar maken met behoud van privacy.

1.1 Voor wie is dit boek bedoeld?

Dit boek is allereerst bestemd voor hoofden informatievoorziening in de zorg, projectleiders informatievoorziening en andere informatie- en automatiseringdeskundigen. Daarnaast is het boek bestemd voor afdelingsmanagers en directieleden die informatiebeveiliging in hun zorgorganisatie op een hoger plan willen brengen. Ook beleidsmedewerkers, medewerkers van koepelorganisaties en studenten kunnen hun voordeel doen met dit boek.

Het boek geeft de eerste doelgroep naast methoden om effectiever om te gaan met bescherming van persoonsgegevens en informatiebeveiliging in hun organisatie, een overzicht van de relevante wetgeving.

Zorgmanagers kunnen met dit boek hun kennis vergroten om meer en concreter invloed uit te oefenen op de uitdijende geautomatiseerde systemen. Dat is nodig omdat zorgvuldig handelen en de persoonlijke geheimhoudingsbelofte van medici al lang niet meer volstaat om te voorkomen dat medische fouten optreden, of om het medisch beroepsgeheim te handhaven. Aan directies en beleidsmedewerkers van zorginstellingen die een overzicht willen hebben van de vraagstukken die spelen, geeft het boek handvatten die nodig zijn om sturing te geven aan de bescherming van persoonsgegevens en beveiliging van informatiesystemen.

1.2 Hoe zit het boek in elkaar?

Deel I is een overzicht van de redenen die verschillende betrokkenen zoals hulpverleners, patiënten en cliënten, directies en hoofden ICT geven aan informatiebeveiliging (hoofdstuk 2). Daarbij blijkt dat beveiligingsvraagstukken op verschillende plaatsen in de organisatie anders worden beoordeeld. Zo is de wettelijke bewaartermijn, ooit door de wetgever bedacht als privacybeschermende maatregel, voor medici een ergernis omdat waardevolle kennis en ervaring verdwijnt, voor automatiseerders een ontwerpcriterium, en voor directies een mogelijkheid om archiefkosten te beheersen. Onderkennen van dit soort tegenstrijdige doelstellingen is belangrijk voor het succes van beveiligingsprojecten. In dit hoofdstuk komt ook naar voren dat men met verschillende onderzoeksmethoden tot tegenovergestelde antwoorden kan komen op de vraag waarom de informatievoorziening van een organisatie kuren vertoont.

In het verlengde van deze constatering komen in hoofdstuk 3 aan de orde de drie gebieden waaraan aandacht moet worden geschonken om van informatiebeveiliging een succes te maken. Die gebieden zijn de componenten van het informatiesysteem, de samenwerking tussen de betrokken in de bedrijfsorganisatie en het gedrag, attitude en opvattingen van medewerkers.

Bij dit alles is regelgeving, zoals wetten en normen, een belangrijke leidraad voor informatiebeveiliging hoewel gewaakt moet worden tegen een te overheersende rol. Zo kan certificering tegen de Norm voor informatiebeveiliging in de zorg, een bijdrage leveren aan de beveiliging maar bij overdrijving ook leiden tot verambtelijking zonder resultaatⁱⁱ.

De belangrijkste voorschriften van informatiebeveiliging zijn in hoofdstuk 4 in een overzicht geplaatst. Deze voorschriften zijn ontstaan uit ervaringsregels en concretiseren de abstracte doelstellingen en mogelijkheden om de betrouwbaarheid te verbeteren met checklists, beschrijvingen van aanpakken en dergelijke. Een deel van de voorschriften is een beschrijving van wat professioneel wordt geacht in de praktijk van moderne informatiesystemen; het is aan directies om te beslissen of en in hoeverre zij daaraan willen voldoen. Een voorbeeld zijn normen voor informatiebeveiliging die het Nederlands Normalisatie-Instituut heeft uitgegeven. Een ander deel van de voorschriften bestaat uit wetten zoals de Wet bescherming persoonsgegevens, die directies verplichten om aandacht te schenken aan informatiebeveiliging op straffe van sancties, opgelegd door het College Bescherming Persoonsgegevens.

In deel II wordt ingegaan op verbeteren en beheren van informatiebeveiliging. Aan de orde komen de voorwaarden (hoofdstuk 5), de fasering waarmee verbeteringen systematisch kunnen worden aangepakt (hoofdstuk 6) en voorbeelden van onderzoeksmethoden waarmee de uitgangssituatie kan worden bepaald (hoofdstuk 7).

