

NEN 7510

De norm in zijn omgeving

Dat de Inspectie voor de Gezondheidszorg (IGZ) twee jaar geleden na onderzoek kon vaststellen dat het gebruik van ICT gemeengoed was geworden in de zorgsector zal weinigen hebben verbaasd. Niets nieuws in dit opzicht. De zorgsector is al decennia lang een interessant en belangrijk toepassingsgebied van ICT, zowel waar het medisch-technische apparaat betreft als in de vorm van medisch-administratieve systemen.

Dat de Inspectie het juist in deze jaren nodig vond om de toepassing van ICT in de zorg te onderzoeken valt te verklaren uit het feit dat nu ook de primaire zorgprocessen steeds afhankelijker zijn geworden van het gebruik van ICT en dus ook van de kwaliteit van dat ICT-gebruik. Een ontwikkeling die nog niet ten einde is. In de nieuwe, minder in functies en meer in

ketens georganiseerde zorgprocessen, neemt het belang aan eenduidige en betrouwbare informatie en betrouwbare informatieoverdracht toe. Zonder ICT gaat dat niet lukken, waarmee het laatste restje vrijblijvendheid van ICT-gebruik in de zorg, zo dat er nog is, zal verdwijnen.

Eveneens in deze jaren heeft het in 2002 opgerichte Nationaal ICT Instituut voor de Zorg (NICTIZ) een programma ontwikkeld dat uiteindelijk moet leiden tot een landelijke ICT infrastructuur voor de zorg. Met ingang van 2006 zullen de eerste delen – NICTIZ noemt ze ‘hoofdstukken’ – van het Elektronisch Patiënten Dossier worden uitgebracht, waarmee ook de eerste stappen zullen zijn gezet op een route waarlangs veranderingen in de zorg hand in hand zullen gaan met ontwikkelingen in de elektronische informatievoorziening en communicatie. De NICTIZ-plannen krijgen brede ondersteuning in de sector, dat enerzijds, maar anderzijds eisen ze ook veel van het veld. En een voorname eis is: bereidheid tot conformeren.

Communicatie veronderstelt afspraken, al was het maar over de taal die men zal spreken. Bij elektronische communicatie is dit niet anders,

- 3 Informatiebeveiliging in de zorg: NEN 7510, 7511, 7512, enzovoorts?**
- 7 NEN 7510: Instrument**
- 9 De praktijk van NEN 7510**
- 15 CBO: NEN 7510 is kwaliteitsinstrument bij uitstek**
- 16 Informatiebeveiliging in kleine praktijken**
- 18 Doe wel. Doe niet.**
- 21 Inspectie voor de Gezondheidszorg: NEN 7510 sterk aanbevolen!**
- 23 De beveiligingsplicht in wet-en regelgeving**

waarbij men bovendien in acht dient te nemen dat elektronica een eigen verzameling met zich mee brengt van dingen-die-geregeld-moeten-worden. Tot die dingen behoort Informatiebeveiliging – een onderwerp dat in een elektronische omgeving totaal nieuwe dimensies krijgt in vergelijking tot een omgeving waarin het papieren dossier het karakteristieke communicatiemiddel is.

De norm NEN 7510 is ontwikkeld met het oog op Informatiebeveiliging in een voornamelijk door ICT bepaalde communicatieomgeving in de gezondheidszorg. Hij stoelt op een internationaal (ISO) geaccepteerde code. Hij wordt gedragen door de belangrijkste (koepel)organisaties in de zorg. En vooral: Hij dekt het hele gebied van informatiebeveiliging en blijft dus niet beperkt

tot technische specificaties maar geeft ook richting aan wworganisatie en menselijk handelen.

Het laatste maakt dat instellingen in individuele zorgverleners zich bij de implementatie van NEN 7510 ook niet kunnen beperken tot het aanbrengen van virusfilters en firewalls. Daar komt meer bij kijken en lang niet alles kan men overlaten aan ICT leveranciers of ICT afdelingen. Iedereen die met de informatie omgaat zal door drongen moeten zijn van het belang van informatiebeveiliging. Het is immers de kwaliteit van de zorg zelf die in het geding is.

Redactie



Colofon

Uitgever

NEN – Gezondheidszorg, Delft

Productiecoördinatie

Piasau, Zoetermeer

Teksten en eindredactie

Dick Overkleef, Gelselaar

Vormgeving

Studio Bau Winkel, Den Haag

Fotografie

Herman Zonderland, Delft

Druk

Van Marken Delft Drukkers

Vragen en opmerkingen

nen7510@nen.nl

Website/nadere informatie

www.nen7510.org

Informatiebeveiliging in de zorg: NEN 7510, 7511, 7512, enzovoorts?

Kees Louwerse (LUMC) is voorzitter van de normcommissie 303001, Informatiebeveiliging in de Zorg, die NEN 7510 e.v. heeft voorbereid.

In november 2002 werd de eerste conceptversie van NEN 7510 gepresenteerd en startte de eerste commentaarronde. We zijn nu 2,5 jaar verder, en ingewijden weten dat er sindsdien veel is gebeurd. Voor een deel speelde zich dat weliswaar af achter de schermen, maar er zijn toch ook dingen zichtbaar geworden. In ieder geval is NEN 7510 begin vorig jaar gepubliceerd, nadat het ontvangen commentaar was verwerkt. En gelukkig is het niet bij publicatie gebleven. In de gezondheidszorg is '7510' al een begrip geworden; zelfs zijn er instellingen die er actief mee aan de slag zijn gegaan.

De norm NEN 7510 vult niet alle details in; het is meer een overkoepelende beschrijving van zaken die geregeld dienen te worden om een goede Informatiebeveiliging te kunnen realiseren. Sinds de publicatie is er verder gewerkt aan de invulling van enkele detailgebieden. Aanleiding voor de nu voorliggende publicatie is het feit, dat twee van die vervolgstappen (inderdaad, NEN 7511 en 7512) inmiddels het stadium van de commentaarronde hebben bereikt.

Waar gaat het over?

We praten over Informatiebeveiliging in de zorg; een onderwerp dat vrij lang nogal onderbelicht is gebleven. Toch zijn er ruimschoots voldoende

redenen om er wel degelijk veel aandacht aan te geven. Informatie is vaak letterlijk van levensbelang in de patiëntenzorg. De kwaliteit van die informatie dient dus buiten kijf te zijn. En dat vergt vanzelfsprekend een aanpak van de Informatiebeveiliging op een hoog niveau. Voor de duidelijkheid: dit betekent dat er aandacht moet besteed worden aan *beschikbaarheid*, *betrouwbaarheid* (integriteit) en *vertrouwelijkheid* (privacy). Dat is niet een uitsluitend technische kwestie; het gaat de hele organisatie aan. Met techniek alleen lukt het niet.

Er wordt (ook onbewust) steeds vaker bijna blind op de resultaten van informatiesystemen vertrouwd, en het wordt bijna als vanzelfsprekend beschouwd dat die systemen ook 'altijd' beschikbaar zijn. Elektronische uitwisseling van informatie tussen verschillende instellingen wordt bovendien steeds meer gebruikt en ook de meeste activiteiten van NICTIZ zijn er op gericht om dit verder mogelijk te maken en te stimuleren.

Al die informatie moet dus wel met zorg behandeld worden. In andere sectoren van de maatschappij gaat dat ook niet vanzelf, maar daar is men er toch al wat langer van doordrongen dat Informatiebeveiliging een zeer belangrijke discipline is. Juist bij de ontwikkelingen in de zorgsector, waarbij communicatie van informatie een belangrijke rol speelt, is het van



Als ik zie hoe vaak er onzorgvuldig wordt omgegaan met informatie, en hoe weinig men zich realiseert welke gevolgen dat kan hebben, dan ben ik erg blij met de norm, waarin aangegeven wordt hoe die zorgvuldigheid, en daarmee de kwaliteit, op een hoger plan gebracht kunnen worden.

Kees Louwerse, LUMC

eminent belang om helderheid te krijgen over de eisen waaraan systemen moeten voldoen. We zijn misschien redelijk zeker van de betrouwbaarheid van onze eigen systemen (en hoe terecht is dat eigenlijk?). Maar als we informatie met een andere instelling uitwisselen, willen we er extra zeker van zijn dat er dáár ook geen gekke dingen gebeuren. Zolang die uitwisseling op kleine schaal gebeurt, kun je er wel onderlinge afspraken over maken. Maar als het op landelijke schaal moet, hebben we toch echt een landelijke 'meetlat' nodig. Alleen dan kunnen we gerechtvaardigd vertrouwen hebben in onze communicatiepartners.

Norm en hulpmiddelen

Er waren al enige tijd normen voor Informatiebeveiliging beschikbaar. De belangrijkste daarvan is de Code voor Informatiebeveiliging, tegenwoordig ook bekend als ISO IEC 17799. Deze werd echter in de Gezondheidszorg niet tot nauwelijks gebruikt. Met NEN 7510, die sterk op deze algemene norm is gebaseerd, werd een soort vertaalslag gemaakt van deze Code naar de zorgsector. Daar werd ook een set handboeken (een 'gereedschapskist') bij geleverd, met allerlei hulpmiddelen die de implementatie beter hanteerbaar moeten maken. De gewenste

hanteerbaarheid wordt onder meer bereikt, doordat de handboeken voor verschillende soorten organisaties zijn uitgewerkt. Een ziekenhuis zit nu eenmaal anders in elkaar dan een éénmanspraktijk en toch is Informatiebeveiliging voor beiden essentieel. Tegelijk met NEN 7510 zijn deze handboeken gepubliceerd voor een zevental varianten van organisaties.