In deel III komen de regels ter sprake. Een deel van deze regels komt uit de wereld van de juristen; een ander deel uit die van de ICT'ers. Hoewel de herkomst van de regels verschilt, stemt het doel daarvan overeen: verbeteren van de informatiebeveiliging en verduidelijken hoe dat te doen. Met het oog daarop is gekozen voor een thematische behandeling van de regels in wetten, normen en methoden. De thema's die aan de orde komen zijn:

- de strategische aspecten: inhoud van registraties en gegevensuitwisseling, respectievelijk de hoofdstukken 8 en 9;
- de inrichtingsaspecten van de informatievoorziening: in hoofdstuk 10 de verantwoordelijkheden, in hoofdstuk 11 de procedures, terwijl de naleving is ondergebracht in hoofdstuk 12;
- de procedures die nodig zijn om het gebruik van ICT in goede banen te leiden staan in hoofdstuk 13.

Deel IV ten slotte bevat twee opiniërende hoofdstukken die het voorgaande illustreren. Hoofdstuk 14 geeft een model voor het leerproces dat management en medewerkers in een organisatie moeten doormaken voor beveiliging van informatievoorziening. In hoofdstuk 15 komt de vraag aan de orde of wetgeving nog wel voldoende sturing geeft aan informatiebeveiliging en het medisch beroepsgeheim in deze tijd van groeiende zorgnetwerken.

1.3 Hoe kunt u dit boek gebruiken?

Ieder hoofdstuk start met een Inleiding, waarna een verdere uitwerking volgt. In aanvulling daarop bevat het boek ook praktijkverhalen (in een kader), waar nodig geanonimiseerd. Als u weinig tijd hebt kunt volstaan met de Inleidingen, maar ook andere manieren van lezen zijn denkbaar.

- Als u een ICT-achtergrond hebt en meer wil weten van juridische achtergronden, begin dan met de hoofdstukken 9, 9 en 10 over respectievelijk de inhoud van medische registraties, gegevensuitwisseling en verantwoordelijkheden.
- Als u een juridische achtergrond hebt en meer wil weten van de ICT-achtergronden, begin dan met hoofdstuk 3 'Basisbegrippen' en deel II, Verbeteren en beheren.
- Als u een managementachtergrond hebt is hoofdstuk 2 'Betrokkenen' een goed begin om daarna verder te gaan met hoofdstuk 11 Verantwoordelijkheden en deel III over veranderingsprocessen, vaststellen van knelpunten in de bestaande situatie en stellen van prioriteiten.
- Voor beleidsmakers zijn de praktijkverhalen uit het boek interessant, evenals de opiniërende hoofdstukken 14 met een groeiemodel voor informatiebeveiliging en hoofdstuk 15 met kritische vragen over de actualiteit van de relevante wetgeving.

1.4 Waarom dit boek?

Hoewel informatie-uitwisseling toeneemt binnen de zorg, constateert de Inspectie voor de Gezondheidszorg in een onderzoek uit 2004 dat "...ziekenhuizen op dit moment onvoldoende aandacht schenken aan de risico's die de toepassing van ICT met zich meebrengt"ⁱⁱⁱ.

Deze situatie is ontstaan doordat management en medewerkers te vaak hun slechte gewoonten van het papieren tijdperk meenemen naar het automatiseringstijdperk. Automatisering kan dan de gevolgen vergroten van wat er in het verleden ook al mis ging. Rondslingerende papieren dossiers zijn vervelend voor individuele patiënten, maar rondslingerende wachtwoorden kunnen tot gevolgen leiden voor alle patiënten van die instelling. Karin Spaink^{iv} liet zien hoe makkelijk men wachtwoorden afgeeft aan een vreemde.

Voor de Inspectie voor de Gezondheidszorg was het gevolg van onvoldoende risicobeheersing van ICT duidelijk: "De patiënt loopt hierdoor een reële kans op gevaar. Er kunnen bijvoorbeeld belangrijke gegevens verloren gaan, gegevens kunnen op de verkeerde plaats terechtkomen en behandelingen kunnen verstoord raken door niet goed functionerende apparatuur".

De geschetste problemen zijn niet nieuw. Al jarenlang schenkt de overheid aandacht aan regelgeving waarin, onder allerlei benamingen, veilig omgaan met informatie prominent aan de orde komt. De Wet bescherming persoonsgegevens (Wbp)^v is er in totaliteit aan gewijd, evenals belangrijke onderdelen van de Wet Geneeskundige Behandelingsovereenkomst (WGBO) (WGBO). Ook de Norm voor informatiebeveiliging in de zorg (NEN7510, NEN7511, NEN7512) is een belangrijk voorbeeld.

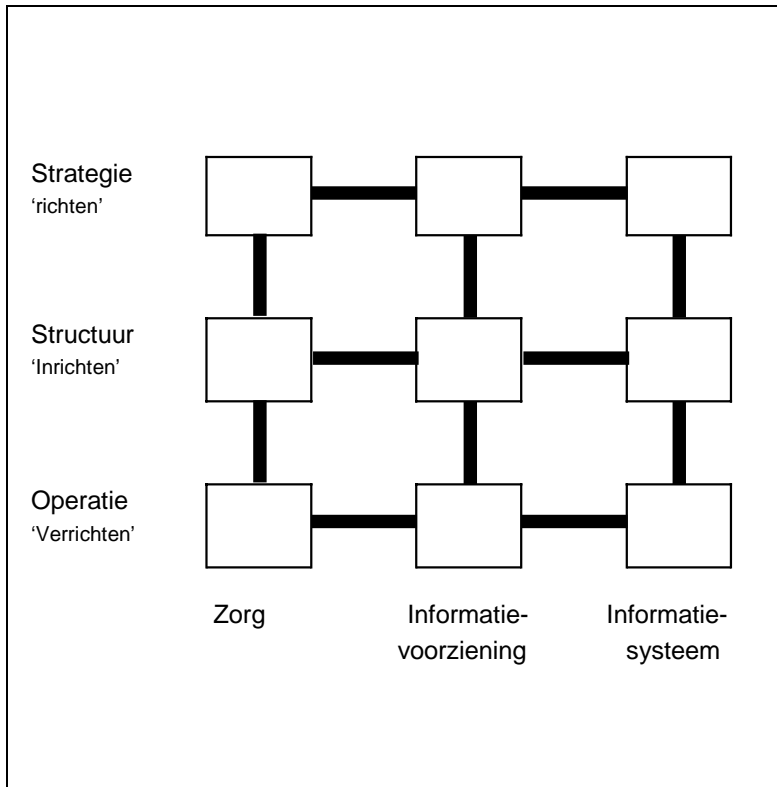
Als 'verzamelde ervaring' zijn deze regels handig, maar tussen de regels en de praktijk blijft een kloof bestaan. Dit boek is hopelijk een bijdrage om deze kloof te dichten.

Deel I Overzicht

Door problemen in de eigen organisatie of publiciteit van problemen elders, bestaat in organisaties gewoonlijk wel eensgezindheid over de noodzaak van aandacht aan informatiebeveiliging. Maar over de concrete aanpak bestaat te vaak verschil van inzicht doordat medicus, manager, medewerkers ICT en andere organisatieleden heel anders tegen de oorzaak van problemen aankijken. Wat de ICT-manager ervaart, als ondercapaciteit van de afdeling, kunnen gebruikers heel anders ervaren. Zij zien ICT-medewerkers die niets begrijpen van service doordat ze nooit bereikbaar zijn en die er bovendien niet in slagen om het systeem voldoende storingsvrij te krijgen. Succes met informatiebeveiliging vereist allereerst inzicht in de meningen van de leden van de verschillende groeperingen in de organisatie, het onderwerp van hoofdstuk 2.

Om richting te scheppen in het wegwerken van risico's en het oplossen van problemen is een analytische aanpak nodig, waarbij voor iedereen zichtbaar wordt gemaakt hoe de beveiliging kan worden verbeterd. De basisbegrippen van dat analysekader komen aan de orde in hoofdstuk 3. Er kan gebruik worden gemaakt van veel regels: wetten, normen voor informatiebeveiliging in de zorg, technische normen. Deze regels zijn niet alleen voorgeschreven, ze zijn ook een hulpmiddel om efficiënt te werken aan informatiebeveiliging. Bovendien kunnen wetten en normen de richting aanwijzen als organisatieleden verschil van inzicht hebben over het te volgen beleid. Zo is het voorgekomen dat gebruikers zelf een website wilden beheren met vertrouwelijke gegevens die geregeld muteerden, waardoor de webserver af en toe verbonden moest worden aan het computernetwerk. De Norm voor informatiebeveiliging in de zorg maakt duidelijk dat de risico's van een ongecoördineerde aanpak te groot zijn en dat technisch beheer alleen door gespecialiseerde medewerkers van de afdeling ICT kan worden uitgevoerd. Als die het niet kunnen, dan kan de gebruiker het zeker niet en moet de directie andere maatregelen treffen, bijvoorbeeld omzien naar andere ICT-medewerkers.