Toetsbare kwaliteit

Het Ministerie van VWS is bezig met de invoering van het Burger Service Nummer in de gezondheidszorg. Daarbij is behoefte aan een formele mogelijkheid om beveiligingseisen op te leggen aan systemen die gebruik maken van dit nummer. De norm NEN 7510 gaf hiervoor een goed aanknopingspunt. Wel bleek het nodig, om de richtlijnen uit de norm in een meer toetsbare vorm te presenteren. Het is lastig om dat te doen en toch de algemene toepasbaarheid te handhaven die in de norm wordt nagestreefd. Zo ontstond het begrip 'toetsbare voorschriften'. Op basis van de norm is eerst een generieke set toetsbare voorschriften opgesteld, waarin de normteksten waar nodig nog wat verder worden gedetailleerd. Er is op dat niveau ook een direct verband gelegd met de eisen die NICTIZ heeft geformuleerd in hun definitie van Goed Beheerde Zorgsystemen. Vervolgens zijn op basis van deze generieke set, specifieke voorschriften opgesteld voor de meest voorkomende organisatievormen in de zorg. Dit is gebeurd in werkgroepen waaraan ook actief is deelgenomen door vertegenwoordigers van de verschillende beroepsgroepen in de zorg. Resultaat van dit alles is de serie NEN 7511-1, -2, -3, waarin voor drie verschillende organisatievormen de norm wordt uitgewerkt in toetsbare voorschriften. Bezien wordt nog, of deze serie uitgebreid moet worden. Bij het maken van deze op de verschillende organisaties gerichte toetsbare voorschriften is ook gekeken naar de (hiervoor reeds genoemde) handboeken. Deze worden momenteel uitgebreid naar aanleiding van de resultaten in de werkgroepen. Zoals uit diverse reacties al gebleken is, bieden deze handboeken een nuttige ondersteuning voor organisaties die de norm willen implementeren. Het is immers niet efficiënt om wielen steeds opnieuw uit te moeten vinden.

Informatie wordt steeds beter en sneller toegankelijk. In de Zorg kunnen we daardoor werken aan een aanzienlijke verbetering van de efficiency en kwaliteit. Maar de kans op verkeerde interpretaties en misbruik neemt evenredig toe. We zullen de gegevens van de patiënt daarom optimaal moeten beheren en beveiligen. Dat moeten we wel zelf doen! NEN7510 is daarbij een handige leidraad.

Frans van Bommel, Vektis



Invulling van details

We zagen al, dat NEN 7510 een nogal algemeen karakter heeft. Er zijn verschillende onderdelen, die in dit document niet in detail worden uitgewerkt. Redenen daarvoor waren vooral: de wens om zo dicht mogelijk in de buurt te blijven bij de bron (ISO IEC 17799) en het feit dat er anders wellicht een te log document zou ontstaan. Toch is er natuurlijk wel behoefte aan enige uitwerking voor verschillende onderdelen. Daaraan is inmiddels ook begonnen. Het eerste van deze onderdelen, het vertrouwensmodel, is nu dan ook in concept beschikbaar gekomen, en de commentaarronde begint nu.

Vertrouwensmodel (NEN 7512)

NEN 7512 geeft een aanvulling op enkele richtlijnen uit NEN 7510 en geeft antwoord op de vraag, welke zekerheid partijen elkaar moeten bieden als voorwaarde voor vertrouwde gegevensuitwisseling. Er wordt in relatie daarmee ook een aanzet gegeven tot een risico-classificatie (immers, maatregelen dienen evenwichtig te zijn, in relatie tot het doel) en er worden eisen geformuleerd ten aanzien van de zwaarte van de identificatie en authenticatie bij een bepaalde risicoklasse.

Door middel van de serie normdocumenten NEN 7510, 7511-... en 7512 en de bijbehorende handboeken is een flinke aanzet gegeven voor het op een hoger niveau brengen van de Informatiebeveiliging in de gezondheidszorg. Zoals bijvoorbeeld blijkt uit ervaringen bij UMC's en ook in verschillende andere instellingen, bieden deze documenten een stevige ondersteuning bij het implementeren van een verantwoorde Informatiebeveiliging.

Uiteraard is dit niet het laatste woord. Er moeten zeker nog meer details worden ingevuld, en het nu beschikbare materiaal zal bij toetsing aan de praktijk ongetwijfeld nog moeten worden aangepast. Het is daarom van belang om er nu mee aan de slag te gaan.

De normcommissie 303001 (Informatiebeveiliging in de Zorg) is zeer geïnteresseerd in uw ervaringen (zowel positieve als negatieve), en vraagt u dan ook dringend om die naar ons te communiceren. Mede voor dit doel is de website ingericht: www.NEN7510.org.

Zorg voor informatie

De aandacht voor kosten en kwaliteit in de zorg neemt toe. Zo kunnen verzekeraars een ziekenhuis kiezen op basis van prijs en kwaliteit van de diagnose behandelcombinaties (DBC's). Ook patiënten kunnen kiezen, geholpen door tests zoals die van de Elsevier.

Comfort-IA speelt in op deze veranderingen met diensten op het gebied van interim-management, projectleiding, informatiebeveiliging en de wettelijke eisen voor informatievoorziening, testmethoden en -technieken en softwareselectie. Onze medewerkers zijn ervaren, gedreven, innovatief en resultaatgericht. Zij kennen de werkomgeving van onze klanten en de ontwikkelingen in de zorg. Zij hebben ervaring met vergelijkbare veranderingen opgedaan in andere bedrijfstakken en dragen die over, tijdens opdrachtuitvoering en met workshops. U verliest zo geen tijd door het wiel weer uit te vinden.

Maak eens een afspraak met ons. Vrijblijvend. De belangen zijn groot. Met onze ervaring en kennis kunnen wij uw organisatie vernieuwen waardoor uw instelling het initiatief kan nemen in de zich ontwikkelende zorgmarkt.

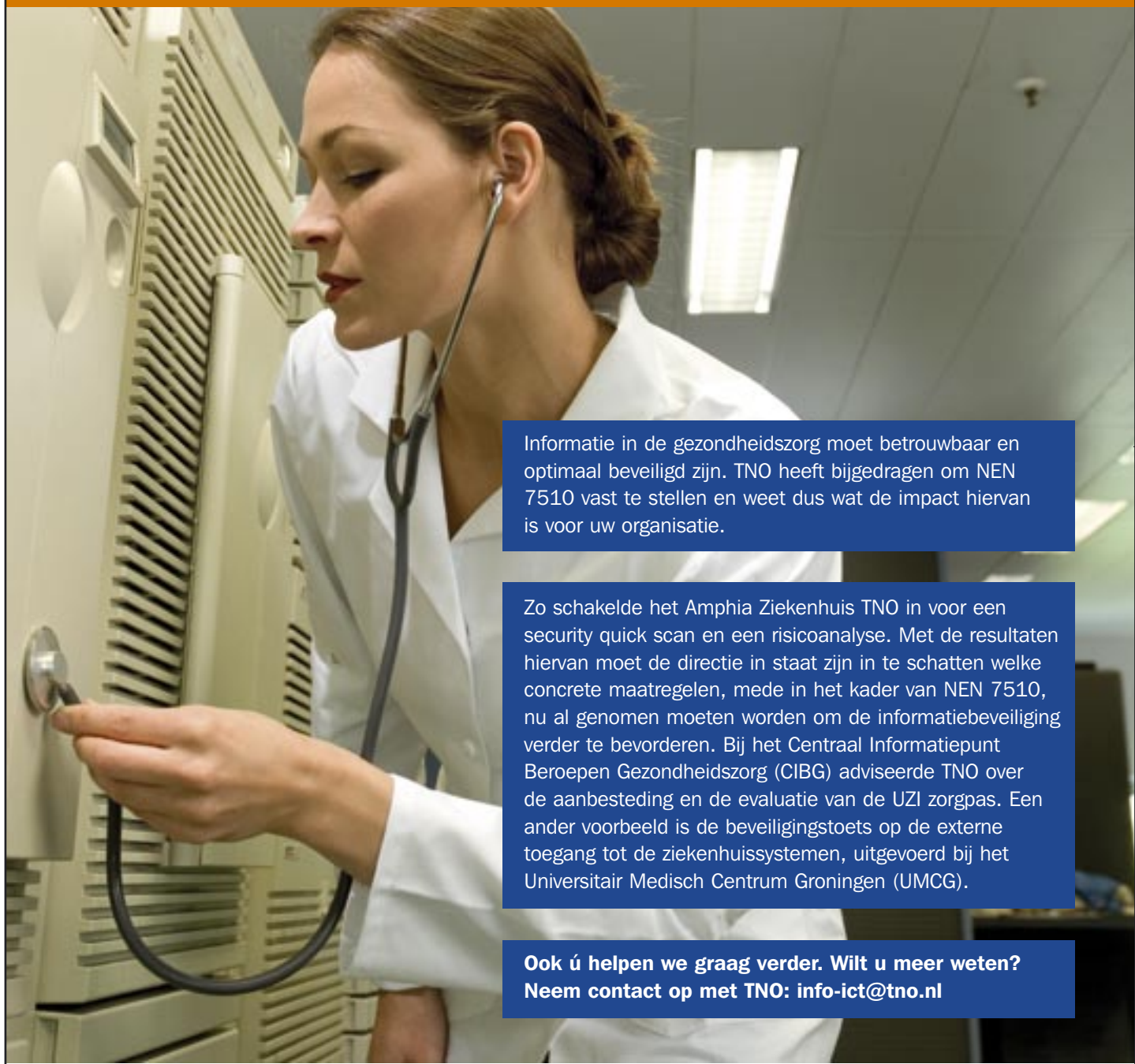
Specialist in:

- *Interim- en projectmanagement;*
- *Informatiebeveiligingsbeleid (NEN7510);*
- *Veilig ICT-gebruik, acceptatietesten,*
- *administratieve organisatie;*
- *Verandermanagement en ICT;*
- *Audits, workshops.*

Mr. drs. Jaap A. van der Wel
(jvdwel@comfort-ia.nl)
Managing Partner Comfort
Information Architects,
Zonnebaan 45, 3542 EB Utrecht
tel: 030 7504 097
www.comfort-ia.nl



Hoe voldoet ú straks aan de normen voor informatiebeveiliging?



Informatie in de gezondheidszorg moet betrouwbaar en optimaal beveiligd zijn. TNO heeft bijgedragen om NEN 7510 vast te stellen en weet dus wat de impact hiervan is voor uw organisatie.

Zo schakelde het Amphia Ziekenhuis TNO in voor een security quick scan en een risicoanalyse. Met de resultaten hiervan moet de directie in staat zijn in te schatten welke concrete maatregelen, mede in het kader van NEN 7510, nu al genomen moeten worden om de informatiebeveiliging verder te bevorderen. Bij het Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG) adviseerde TNO over de aanbesteding en de evaluatie van de UZI zorgpas. Een ander voorbeeld is de beveiligingstoets op de externe toegang tot de ziekenhuissystemen, uitgevoerd bij het Universitair Medisch Centrum Groningen (UMCG).