Een overzicht van de regels en hun gebruiksmogelijkheden wordt gegeven in hoofdstuk 4, dat zowel ingaat op het wettelijk kader als de Norm voor informatiebeveiliging in de zorg.



Figuur 1 De IM-kaart: indeling van de activiteiten van een organisatie

Om de activiteiten van een zorgorganisatie te visualiseren, wordt in dit deel gebruik gemaakt van een 'landkaart' van de organisatieactiviteiten. Zie figuur 1, die een vrije interpretatie is van de Informatie Managementkaart. (IM-kaart) van Maes^{vi}.

De verticale as van figuur 1 is ingedeeld naar de aard van de activiteiten van de organisatie.

- **Strategie:** richten van de organisatieactiviteiten om die aan te laten sluiten op de omgeving van de organisatie.
- **Structuur:** inrichten van de organisatie.
- **Operatie:** verrichten van de organisatieactiviteiten.

Langs de horizontale as:

- **Zorg:** het primaire proces dat eisen stelt aan informatievoorziening.
- **Informatievoorziening:** de kolom met activiteiten die nodig zijn om betekenis voor de zorg te geven aan het informatiesysteem.

Informatiesysteem: wordt gebruikt om data zoals patiëntgegevens en röntgenfoto's op te slaan.

Deel II Verbeteren en beheren

Inleidingen voor veranderingsprocessen bevatten vaak het pessimistische citaat van Machiavelli: 'Niets is moeilijker om aan te pakken, gevaarlijker om uit te voeren, en onzekerder in haar slagen dan de leiding te nemen bij een veranderingsproces, want de vernieuwer heeft vijanden in allen die het goed doen onder de bestaande omstandigheden, en nauwelijks verdedigers in zij die het misschien goed zullen doen onder de nieuwe omstandigheden'.

In dit deel wordt uitgegaan van een optimistischer visie dan die van Machiavelli. De effectiviteit van veranderingen kan worden verhoogd met een systematische aanpak waarin rekening wordt gehouden met de uiteenlopende belangen van de betrokkenen en de factoren die de veiligheid bepalen. Die factoren kunnen worden verdeeld in de volgende aandachtsgebieden:

- informatievoorziening, informatiesystemen en het beheer daarvan;
- het samenspel van betrokkenen in de bedrijfsorganisatie;
- het gedrag van individuen.

Werken aan informatiebeveiliging is vernieuwen, maar te vaak krijgt beheersen van bestaande procedures de overhand. Beheersen is vaak ook makkelijker omdat dan slechts het documenteren van bestaande procedures is vereist. Zo worden ingewikkelder projecten zoals die voor technologische vernieuwing en gedragsverbetering vermeden. Duidelijk effect blijft dan echter uit doordat de proceduredocumentatie ongebruikt blijft.

Er zijn tal van momenten in het verbeterproces om de effectiviteit van veranderen te verhogen. De eerste mogelijkheid is voorwaarden stellen aan het begin. Voor nieuwe informatievoorziening is deze voorwaarde eenvoudig: ontwikkel die gelijk goed want later aanpassen altijd extra werk. Niettemin zal verbeteren van de bestaande informatievoorziening de overhand hebben. Geschikte voorwaarden vooraf kunnen ook in dat geval de effectiviteit van het proces doen toenemen, hetgeen het onderwerp is van hoofdstuk 5.

Met fasering van het werk ontstaat nog een mogelijkheid om de effectiviteit van informatiebeveiliging te verhogen. Dit is het onderwerp van hoofdstuk 6, waarin een cyclisch verlopend stappenplan wordt beschreven. Er zijn meerdere mogelijkheden om dit proces te starten. Met de fasering ontstaat een schematisch overzicht van de verschillende stappen om tot betere beveiliging te komen. Dit schema is ook handig om te bepalen met welke stap het beste kan worden begonnen, zie paragraaf 3 van hoofdstuk 6. Welke stap dat is hangt af van de omstandigheden bij de start. De ene keer is de start een reactie op een ernstig voorval, de andere keer verhoogt het management de aandacht voor informatiebeveiliging omdat men begint te beseffen dat risico's zijn toegenomen door snelle groei van ICT, ook al zijn ongelukken tot dan toe nog uitgebleven.