**Ook ú helpen we graag verder. Wilt u meer weten?
Neem contact op met TNO: info-ict@tno.nl**

TNO.NL



NEN 7510: Instrument

VWS, NEN en NICTIZ. Het ministerie van Volksgezondheid, Welzijn en Sport. Het Nederlands Normalisatie-Instituut. Het Nationaal ICT Instituut in de Zorg.

Ze spelen alle drie hun eigen rol in de totstandkoming van NEN 7510, de norm voor Informatiebeveiliging in de zorg. Ze zijn alle drie overtuigd van de noodzakelijkheid van de norm.

Ze hechten dan ook alledrie het grootst mogelijke belang aan een soepele en vooral ook tijdige invoering van de norm. Des te opvallender is het dat geen van de drie toch zeer nauw betrokken instituten veel willen zeggen over de norm zelf. Des te meer over functie, plaats en doel ervan.

‘Zonder die norm komen we geen stap verder.’ Met dit ene nuchtere zinnetje vat Gert-Jan van Boven samen hoe hij de betekenis van NEN 7510 in schat. Hij is directeur van NICTIZ, het instituut dat in 2002 is opgericht om richting te geven aan ICT ontwikkelingen in de zorg. Die ontwikkelingen zijn het waar hij op doelt en waarmee hij, zoals hij zegt, zonder NEN 7510 geen stap verder komt.

Hoewel de letters ICT prominent in de naam van zijn instituut staan, gaan de veranderingen die Van Boven voorstaat het terrein van de ICT ver te buiten. Het gaat om veranderingen in de zorg; veranderingen die mogelijk zijn geworden door de komst van ICT en die nodig zijn om de zorg als geheel effectiever en efficiënter te maken in een samenleving die niet alleen vergrijst (2,5 miljoen mensen in de AOW) maar ook mondiger en veeleisender wordt.

Dat ietwat tweeslachtige – we doen alsof het ICT is, maar het is veel méér – vindt men ook elders in het spraakgebruik rondom NICTIZ. Bijvoorbeeld worden veel van de veranderingen samengevat onder de noemer EPD (Elektronisch Patiënten Dossier). Een typische ICT naam, zou men zeggen, maar wat er mee wordt aangegeven is een complexe vernieuwing in de zorg als geheel, waarin nieuwe opvattingen over de (keten)organisatie van de zorg tot hun recht komen.

Eerste vereiste: regie

Bij VWS wordt de noem het maar dubbelrol van NICTIZ wel degelijk onderkend. Nico Oudendijk, wiens afdeling de ontwikkelingen aanstuurt, vertelt het aldus: ‘NICTIZ kun je zien als het resultaat van een omslag die onder Paars II vorm kreeg. Ook in het veld drong het besef door dat er meer regie nodig was en dat we niet veel verder zouden komen als niet iemand de teugels zou pakken. Je moet altijd afwegen in hoeverre je initiatieven van onder uit laat ontstaan dan wel vanuit één visie het geheel stuurt. In de jaren

van Paars II zagen we in dat de vele subsidiepotjes ons eigenlijk niet verder brachten.

Dus: méér regie. Dat werd NICTIZ. Grof gezegd, werden alle subsidies gestopt en ging het geld naar NICTIZ, die het besteedt aan werk dat nodig is voor de door NICTIZ zelf uitgedragen veranderingstrajecten.’

Uit het betoog van Oudendijk valt op te maken dat er in de sector van de gezondheidszorg al een zekere bereidheid was om zich neer te leggen bij centraal aangestuurde beslissingen. Maar ook als men dat in aanmerking neemt, valt het op hoe stevig het draagvlak van NICTIZ is. Van Boven heeft er wel een verklaring voor: ‘We hebben de Verelendung vermarkt,’ zegt hij met gevoel voor ironie. ‘We konden zonder veel moeite aantonen dat het niet goed liep in de zorg, en dat hebben we gedaan. Vervolgens zijn we met een verbeteringsplan gekomen. In ons eerste jaar hebben we dat uitgedragen en sindsdien wordt er aan gewerkt.’

De goeie naam van NICTIZ zal er ook zeker toe bijgedragen hebben dat NEN 7510 in betrekkelijke rust kon worden voorbereid, zonder al te veel strubbelingen. De norm past natuurlijk volledig in het geregisseerde proces. Als Van Boven stelt dat we zonder norm geen stap verder komen, dan bedoelt hij óók te zeggen dat een norm nodig is om het proces in de hand te houden. Want het gaat snel. Zoals het er nu (zomer 2005) naar uitziet, zullen per 1 januari 2006 de eerste delen (Oudendijk noemt ze hoofdstukken) van het EPD getest kunnen worden. Dan zal er een landelijk schakelpunt zijn (Van Boven: ‘Een google voor de zorg’) dat geautoriseerde informatiegebruikers de weg zal wijzen naar de data bases waarin zij de gewenste patiënteninformatie kunnen vinden. Dan zal er een Elektronisch Medicatie Dossier zijn, zodat de foutenkans bij medicaties fundamenteel kan worden teruggebracht. En dan zal er een Huisartsen WaarnemingsDossier zijn, zodat

waarnemers op de huisartsenposten in principe kunnen weten welke patiënten zij ontmoeten.

Gekozen voor NEN

Zowel Van Boven als Oudendijk noemt de keuze voor NEN een belangrijke. Ook dat past in het beeld van een geregisseerd proces. De zorgsector heeft een lange geschiedenis van zelfregulering, intercollegiale toetsing en dergelijke, maar met de keuze voor NEN heeft VWS zich aan die traditie onttrokken en de gewenste normering als het ware uit de zorg getild.

Belangrijk argumenten daarbij: We moeten zoveel mogelijk profiteren van wat in andere sectoren al gedaan is en we moeten zeker stellen dat we internationaal aansluiting vinden en vasthouden.

Het Nederlands Normalisatie-Instituut, NEN dus, stelt zich tamelijk bescheiden op bij het tot stand brengen van een norm. Nan Besseler, cluster manager Gezondheidszorg bij NEN, zegt het zo: 'We hebben er niets aan als we met een norm aankomen waarin het veld zich niet herkent. We zoeken dus in de eerste plaats contact met alle belanghebbende partijen, zoals in dit geval de ICT-afdelingen, de leveranciers van informatiesystemen en natuurlijk ook de beroepsorganisaties. We stellen vervolgens een normcommissie in en samen met de commissie gaan we op weg naar consensus. Zo'n proces begeleiden, kunnen we goed, bij NEN. Daar hebben we ervaring in. We weten bijvoorbeeld dat consensus niet kan inhouden dat alle partijen op alle details hun zin krijgen. Dan kom je er nooit. Consensus heb je bereikt er als er geen georganiseerde oppositie meer is. Met NEN 7510 zijn we zo ver.'

Extra's ter bespoediging

Helemaal vanzelf is het natuurlijk niet gegaan. Dat blijkt wel uit de extra's die de sector nodig achtte. Extra's in de vorm van implementatiehandboek en drie set Toetsbare Voorschriften. Deze extra's (bekostigd door VWS) zullen de implementatie van NEN 7510 bespoedigen, maar zorgen er anderzijds voor dat de norm zelf tamelijk algemeen en generiek kon blijven en dus heel dicht bij het internationale origineel van de ISO IEC code voor Informatiebeveiliging.

'Het mag ook wel enige extra inspanning kosten,' zegt Oudendijk. 'Als we die drie hoofdstukken van het EPD volgend jaar echt in de lucht hebben dan lopen we internationaal voorop. Dat mag dan ook wel eens gezegd worden. We hebben misschien tijd verloren toen we de dingen nog te veel op hun beloop lieten, maar met deze aanpak halen we dat snel weer in. Bovendien: We hebben nu het momentum. Nu moeten we doorpakken.'

En het vervolg?

Dat laatste beaamt ook Van Boven. Hij heeft al enkele in het oog springende applicaties op het oog, waarmee hij wil gaan scoren. 'Benoembare zorgketens,' zegt hij, 'zoals die rondom diabetes en CVA. Als we daar verbeteringen kunnen aanbrengen door de informatievoorziening te optimaliseren dan zal dat meer opvallen dat het introduceren van een norm. Over NEN 7510 zal het grote publiek zich niet druk maken. Men verwacht nu al niet anders dan dat informatie overal en altijd vlekkeloos wordt uitgewisseld. Over de kwaliteit van de zorg maakt men zich wel zorgen en als NEN 7510 ertoe bijdraagt dat die zorgen kleiner worden, wel – dan hebben we het goed gedaan.'



Het beveiligen van informatie is niet meer weg te denken uit onze huidige maatschappij, ook niet uit de zorg. Het praktisch en realistisch toepassen van informatiebeveiliging is echter nog een hele kunst. NEN7510 is juist vanuit deze gedachten opgesteld!

Alex Beckers, In View bv

De praktijk van NEN 7510

Jaap van der Wel (jvdwel@comfort-ia.nl) is directeur van Comfort-IA en lid van de norm-commissie voor Informatiebeveiliging in de zorg. Publicatie is onder persoonlijke titel.

De Inspectie voor de Gezondheidszorg constateerde na een onderzoek bij twintig ziekenhuizen dat: '(...) ziekenhuizen op dit moment onvoldoende aandacht schenken aan de risico's die de toepassing van ICT met zich meebrengt. 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'¹. Recentelijk bleek weer hoe juist deze opmerking is: de poli van het Spaarne Ziekenhuis moest twee dagen de deuren sluiten omdat een computervirus het bedrijfsnetwerk had platgelegd. Ook de eerstelijnszorg kampt met problemen om de informatievoorziening stabiel te laten functioneren. Bij tal van HAP's en HOED's traden problemen op bij de overgang van het oude Elias systeem naar iets nieuws. Zo gingen brieven uit naar reeds overleden patiënten of werden historische gegevens niet goed overgenomen.

Wie is aan zet?

Directies van zorginstellingen en praktijkhouders in de eerste lijn realiseren zich de risico's gewoonlijk wel maar weten er niet altijd goed raad mee. Bij de zorginstellingen waar zich dit voordoet, moet het hoofd Informatievoorziening dan de problemen maar zien te voorkomen, met af en toe een bijdrage van de huisjurist over patiëntenprivacy. En in de eerste lijn geven de klanten hun ICT-leverancier onder uit de zak als er iets mis gaat, waarop de leverancier met wat gratis dienstverlening weer enige compensatie geeft.

Nu ICT steeds belangrijker wordt, gaat dit zo niet langer. De risico's móeten worden teruggedrongen. Daarvoor is teamwork nodig. In de zorginstellingen door het managementteam. In de eerste lijn door de gebruikers en alle betrokken ICT-leveranciers. De nieuwe norm voor Informatiebeveiliging in de zorg, NEN 7510, concretiseert dit. De norm maakt overigens ook duidelijk dat een professionele opzet van informatievoorziening een complexe



aangelegenheid is geworden. Zo complex dat een individuele praktijkhouder voor de keuze staat om ofwel het meeste uit te besteden ofwel studie te maken van netwerken en computers, om vervolgens nog veel tijd kwijt te zijn met de uitvoering.

Inventariseren als eerste stap

De norm bestaat uit een checklist die, afhankelijk van de manier van tellen, tussen de 125 en 200 punten bevat. Dat is teveel voor behandeling in dit artikel. Daarom beperken we ons tot de 'tien belangrijkste maatregelen', zoals die ook in de bijlagen van de norm worden vermeld (zie kader). Om te beginnen kan de checklist – de volledige



IRIS, OOG VOOR UW ZORG

IGN Automatisering BV Veenendaal

Met **IRIS** heeft IGN Automatisering de opvolging van I.R.I.S.-G en I.R.I.S.-V gerealiseerd. De bestaande EPD systemen waren vanaf 1995 geïmplementeerd bij diverse instellingen in de geestelijke gezondheidszorg en de ouderenzorg. Onder andere de registratie van de basisgegevens, de sociale kaart, het zorg- en/of verpleegplan, medicatie en correspondentie worden middels de standaard functies van **IRIS** ondersteund.

Daarnaast kunnen met **IRIS** alle elektronische berichten van bijvoorbeeld AZR, EI en Prismant worden verwerkt. De activiteiten en verrichtingen worden gepland in de agenda, waarna door het accorderen de gehele administratieve verwerking gereed is. Een grafische en naar eigen inzicht vast te stellen zorgplanfunctie geeft de hulpverlener direct inzage in de status van het zorgproces.

IRIS is toepasbaar in nagenoeg alle sectoren van de zorgketen en is zodanig flexibel opgezet, dat iedere instelling naar eigen behoefte de applicatie kan inrichten. **IRIS** kenmerkt zich door de volledige integratie van registratieve en zorginhoudelijke functies. Vanuit de zorgfuncties worden automatisch de registratieve gegevens verwerkt tot en met de facturering. Middels de geïntegreerde HL-7 communicatiemodule bent u in staat om informatie uit **IRIS** beschikbaar te stellen aan andere informatiesystemen zoals Keuken en ZIS.

Voor meer informatie of een vrijblijvende presentatie neemt u contact op met:

IGN Automatisering BV
Vendelier 55-A 3905 PC Veenendaal
info@ignautomatisering.nl
www.ignautomatisering.nl
0318-690201



HÈT EPD VOOR DE GEZONDHEIDSZORG

Dossiervoering en geheimhoudingsplicht vereisen nou eenmaal beveiliging van medische gegevens. Goed dat deze norm naadloos ingepast kan worden in het NIAZ en HKZ kwaliteitssysteem. Trouwens wel evenveel werk!

Hein van der Reijden, directeur patiëntenzorg Dianet Dialysecentra, namens de KNMG lid van NEN Normcommissie 7510



lijst of de tien punten van het kader – gebruikt worden om de eigen organisatie na te lopen. Managers van grotere organisaties, zoals ziekenhuizen, verpleegtehuizen, revalidatie-instellingen en instellingen voor thuiszorg, zouden dat ook met enige regelmaat moeten doen. Daarnaast is de checklist geschikt als toets van het samenwerkingsverband van kleinere zorginstellingen met ICT leveranciers. Ieder punt van de norm moet ergens in dit verband belegd zijn. In de praktijk vallen echter tal van punten tussen wal en schip. Vooral in de eerstelijnszorg dreigt dit risico. Daar kunnen meerdere ICT-leveranciers namelijk een complexe keten vormen: één voor ASP-diensten, een ander voor de huisartsensoftware, nog één voor de hardware en één voor datacentrum en netwerkdiensten en voor beveiligde opstellingen. Resultaat van de inventarisatie is niet alleen dat risico's zichtbaar worden, maar óók dat de waarde zichtbaar wordt van de goed geregelde zaken. Dat laatste is belangrijk, vooral waar men de specialistische kennis mist om zelf die waarde vast te stellen maar intussen wel aanhikt tegen een hoge prijs – bijvoorbeeld in de eerste lijn.

Met de genoemde tien punten lijst heeft men binnen de kortst mogelijke tijd een eerste indruk van de controle over de informatievoorziening en de nog te verbeteren punten. Bent u tevreden over uw score? Durft u te voorspellen wat de uitkomst is van een check op uw organisatie met de volledige lijst? Zijn de belangrijke beveiligingsmaatregelen getroffen? Krijgt het hoofd Informatievoorziening wel voldoende budget en steun van het managementteam? Volgen de huisartsen wel voldoende de aangeboden cursussen van de softwarefabrikant of bellen ze in plaats daarvan de helpdesk plat?

Nalopen van de organisatie met de volledige checklist hoeft niet veel werk te zijn als goed gebruik gemaakt wordt van de aanwezige kennis en ervaring. Wie kent de sterke en zwakke plekken beter dan de medewerkers van de eigen organisatie? Een objectieve kijk van buiten is daarbij wel wenselijk want wie heeft er beter geleerd om zijn mond maar te houden over steeds terugkerende problemen dan de medewerkers van de eigen organisatie? En wie heeft er beter geleerd om medewerkers-met-stokpaardjes maar een beetje te laten voor wat ze zijn dan het eigen management?

Vervolgens: beleid

Nadat de risico's zichtbaar zijn geworden, kan het management van de zorginstelling het beleid vaststellen waarin prioriteiten worden bepaald, taken verdeeld en budgetten toegewezen. Prioriteiten hangen af van de gevolgen van falende informatievoorziening en de risico's dat dit gebeurt. Voor wat betreft de taken is de ene keer het hoofd Informatievoorziening aan zet om, bijvoorbeeld, het systeembeheer te verbeteren of om, samen met een jurist, ervoor te zorgen dat de uitbestedingscontracten aan de Wet Bescherming Persoonsgegevens gaan voldoen. Maar in andere gevallen is de directie aan zet, bijvoorbeeld om problemen op te lossen die ontstaan door slecht samenspel tussen de afdeling informatievoorziening, medici en verplegend personeel. Slecht samenspel uit zich bijvoorbeeld in gemopper over de ingewikkelde aanlogprocedures (de ontwerper daarvan: het moest toch veilig zijn?) waarvan het lijn-management nooit heeft gezegd hóe veilig die moesten zijn.

Beveiliging kost tijd en geld. Dat is niet het gevolg van de norm voor informatiebeveiliging in de zorg, die is slechts een hulpmiddel. De investeringen zijn nodig om risico's te beheersen zoals die voor patiëntenzorg, imago-verlies en het omzetverlies dat daarop volgt als de potentiële klandizie over problemen leest in een Elsevier-test en vervolgens wegblijft. Draagvlak is belangrijk en wordt onderhouden met quick wins. Kosten worden beheerst door de invoeringsmomenten van maatregelen ook op langere termijn te plannen. Sommige maatregelen kunnen direct worden ingevoerd; voorbeelden zijn het invoeren van een beveiligingsbeleid, het instellen van een beveiligingsorganisatie en het treffen van personele maatregelen (de hoofdstukken 5, 6 en 8 van de norm voor Informatiebeveiliging in de Zorg). Een ander deel kan alleen worden gerealiseerd als het gebruikte softwarepakket wordt aangepast. Deze aanpassingen moeten als wens worden ingebracht in de gebruikersgroep en door de leverancier worden opgenomen in de releaseplanning. Een voorbeeld vormen de functies voor toegangsbeveiliging, die in tal van softwarepakketten tekort schieten². Formeel moet de toegangsbeveiliging voldoen aan de wettelijke regeling voor het medisch beroepsgeheim. Maar in de praktijk is dat problematisch omdat de huidige wetgeving nog uitgaat van het papiertijd-perk³. Wellicht brengt de invoering van de Landelijke Verwijsindex ook op dit punt verbetering.

Al met al blijkt de lijst van noodzakelijke en wenselijke maatregelen gewoonlijk voor jaren werk op te leveren. Informatiebeveiliging is niet een kwestie van een verbeterprojectje doen maar een proces van voortdurende verbeteringen dat gelijke tred moet houden met de toenemende automatiseringsgraad.

En dan aan de slag⁴

Bij de realisatie van de beveiligingsmaatregelen moet men het niet te mooi maken. Het kenmerk van goede informatiebeveiliging is niet de perfectie van de afzonderlijke maatregelen maar het evenwichtige samenspel. Een kwestie van geld zijn de technologische maatregelen. Een grote uitdaging is ervoor zorgen dat iedereen verantwoord omgaat met die technologie.

1 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

2 Zie Jaap van der Wel, Nanne Homma, *Gegevensbeveiliging aan alle kanten lek*, Automatisering Gids 5 september 2003, te vinden op www.comfortia.nl/ag1.pdf

3 Zie Jaap van der Wel, *Spoort de medische praktijk nog met de wettelijke regeling voor het beroepsgeheim?*, Journaal Privacy in de Gezondheidszorg van 18 april 2005, zie www.comfort-ia.nl/wgbo.pdf

4 Zie www.nen7510.org voor praktische voorbeelden

5 De vragen zijn afkomstig uit bijlage B die is opgenomen in de drie toetsbaar voorschriften NEN7510 waarvan de ontwerpnorm op 18 mei 2005 is gepubliceerd (het 'groentje' door het Nederlands Normalisatie-instituut (NEN))

Afkortingen

ASP: Application Service Provider, een

leverancier die rekencentrumdiensten levert.