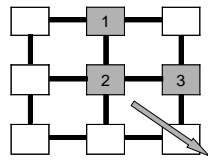
Een verbeterproces vereist ook afbakening van taken en verantwoordelijkheden, het onderwerp van paragraaf 6.4, waarin aan de orde komen de verantwoordelijken voor informatiebeveiliging, hun samenwerking en de inhoudelijke coördinatie van beveiligingsactiviteiten. Ook onderdeel van dit vraagstuk is de verantwoordelijkheid van partijen waaraan taken zijn uitbesteed zoals softwareleveranciers die relatief veel invloed hebben op de informatiesystemen van de instelling.

Verdere verhoging van de effectiviteit wordt bereikt met de inzet van geschikte technieken, het onderwerp van hoofdstuk 7.

Deel III Regels, normen, methoden

Met een lappendeken van wetten, normen, methoden en ongeschreven gebruiken wordt informatiebeveiliging concreet gemaakt. In dit deel worden de juridische regels, normen en methoden met elkaar in verband gebracht door deze in te delen in de IM-kaart. Deze indeling is onvermijdelijk enigszins arbitrair, omdat de verschillende onderwerpen niet scherp af te bakenen zijn. De verdere behandeling van de stof is beperkt tot de hoofdlijnen vanwege de uitgebreidheid van de stof. Voor de finesses wordt verwezen naar de gespecialiseerde boeken op bijvoorbeeld juridisch gebied, ICT-beheer of methoden.

De indeling wordt samengevat in het volgende schema.



	Persoons-gegevens	Andere gegevens	
1. Informatiefunctie / Strategie	Wbp Wgbo		Hoofdstuk 9: Verwerken van medische gegevens • Hoofdstuk 10: Gegevensuitwisseling
2. Informatiefunctie / Structuur	Wbp, Wgbo		Hoofdstuk 11 - Verantwoordelijkheden Hoofdstuk 12: Procedures informatiefunctie (Beleid, personeel, fysieke- en omgevingsbeveiliging, continuïteitsbeheer, wettelijke vereiste procedures voor transparantie e.d.)
	Wbp Strafrecht, Arbeidsrecht Norm voor IB in de zorg		Hoofdstuk 13: Naleving
3. ICT-functie / Structuur	Norm voor IB in de zorg Methoden zoals ITIL, testmethoden		Hoofdstuk 14: ICT-procedures (operationeel beheer, toegangsbeveiliging, aanschaf, ontwikkeling en onderhoud van informatiesystemen, afhandelen beveiligingsincidenten)

De middelste kolom van de IM-kaart, die van de 'Informatiefunctie', is in het schema gesplitst voor persoonsgegevens en andere dan persoonsgegevens. Daarbinnen komen de volgende onderdelen aan de orde.

1 De strategische aspecten van informatiebeveiliging

Het gaat daarbij om thema's zoals bevoegdheid om te registreren, verdere verwerking, bewaartermijn, met als gemeenschappelijke noemer: mogen gegevens überhaupt verwerkt worden. Voor bedrijfsgegevens gelden geen regels, voor persoonsgegevens wel. Hoofdstuk 9 gaat daar nader op in. In hoofdstuk 10 wordt dit onderwerp verder uitgediept voor het aspect gegevensuitwisseling tussen medici.

2 De structurele (inrichtings-)aspecten van informatiebeveiliging

De thema's hier zijn de techniekonafhankelijke voorwaarden die worden gesteld aan de gegevensverwerking. Voor persoonsgegevens zijn voorwaarden te vinden in wetten zoals de Wbp (voorbeeld: de transparantie-eis) en meer recent de "Wet op het gebruik van het Burgerservicenummer in de Zorg". De Norm voor informatiebeveiliging in de zorg kan voor wat betreft

persoonsgegevens worden beschouwd als een nadere uitwerking van deze voorwaarden en voor andere dan persoonsgegevens, richtinggevend. Hoofdstuk 11 gaat in op de verantwoordelijkheden, en hoofdstuk 12 op de procedures. Hoofdstuk 13 behandelt de naleving en gaat daarvoor in op wetten zoals het arbeidsrecht en strafrecht en ook de Norm voor informatiebeveiliging in de zorg.