HAP: Huisartsen Post, samenwerkingsverband rondom vervangings-/weekenddiensten.

HOED: Huisarts Onder Eén Dak, samenwerkingsverband rondom gezamenlijke faciliteiten zoals huisvesting

NEN: Nederlands Normalisatie-instituut

We moeten natuurlijk wél uiterst voorzichtig omgaan met vertrouwelijke, medische informatie van mensen. De veiligheid met betrekking tot het inzien van de gegevens dient goed geregeld te zijn.

Hans Hoogervorst, Minister van VWS, (uitsproken op het Medisch-Informatica Congres)



Geef uw informatiebeveiliging een rapportcijfer!⁵

Tel één punt voor ieder antwoord dat met ja beantwoord wordt. Nul punten ingeval van nee, of onbekend of 'lossen we op als we tegen een probleem oplopen'. Een aftrekpunt als vraag 10 met nee wordt beantwoord.

Vraag	Directies van zorginstellingen	Directies van zorginstellingen
	<i>Voorbeeld: Ziekenhuis met twee locaties</i>	<i>Voorbeeld: HAP waarbinnen de huisartsen gezamenlijk de huisartsen software hebben geselecteerd</i>
1 Beleidsdocument voor informatiebeveiliging	Zijn zwakke plekken bekend? Is een selectie gemaakt om het komende jaar aan te pakken?	Voorbeeld: Analyse van de rapportage van de beveiligingsincidenten van vraag 10/Bundeling van de ervaring van huisartsen met hun gezamenlijke leverancier. Met selectie van actiepunten voor het komend jaar.
2 Toewijzing en vastlegging van verantwoordelijkheden voor informatiebeveiliging	Bijvoorbeeld in de vorm van inventarisatie van de taken van het lijnmanagement, de afdeling Informatievoorziening, de directie en gezamenlijke goedkeuring.	Zijn checklistitems van NEN7510 verdeeld over de con-tractpartners en in contracten (of nadere brieven) opgenomen?
3 Bewustwording, opleiding en training voor informatiebeveiliging	Worden de ervaringen van nieuwkomers na enkele maanden geïnventariseerd, lettend op snelheid van inwerken, opvallende punten, punten die beter zouden moeten?	1) Is er een opleiding voor het gebruik van het pakket (inclusief beveiliging zoals backup procedures, beveiliging tegen diefstal e.d.), 2) Volgen huisartsen die opleiding?
4 Maatregelen tegen kwaadaardige programmatuur	Virusscanner, firewall, mogelijkheden van medewerkers om zelf software te installeren (verbiedt bijvoorbeeld 'handige programmaatjes' van derden die via internet contact leggen met de buitenwereld)	Virusscanner, firewall, wie neemt dit voor zijn rekening (gewoonlijk de ASP leverancier)
5 Ontwikkelen en implementeren van continuïteitsvoorzieningen en -plannen	Is er een dergelijk plan? Wordt er jaarlijks/twee jaarlijks wel eens een oefening gehouden?	Welke afspraken zijn er met de ASP leverancier? Heeft u zich laten rondleiden langs de apparatuur en voor de hand liggende vragen gesteld?
6 Intellectueel eigendom	Worden bijvoorbeeld alle plekken van kantoor-automatisering afgerekend?	Worden alle installaties van de huisartsensoftware afgerekend met de pakketleverancier?
7 Beveiliging van bedrijfsdocumenten (Voorbeelden zijn medische dossiers, declaraties e.d.)	Blijven deze toegankelijk, worden deze conform de wettelijke bewaartermijn (nu voorlopig 15 jaar) vernietigd?	Extra aandachtspunt is de overgang van een oud naar een nieuw huisartsensysteem: worden alle gegevens meegeconverteerd, zo niet, blijven de gegevens uit het oude systeem gemakkelijk beschikbaar de komende jaren?
8 Bescherming van persoonsgegevens	Worden de goede gegevens in de medische registratie vastgelegd (niet te veel, niet te weinig, zie het groene boekje van de KNMG)	
9 Naleving beveiligingsbeleid	Wordt de naleving af en toe geëvalueerd en onafhankelijk gecontroleerd? (zien is geloven)	Testen is een notoir probleem in de eerste lijn omdat het teveel werk kost om dat grondig te doen.
10 Het rapporteren van beveiligingsincidenten	Is er een overzicht van problemen ('incidentenregistratie')	Is er een overzicht van problemen, per huisarts bijgehouden (spreadsheet, nog mooier: storingsadministratie van de ASP leverancier)



Platform onafhankelijk gegevens uitwisselen met Siemens OPENLink™

Doeltreffend inspelen op de toekomst met integratie van informatiesystemen

Het zorgproces speelt zich niet meer uitsluitend af binnen de muren van één zorginstelling. Zoekt u naar een oplossing voor de integratie van informatiesystemen binnen én buiten uw organisatie?

Siemens biedt met OPENLink™, een applicatie waarvan het succes al wereldwijd is bewezen, met de implementatie bij meer dan 1.000 zorginstellingen. Met SiemensOPENLink™ beschikt u over een onafhankelijk integratie platform voor de gestandaardiseerde uitwisseling van gegevens.

Siemens speelt al jaren een voortrekkersrol in ICT en heeft zitting in nationale en internationale commissies, die zich onder andere bezighouden

met HL7, DICOM, XML, IHE en normeringen voor medische technologie (door ISO, CEN en NEN). Wij delen die kennis graag en zoeken samen met u naar een toepassing die op uw organisatie is toegesneden om zo mee te bouwen aan een gezonde en ondernemende zorginstelling.

Toe aan een zorg minder? Neem dan contact met ons op.

Siemens Nederland N.V.
Medical Solutions
Postbus 16068
2500 BB Den Haag
tel. 070 - 333 3014

www.siemens.nl/gezondheid

SIEMENS

CBO: NEN 7510 is kwaliteits-instrument bij uitstek

'Wij zijn de inspectie niet,' zegt Strasmir Cucic. 'Het is voor ons dus niet essentieel dat NEN 7510 aanknopingspunten biedt voor externe toetsing. Wat ons instituut zou willen benadrukken is dat instellingen de norm kunnen benutten als instrument bij het verbeteren van zorgprocessen.'

Cucic werkt bij het Kwaliteitsinstituut voor de Gezondheidszorg CBO. Hij is daar manager van een afdeling die de opmerkelijke naam Kennis draagt. Onder meer houdt deze afdeling de ontwikkelingen in de ICT bij, voor zover deze van betekenis (zouden) (kunnen) zijn voor de kwaliteit van de gezondheidszorg. Het CBO is ruim 25 jaar geleden door de Landelijke Specialisten Vereniging opgericht als Centraal Begeleidings-Organ voor de Inter-collegiale Toetsing. In de letters CBO is deze oorspronkelijke naam nog wel terug te vinden, maar voor het overige blijkt het huidige instituut erg veel breder van opzet dan het oorspronkelijke 'begeleidingsorgaan'. Naast toetsing zijn ook andere activiteiten ontwikkeld op het vlak van scholing, richtlijnontwikkeling en kwaliteitsverbetering. En in een tijd waarin ketenzorg centraal in de aandacht staat beperkt het CBO zich niet tot de specialisten, maar dekken de activiteiten de eerste tot de derdelijn.

Informatievoorziening en kwaliteit

'Je moet goed bedenken dat wij het aan de zorgprocessen kunnen zien of de informatievoorziening in een instelling heel goed of heel slecht geregeld is. Daar hoeven we niet voor naar de informatievoorziening zelf te kijken; dat zien we al aan de effecten. En dat houdt in dat ICT wel degelijk tot ons aandachtsgebied behoort. Wij zijn een kwaliteitsinstituut in de gezondheidszorg, en ICT bepaalt mede de kwaliteit van de zorg. In dit perspectief zien wij de norm NEN 7510. Draagt deze bij aan de verbetering van zorgkwaliteit? Het antwoord is 'ja'. Dus is het goed.'

Een 'handig' instrument

Cucic gebruikt veelvuldig het woord 'handig' in zijn betoog over NEN 7510. Hij vindt de norm een handig referentiekader en een handig instrument. Met een zekere flair plaatst hij de norm in de traditie van de gezondheidszorg. 'De zorg heeft altijd veel aandacht gehad voor normen en standaarden. Dat waren dan wel vooral 'eigen' normen, met daaromheen ook

eigen systemen voor accreditatie en dergelijke. Maar men is zich in de zorg altijd wel bewust geweest van het belang van normering.' Hij zegt het er niet bij, maar in zekere zin illustreert zijn instituut, opgezet immers voor 'intercollegiale toetsing', zijn bewering.

'De NEN norm,' vervolgt hij, 'tilt de standaardisatie juist uit de eigen kring. En dat is goed. Ik vind het dan ook vooral van belang dat NEN 7510 heel dicht bij de internationale code voor informatiebeveiliging (ISO IEC 177799) is gebleven. Dat is een internationale norm. Die geeft houvast, in die zin dat je als instelling zeker weet dat je het internationaal geaccepteerde niveau van Informatiebeveiliging nastreeft. De NEN norm vertaalt deze internationale norm naar nationaal niveau, en zet dan ook nog de generieke ISO-code om naar een zorgspecifieke standaard. Wat zou je nog meer willen?'

NEN 7510: tussen specifiek en generiek

Volgens Cucic heeft de zorgsector een sterke neiging om zichzelf 'anders' te vinden. Anders dan andere sectoren in de maatschappij. Dat is ook te verklaren uit het feit dat de zorg nu eenmaal met mensen van doen heeft en dus inderdaad bijzondere voorzieningen moet treffen als het gaat om privacy-bescherming en dergelijke.

Tegelijkertijd is de zorg een heel gewone bedrijfstak. 'Ruim 80% van de ziekenhuizen in Nederland gebruikt SAP,' stelt Cucic vast. Waarmee hij maar zeggen wil dat de ICT-leveranciers van de zorg ook nu al internationale bedrijven zijn en dat dit alleen zal maar toenemen. De ICT-ontwikkelingen laten zich niet dwingen nationale opvattingen en al helemaal niet door de zorg-sector in een land. In dat licht bezien, is het van belang dat er een balans wordt gevonden tussen enerzijds het eigene van de zorg en het eigene van Nederland en anderzijds het algemeen geldende, dus zeg maar generieke, van de internationale ICT-ontwikkelingen. De norm NEN 7510 kan volgens Cucic een belangrijke brugfunctie hebben, mits het veld de norm ook werkelijk omarmt.

NEN 7510: ook ter interne stimulering

'De kracht van de norm.' zegt Cucic, 'is dat hij stimuleert om de dingen zo goed mogelijk te doen. De instelling die de norm correct implementeert krijg boven tafel wat er niet helemaal goed, of misschien zelfs helemaal niet goed gaat in de informatievoorziening en de communicatie. Dat zou mijn advies zijn aan de sector: Gebruik de norm om de informatie-uitwisseling te verbeteren, zowel binnen de eigen organisatie als tussen de eigen instelling en andere stations in de zorgketen.'

Met het laatste plaatst Cucic eens te meer het ontstaan van NEN 7510 in het totaalbeeld van de hedendaagse ontwikkelingen in de zorg. Van 'eiland' naar 'keten'. Van eilandautomatisering naar (supply) chain management. Een goed gedefinieerde norm voor de informatie-overdracht is in dit proces van levensbelang. Volgens het CBO, bij monde van Strasmir Cucic, voorziet NEN 7510 is deze voorwaarde.

Informatiebeveiliging in kleine praktijken

Het ligt voor de hand dat huisartsen, fysiotherapeuten, tandartsen en in het algemeen 'kleine zelfstandigen' in de zorg een ander zicht hebben op het gebruik van ICT in hun werk dat hun collega's in grotere instellingen. Zij hebben geen ICT-afdeling die de techniek up to date houdt, die in de slag gaat met leveranciers, die softwarepakketten vergelijkt en nieuwe functies implementeert. Dat is allemaal hun eigen verantwoordelijkheid. Zoals die huisarts zei: 'Ik kan er wel iemand voor aanwijzen, maar dat blijkt ik dan toch weer zelf te zijn.' Het ligt dus ook voor de hand dat er in de eerste lijn anders over NEN 7510 gedacht wordt dan elders in de zorgsector. NEN-norm gaat voor extra werk zorgen, zoveel is zeker. En voor wie? Ook dat is te voorspellen.

In de Toetsbare Voorschriften die bij NEN 7510 onder de naam NEN 7511 zijn gemaakt wordt het verschil in perceptie en ervaring tussen de verschillende spelers in de gezondheidszorg onderkend. Waarom anders zouden er drie sets Toetsbare Voorschriften zijn ontwikkeld? Eén set voor de complexe organisaties, een tweede voor allerlei samenwerkingsverbanden en, inderdaad, een derde set voor wat genoemd wordt de 'solopraktijken'. Een niet geheel correcte benaming, die bij nader inzien blijkt te slaan op de kleine praktijken, van de zelfstandig en alleen werkende huisarts tot de groepspraktijk van twee tot vijf of zes (tand)artsen, therapeuten, psychologen of verloskundigen. Een grote groep al bij al, van in totaal een kleine 70.000 beroepsbeoefenaren, verdeeld over zo'n 15.000 praktijken. Een in termen van informatie-beveiliging ook uiterst belangrijke groep, al was het maar omdat een zeer groot deel van het totaal aan patiënteninformatie in eerste instantie via dit fijn vertakte net van zorgverleners wordt vergaard. (Dat in later stadium instellingen in de tweede lijn veel van die informatie opnieuw

moeten vergaren is nu juist iets dat door slim ICT-gebruik zou moeten kunnen worden voorkomen...)

Dilemma's

De presentatie van de Toetsbare Voorschriften vond plaats op 18 mei 2005. Zo ook de presentatie van de Toetsbare Voorschriften voor solopraktijken.

Wat er naar voren kwam tijdens deze presentatie was dat het (a) een goede gedachte is geweest om NEN 7510 via Toetsbare Voorschriften te verbijzonderen voor de kleine zelfstandigen in de zorg, en (b) dat die goede gedachte niet genoeg is en vraagt om een vervolg. Carinke Buiting, die als stafmedewerker automatisering is verbonden aan het Nederlands Huisartsen Genootschap (NHG), verzorgde de presentatie, daarin bijgestaan door Gerard Freriks, lid van de normcommissie. Zij schetsten de dilemma's van de kleine praktijken als volgt: Kleine praktijken hebben er enerzijds alle belang bij dat er een norm zoals NEN 7510 komt. Zo'n norm geeft houvast. Het is vaak moeilijk om te

bepalen of je iets goed doet, of althans goed genoeg. Een norm kan dan helpen. Als je moet kiezen is het erg plezierig als je kunt uitgaan van een norm. De software die er niet aan voldoet valt zonder meer af; de software die er wel aan voldoet heeft in ieder geval een zekere basiskwaliteit.

Anderzijds is er een zekere beduchtheid ten opzichte van een norm. De kleine praktijk heeft immers grote en machtige organisaties als tegenspelers en wat gaan die met de norm doen? Wat gaat de inspectie en wat gaan de zorgverzekeraars doen met de norm? Hoe gaan die de norm interpreteren en hanteren en met ingang van wanneer? Wat halen we ons op de hals, of misschien zelfs 'om' de hals, als een strop?

Gewenste extra's

Buiting en Freriks benadrukken dat het weinig zin heeft om de 59 pagina's Toetsbare Voorschriften zonder meer naar de individuele praktijkhouders te sturen met de opdracht de norm te implementeren. Dat zal niet goed gaan. Beiden zien zowel voor de koepelorganisaties als voor NEN zelf ondersteunende taken weggelegd. Bijvoorbeeld het ontwikkelen van modellen. Het is één ding om voor te schrijven dat er ook in een kleine praktijk een beleidsplan informatie-beveiliging moet komen, iets anders is, aan te geven wat daar dan in moet staan. Dat is heel goed in een model te vangen en daar zouden de koepelorganisaties, samen en samen met NEN, aan moeten gaan werken. Dergelijke ondersteuning, die bij veel van de nieuwe voorschriften te geven is, zou het proces van implementatie alleen maar verbeteren en versnellen.

Ook wanneer er adequate ondersteuning komt mogen de normstellers er niet van uitgaan dat NEN 7510 op zeer korte termijn zal zijn ingevoerd in alle kleine praktijken. Het is één van de bezorgdheden die er leeft: Stel je voor dat de inspectie en dat verzekeraars al gaan 'afrekenen' op werken volgens de norm terwijl de praktijkhouders deze redelijkerwijs nog niet hebben kunnen invoeren. Tot de extra's die vanuit deze kring worden gevraagd behoort dus ook extra tijd. De koepelorganisaties, die de kleine praktijken vertegenwoordigen in de discussie, zien NEN 7510 als 'groeimodel'. Eerst de tien belangrijkste maatregelen, zoals die ook door de normcommissie(s) worden aangewezen.

Daarna het vervolg, met tussentijdse evaluaties en zonodig ook bijstellingen. Dus kan er nu nog geen sprake zijn van 'het' implementeren van 'de' norm – een mening die anderen al wel verkondigen.

Bijvoorbeeld: ASP/SLA...

Een gebied waarop zeker ondersteuning door koepelorganisaties vereist zal zijn is dat van de zogeheten Application Service Providers (ASP's) en de zogenaamde Service Level Agreements (SLA's). Deze twee begrippen zullen een vrij belangrijke rol kunnen spelen in toekomstige ICT-toepassingen, terwijl er gerede kans is dat praktijkhouders niet eens weten waar ze voor staan.

ASP's komen in beeld als men bedenkt dat NEN 7510 zulke hoge beveiligingseisen gaat stellen aan de pc's, de netwerken waarin deze zijn opgenomen en de ruimte waarin de apparatuur staat opgesteld, dat als vanzelf de gedachte opkomt om dit geheel dan maar uit te besteden. Je koopt dan geen computer meer. Je koopt computercapaciteit bij een leverancier (provider) die zich heeft gespecialiseerd in computerdiensten (services) en de software (applications) die daarvoor nodig is. Via het internet krijg je als praktijkhouder aansluiting op de computers van de provider en het is vervolgens aan hem om de fysieke beveiliging van de computers te waarborgen. Probleem minder, zal men zeggen. Het nieuwe probleem is dat men wel zelf verantwoordelijk blijft voor het werk dat nu door een ander wordt gedaan. Om daar zo goed mogelijk aan te beantwoorden moet er een SLA worden gesloten. En zo'n SLA is moeilijk. Dat komt niet alleen door de aard van de afspraken, die niet alleen een financiële maar ook een juridische kant hebben. Dat komt ook door de procedures die moeten worden opgesteld, die zeker moeten stellen dat de afspraken, niet alleen aan leverancierszijde maar ook aan afnemerszijde, ook werkelijk worden opgevolgd. Volgens Buiting en Freriks ligt hier een schone taak voor de koepelorganisaties.

Intussen bevestigen alle koepelorganisaties het belang van de norm. Eenmaal geïmplementeerd zal NEN 7510 de positie van de kleine zelfstandige niet verzwakken maar versterken. Juist omdat de geïmplementeerde norm toetsbaar zal zijn, zullen praktijkhouders minder moeite hebben met het overtuigen van inspectie of verzekeraar van de kwaliteit van hun werk.

Ruud Bongers (PwC) en Kees Louwerse (LUMC)

Doe wel. Doe niet.

Tips bij het implementeren van NEN 7510

Het was natuurlijk geen toeval dat er in de periode waarin NEN 7510 tot stand kwam onderzocht werd hoe goed of slecht het met de informatiebeveiliging gesteld was. Integendeel. Informatiebeveiliging was een onderwerp dat de aandacht kreeg, mede ook vanuit de opvatting dat de kwaliteit van de zorg rechtstreeks beïnvloed wordt door de kwaliteit van informatievoorziening.

Wij zijn beiden bij zo'n onderzoek betrokken geweest. Die onderzoeken hadden een doel in 'eigen kring'. Het zijn dan ook niet zozeer de onderzoeksresultaten die we hier willen publiceren als wel een handvol ervaringen die ons inziens van nut kunnen zijn bij het implementeren van NEN 7510. Ervaringen die we beiden opdeden, ondanks het feit dat onze onderzoeken qua setting en doel nogal verschilden. Dat maakt de onderstaande opmerkingen wellicht extra relevant. Wanneer je bijvoorbeeld in academische ziekenhuizen precies hetzelfde vaststelt als in algemene, dan betekent dat iets voor de waarde van de observatie.