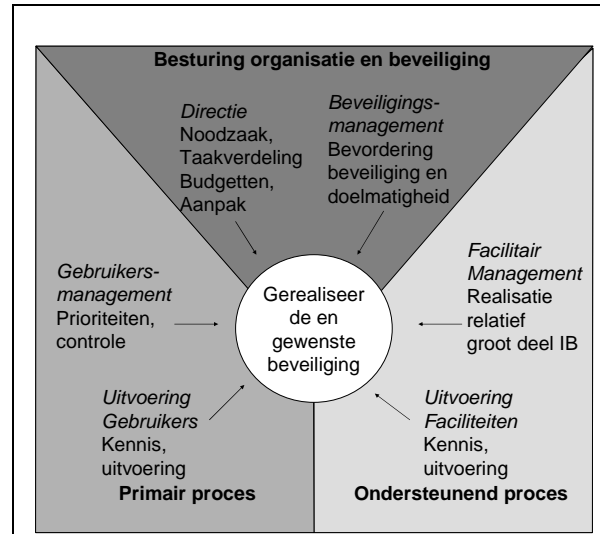
Van de rechterkolom van de IM-kaart, die van de 'ICT-functie', wordt het volgende behandeld.

3 De structurele aspecten van de ICT-functie
met als thema's de voorwaarden die worden gesteld aan de beheersing van de technologie zoals het operationeel beheer van informatie- en communicatievoorzieningen, toegangsbeveiliging, aanschaf, ontwikkeling en onderhoud van informatiesystemen en acceptatietesten. Zie verder hoofdstuk 13. Ook hiervoor is de Norm voor informatiebeveiliging in de zorg een belangrijke leidraad.

Deel IV Opinions

Inleiding

Verbeteren van de beveiliging is een veranderingsproces voor de organisatie. Dit hoofdstuk beschrijft een model voor de groei van de organisatie tijdens die verandering. Uitgangspunt vormen de leerprocessen die de betrokkenen doormaken bij het verbeteren van de informatiebeveiliging en bij het vasthouden van het eenmaal bereikte niveau. In paragraaf 4.3 zijn die betrokkenen al besproken en samengevat in de hiernaast weergegeven figuur.



Figuur 1 De betrokkenen bij informatiebeveiliging

ⁱ ITIL, v.Looijen, e.a.

ⁱⁱ Zie bijvoorbeeld 'Lessen uit Mislukkingen, veilige informatie-uitwisseling zonder de zorg te compliceren', Mr. drs. J.A. van der Wel, Medisch Contact 17 september 2004, www.comfort-ia.nl/mc.pdf

ⁱⁱⁱ Inspectie voor de Gezondheidszorg, *ICT in de ziekenhuizen, Een inventariserend onderzoek bij twintig ziekenhuizen, uitgevoerd najaar 2003, den Haag augustus 2004*, zie www.igz.nl

^{iv} Karin Spaink, ...

^v De Wet bescherming persoonsgegevens (Wbp) geeft regels ter bescherming van de privacy van burgers. De wet is op 1 september 2001 in werking getreden.

^{vi} Rik Maes, *PrimaVera Working Paper 2004-12*, <http://primavera.fee.uva.nl/PDFdocs/2004-13.pdf>

INFORMATIEBEVEILIGING IN DE ZORG

J.A. van der Wel

**Graag ontvang ik Informatiebeveiliging in de zorg (ISBN 90 395 2498 X).
Ik betaal € 23,54 excl. BTW en administratie- en verzendkosten. De factuur
wordt bijgesloten bij het boek.**

Naam bedrijf _____

De heer / mevrouw * _____

Voorletters _____

Functie _____

Postadres werk/privé* _____

Postcode _____

Plaats _____

Telefoon _____

Fax _____

E-mail _____

Handtekening _____

* svp doorhalen wat niet van toepassing is

Stuur deze bon terug naar Sdu Uitgevers, t.a.v. M. Demmer, Postbus 20025, 2500 EA Den Haag
Of fax naar: (070) 799 98 78 t.a.v. M. Demmer

Prijs is exclusief BTW en verzend- en administratiekosten. Sdu Uitgevers gaat zorgvuldig met persoonsgegevens om.