Zorg kan niet zonder aandacht voor kwaliteit. Kwaliteit in de zorg betekent aandacht voor patiëntveiligheid en informatiebeveiliging. NEN 7510 en de toetsbare voorschriften geven een invulling aan informatiebeveiliging.

Gerard Freriks, TNO

Zie informatiebeveiliging als proces

Het is onze ervaring dat informatiebeveiliging moet worden gezien als proces, en dus vooral niet als project. Informatiebeveiliging heeft geen begin en geen eind, maar vergt blijvende aandacht.

Het is zeker relevant op dit juist in de huidige periode vast te stellen. Nu NEN 7510 er ligt, is de verleiding groot om het implementeren van de norm als project op te voeren, met de suggestie van 'als dat achter de rug is zijn we klaar'. Dat is dus geen goede aanpak.

Werk samen

De academische ziekenhuizen bleken niet allemaal even ver gevorderd op alle deeltrajecten van de informatiebeveiliging. Dat geconstateerd hebbend, spraken zij af, twee aan twee die hoofdstukken van NEN 7510 aan te pakken waarin men het verst gevorderd is. De ervaringen worden vervolgens overgedragen aan de collega's. Zo kan men maximaal van elkaar leren en krijgt het implementatieproces optimale ondersteuning.

Dergelijke vormen van samenwerking tussen instellingen zijn sterk aan te bevelen. Dit te meer omdat het doel toch ook al ligt in een gezamenlijke informatie infrastructuur.

Doe het zelf; uitbesteden kan (bijna) niet

Informatiebeveiliging is vrijwel niet te realiseren via outsourcing. Het is de eigen organisatie waarin het proces een plaats moet krijgen en het zijn de eigen mensen die ernst moeten maken met het beveiligen van de informatie en de kwaliteit van de communicatie. Dit principe geldt ook voor de kleine praktijken, ook al gaan daar stemmen op om via ASP-achtige oplossingen aan NEN 7510 tegemoet te komen. Daar zijn argumenten voor te geven (kennis, kosten) en voor zover het de technische voorzieningen betreft zijn er ook afspraken te maken met leveranciers om aan de norm te voldoen. Maar feit blijft dat praktijkhouders zelf verantwoordelijk zijn voor de informatiebeveiliging en dat hun eigen mensen, in hun dagelijkse omgang met informatiesystemen, het sluitstuk op de beveiliging vormen. Daar verandert het feit dat systemen wellicht elders staan opgesteld helemaal niets aan.



Ik ben als extern consultant betrokken bij de ontwikkeling van de architectuur van de basisinfrastructuur bij NICTIZ. Vanuit die rol heb ik een direct belang bij het realiseren van een goede informatiebeveiliging. Het uitwisselen van patiëntinformatie kan namelijk alleen plaatsvinden indien er voldoende waarborgen zijn dat de informatiebeveiliging niet alleen in de basisinfrastructuur, maar ook bij de zorgverleners goed is geregeld. Daarin speelt het implementeren van de toetsbare voorschriften gebaseerd op NEN 7510 een cruciale rol.

Frans van den Dool, Verdonck, Klooster & Associates

Zie beveiliging als organisatievraagstuk

Het is verleidelijk om informatiebeveiliging te zien als technisch probleem, zo één waarmee je naar de ICT afdeling stapt met de opdracht: 'Regel dit'. Maar het is geen technisch probleem. Informatiebeveiliging is een organisatievraagstuk dat maar zeer ten dele met technische middelen kan worden opgelost. Natuurlijk zijn er technische voorzieningen nodig om computers en netwerken te beveiligen, om de toegang tot gegevensbestanden te regelen en te bewaken, om het gebruik van programma's te reguleren enzovoorts. En natuurlijk moeten deze voorzieningen voldoen aan de kwaliteitsnormen die worden gesteld. Maar daarmee is het vraagstuk van de informatiebeveiliging niet opgelost. Daarmee zijn hooguit de technische 'afhech-tingen' genoemd. Het vraagstuk zelf moet worden opgelost in het dagelijks werk van alle informatiegebruikers, ergo: in de organisatie.

Denk in ketens


We kunnen ook zeggen: denk in termen van communicatie. Informatie is van betekenis en van waarde naar gelang ze overdraagbaar is. Neem dit als uitgangspunt. Informatie is niet goed vastgelegd als ze niet dáár in het zorgproces voorhanden kan zijn (beschikbaarheid) waar ze op zeker moment nodig is en als ze op dat moment op die plaats niet gegarandeerd juist is (integriteit). Het is niet langer voldoende om informatie te vergaren en vast te leggen voor eigen gebruik, voor gebruik binnen de afdeling of zelfs voor gebruik binnen de instelling. Informatie is er omwille van de informatieoverdracht.

Zie NEN 7510 als middel tot...

NEN 7510 is geen doel op zichzelf, maar een middel om te komen tot verbeteringen in de zorg. Zo bezien biedt NEN 7510 ook kansen. Implementeren van de norm maakt zaken

zichtbaar en brengt met zich mee dat onderwerpen expliciet aan de orde komen die wezenlijk zijn voor de kwaliteit van de zorg. Waartoe precies men de norm als middel wil zien kan de organisatie zelf bepalen. De norm is gewillig... De norm is voor de één een middel om het denken in processen te bevorderen; voor de ander een middel om het niveau van procesbeheersing op te voeren. Hier wordt de norm gebruikt om het denken in eilanden af te leren (en het denken in ketens te stimuleren); daar wordt de norm gezien als (kwaliteits)-managementinstrument. De uitgangssituatie van de organisatie zal mede bepalen waar de accenten worden gelegd.

De auteurs van deze bijdragen zijn beide betrokken geweest bij onderzoek naar de stand van zaken bij informatiebeveiliging in de zorg. Bij Ruud Bongers ging het om een afstudeeronderzoek, met enquêtes onder algemene ziekenhuizen. Kees Louwerse organiseerde samen met zijn collega's in andere academische ziekenhuizen een soort nulmeting aan de hand van de (toen nog) conceptnorm NEN 7510. Hoe verschillend de onderzoekssituaties ook waren, in de bevindingen bleken veel overeenkomsten. Afgezien van meetgegevens e.d. bleken er ook een aantal do's and don'ts uit beide onderzoeken naar voren te komen. Enkele daarvan worden hier besproken. (red.)



Veilig Digitaliseren met Oldelft Benelux



Oldelft Benelux



System Integrator en Service Provider

analoge en digitale medische apparatuur
en innovatieve Healthcare ICT systemen



www.oldelftbenelux.nl
tel. 0318-583125
info@oldelft.nl



Inspectie voor de Gezondheidszorg: NEN 7510 sterk aanbevolen!

NEN 7510 blijkt wonderwel aan te sluiten bij de wensen die de Inspectie voor de Gezondheidszorg na eigen onderzoek ten aanzien van ICT gebruik in de zorg heeft geformuleerd. 'De vastgestelde problemen zouden zijn opgelost als NEN 7510 zou zijn geïmplementeerd,' zegt Jan Vesseur, die ICT aangelegenheden binnen de IGZ coördineert. 'Doe er je voordeel mee!' roept hij het veld toe.



Dat de IGZ de norm NEN 7510 omarmt impliceert dat de inspectie de norm ook zal gaan gebruiken. Vesseur laat daar weinig twijfel over bestaan: 'Als een methode of een systeem onder beroepsgenoten gebruikelijk is geworden, vinden wij als inspectie dat een individuele zorgverlener of instelling een goed verhaal moet hebben als men een andere koers wil varen. NEN 7510 heeft nu al een brede acceptatie en zal dus de status 'gebruikelijk onder beroepsgenoten' spoedig bereiken. Men mag er dus van uit gaan dat de IGZ de norm zal gaan hanteren. We zijn blij dat de norm er is. Als hij goed geïmplementeerd wordt zullen veel van de huidige bezwaren vervallen die we als inspectie hebben tegen het ICT gebruik in de zorg.'

Eigen onderzoek IGZ

De door Vesseur aangehaalde bezwaren waren zichtbaar geworden door een door de IGZ inge-

steld onderzoek (najaar 2003) naar de kwaliteit van ICT toepassingen in de zorg. Dit onderzoek stond los van het traject dat leidde tot NEN 7510, maar toonde dus wel de wenselijkheid van de norm aan. Bij het onderzoek waren twintig ziekenhuizen betrokken.

De bevindingen vielen niet mee. Vesseur: 'Er moesten veel onvoldoendes worden gegeven. Het inhoudelijke, meestal decentrale beheer van applicaties bleek vaak slecht afgestemd op het technische, meestal centrale beheer van de ICT-voorzieningen. Als er al ICT beleid geformuleerd was, bleek het maar al te vaak onduidelijk wie daar verantwoordelijk voor was en wie er bevoegd was om bepaalde beslissingen te nemen. Daarbij bleek de centrale sturing over het algemeen zwak. Heel belangrijk vinden wij dat het risico management onder de maat bleek. Er zijn heel veel mogelijke oorzaken voor het uitvallen van ICT systemen; van een eenvoudige

stroomstoring tot heel gecompliceerde conflict-situaties in procedures, software of gegevensbestanden. En we kunnen niet genoeg benadrukken dat het uitvallen van ICT systemen zeer ernstige gevolgen kan hebben voor de zorgverlening. Veel meer dan vroeger is ICT gebruik direct verbonden met zorgprocessen. Des te belangrijker is het dat de risico's systematisch worden geanalyseerd en in kaart gebracht. En des te belangrijker is het dat er maatregelen worden getroffen die zich qua zwaarte verhouden tot de risico's die men wil bestrijden. Dat gebeurt nu onvoldoende.'

In verband met het laatste komen de rapporteurs van het IGZ met een aanbeveling die zonder veel moeite zou kunnen worden opgenomen in de tekst van NEN 7510. 'Zorg voor een goede opvang, registratie en analyse van de problemen die zich voordoen,' zeggen Vesseur c.s. Zorg voor 'incidentenregistratie' zegt de norm. Het is een van de vele voorbeelden waarin de norm een antwoord geeft op de vragen die de inspectie stelt.

'We hebben in onze verslaglegging een andere clustering gekozen dan die in de norm,' zegt Vesseur. 'We hebben om het zo maar te zeggen minder hoofdstukken dan de elf onderwerpen die de norm onderscheidt. Maar je kunt ons rapport en de norm makkelijk naast elkaar leggen en dan blijkt dat we het echt over dezelfde dingen hebben. Eén van onze hoofdaanbevelingen is dan ook dat instellingen in de gezondheidszorg NEN 7510 moeten volgen. Dan zullen heel veel van de door ons aangewezen tekortkomingen zichtbaar worden; dan kunnen er dus ook passende maatregelen worden genomen en kunnen ook de verbeteringen zichtbaar worden gemaakt.'

Veiligheid, kwaliteit en ICT

Vesseur ziet het toepassen van NEN 7510 als noodzakelijk onderdeel van veiligheidsmanagement, en dit vervolgens als noodzakelijk onderdeel van kwaliteitsbeleid. 'Daarmee past het een en het ander ook in het perspectief van de Inspectie,' zegt hij. 'Wij werken nu eenmaal op basis van de Kwaliteitswet en de Wet BIG. Ook als we ons bemoeien met ICT gebruik moet kwaliteit in de zorg het perspectief bepalen.'

Hij zou daarbij overigens willen voorkomen dat ICT alleen maar gezien wordt als iets dat schade kan veroorzaken. Bij onderwerpen zoals beveiliging ontstaat de neiging daartoe enigszins, maar Vesseur wil die neiging tegengaan. ICT kan ook wel degelijk worden gebruikt om schade (in de gezondheidszorg) te voorkomen en kan dus ook wel degelijk bijdragen aan de kwaliteitsverbetering in de zorg. Als voorbeeld noemt Vesseur de ICT systemen voor het voorschrijven van medicatie. 'Met zulke systemen kun je het risico van conflicterende medicijnen tegengaan,' stelt hij vast. 'Dat is een bestaand risico en een onderkend probleem. De technologie voor dergelijke systemen is er inmiddels. En dan komt er een keer een moment waarop het wel-beschouwd niet langer verantwoord is om zulke systemen niet te gebruiken. Dat moet dan natuurlijk ook weer met de nodige waarborgen op het vlak van bedrijfszekerheid en betrouwbaarheid en dus ook informatiebeveiliging. Als we, bijvoorbeeld vanuit de inspectie, het toepassen van dergelijke systemen willen bevorderen, kan dat erg veel beter in een omgeving die zowel technisch als organisatorisch, aantoonbaar voldoet aan NEN 7510. Doen dus, die norm. Implementeren die norm. Dat is echt een stap vooruit!'



Ik vind de norm NEN 7510 belangrijk, omdat elektronisch uitwisselen van gegevens steeds vaker gaat voorkomen en dan is het essentieel dat de gegevens goed beveiligd zijn opgeslagen en goed beveiligd worden getransporteerd.

Frits de Roever, GGZ Noord-Holland Noord, voorzitter VI&G

De beveiligingsplicht in wet- en regelgeving

Sjaak Nouwt is werkzaam bij het Centrum voor Recht, Technologie en Samenleving (TILT) van de Universiteit van Tilburg.

Inleiding

De beveiliging van persoonsgegevens is één van de algemene privacybeginselen zoals die aan het begin van de jaren '80 al zijn geformuleerd door de Organisatie voor Economische Samenwerking en Ontwikkeling in de *OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Parijs 1981) en door de Raad van Europa in het *Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens* (Straatsburg 28 januari 1981).

De algemene privacybeginselen uit deze internationale documenten vormen nog steeds de grondslag voor de huidige bescherming van persoonsgegevens, ook wel informatiele privacy genoemd, in ons land. Het Nederlandse stelsel van privacybescherming bestaat uit een nadere uitwerking van deze beginselen. Met de maatregelen op nationaal niveau is invulling



De DBC's maken de zorgbedrijven tot ondernemingen die opereren in een markt die de Elseviertest transparant maakt. Degenen met een zwakke informatievoorziening zullen het niet redden. Het is up –met NEN 7510– or out.

Jaap van de Wel, Comfort-IA

gegeven aan de doelen die zijn neergelegd in de afzonderlijke privacybeginselen.

Het beveiligingsbeginsel houdt in dat persoonsgegevens moeten worden beschermd met redelijke beveiligingsmaatregelen tegen verlies van of ongeoorloofde toegang tot gegevens alsmede tegen ongeoorloofde vernietiging, gebruik, verandering of uitlekken daarvan. Bij het treffen van maatregelen ter beveiliging van persoonsgegevens moet onder andere worden gelet op de mate van gevoeligheid van de gegevens, de mate waarin de toegang tot de gegevens binnen een organisatie beperkt dient te worden en de behoefte aan het kunnen bewaren van de gegevens gedurende langere tijd. Beveiligingsmaatregelen moeten zijn gebaseerd op gangbare methoden en technieken van gegevensbeveiliging.

Wat gangbaar is hangt af van de stand van de techniek, die voortschrijdt met de tijd. De maatregelen worden getroffen om persoonsgegevens te beschermen tegen:

- a verlies en onbedoeld wissen van gegevens;
- b onbevoegde toegang tot gegevens;
- c de ongeoorloofde vernietiging van gegevens, waaronder begrepen het onbevoegd vernietigen en ontvreemden van opslagmedia;
- d onbevoegd gebruik van persoonsgegevens inclusief het ongeautoriseerd kopiëren van gegevens;
- e ongeoorloofde wijziging of vervalsing van gegevens, met inbegrip van het ongeautoriseerd invoeren van gegevens: iemand kan bevoegd toegang hebben tot bepaalde gegevens teneinde deze te raadplegen, hetgeen echter niet automatisch het recht inhoudt deze gegevens te wijzigen of nieuwe gegevens aan het bestand toe te voegen;
- f ongeoorloofde verspreiding of openbaarmaking.

Beveiligingsmaatregelen kunnen worden getroffen op het niveau van (a) fysieke beveiliging: gesloten deuren of identificatie-

pasjes, (b) organisatorische beveiliging: bevoegdhedenregeling met betrekking tot de toegang tot gegevens of (c) informatiebeveiliging: encryptie of elektronisch toezicht op ongebruikelijke activiteiten. Tot de organisatorische maatregelen wordt ook gerekend de geheimhoudingsplicht voor het gegevensverwerkend personeel. De maatregelen die voortvloeien uit dit beginsel vertonen enige overlap met de toegangs- en verstrekkingenproblematiek: wie mogen toegang hebben tot patiëntgegevens en aan wie mogen ze worden verstrekt? Daarvoor bestaan aanknopingspunten in wet- en regelgeving.

Wet bescherming persoonsgegevens

Ter implementatie van de richtlijn van de EU ter bescherming van persoonsgegevens¹ bevat artikel 13 van de Wet bescherming persoonsgegevens (WBP) de volgende beveiligingsplicht:

'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.'

Uiteraard zal eerst moeten worden vastgesteld of de WBP van toepassing is. Dat houdt in dat vast moet staan dat persoonsgegevens worden verwerkt op een geheel of gedeeltelijk geautomatiseerde wijze. Als dat het geval is, dan is de WBP van toepassing. Dan is voorts van belang dat voldoende duidelijk is wie de 'verantwoordelijke' is voor de gegevensverwerking. Dat is de persoon of organisatie die het doel en de mid-delen van de gegevensverwerking bepaalt. Een ziekenhuis zal bijvoorbeeld 'verantwoordelijke' zijn voor het ziekenhuisinformatiesysteem. Bij samenwerkingsverbanden is het soms lastiger om vast te stellen wie 'de verantwoordelijke' is. Dat is echter wel belangrijk, mede met het oog op de vraag wie verantwoordelijk is of zijn voor het treffen van voldoende beveiligingsmaatregelen.

Op grond van artikel 14 WBP geldt de beveiligingsplicht ook voor de eventuele bewerker van de persoonsgegevens. Een bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder rechtstreeks aan diens gezag te zijn onderworpen. Het gaat dan bijvoorbeeld om een bedrijf waaraan de geautomatiseerde verwerking is uitbesteed.

Wanneer een verantwoordelijke (bijvoorbeeld een ziekenhuis) gebruik maakt van de diensten van een bewerker, dan heeft deze verantwoordelijke de zorgplicht dat de bewerker de persoonsgegevens uitsluitend verwerkt in opdracht van de verantwoordelijke en dat de bewerker de beveiligingsverplichtingen nakomt die op grond van art. 13 WBP op de verantwoordelijke rusten. Daartoe zal de verantwoordelijke een bewerkersovereenkomst, bijvoorbeeld in de vorm van een Service Level Agreement (SLA) met de bewerker moeten aangaan waarin aan de bewerker deze en andere verplichtingen kunnen worden opgelegd.

Volgens minister Hoogervorst bevat NEN norm 7510 goede aanknopingspunten om concreet invulling te geven aan de plicht van art. 13 WBP tot het treffen van passende technische en organisatorische maatregelen: *'Een passend beveiligingsniveau is een vereiste om gegevens uit te wisselen. Als uitgangspunt daarvoor zal de recent vastgestelde norm voor informatiebeveiliging in de zorg gaan gelden, NEN 7510.'*²

Behalve in NEN norm 7510 kan ook in het onderzoeksrapport van het College bescherming persoonsgegevens over beveiliging van persoonsgegevens een praktisch hulpmiddel worden gevonden voor de concretisering van de algemene beveiligingsplicht.³

Wet geneeskundige behandelingsovereenkomst

In het geval persoonsgegevens over iemands gezondheid worden gebruikt in de context van een geneeskundige behandeling, zijn de regels uit het Burgerlijk Wetboek (waarin de Wet geneeskundige behandelingsovereenkomst WGBO is opgenomen) van toepassing. De WGBO kent een geheimhoudingsplicht voor hulpverleners.⁴ Die geheimhoudingsplicht is mede van belang voor de beveiliging van patiëntgegevens. Met het oog op de naleving van de geheimhoudingsplicht moet een hulpverlener er dus voor zorgen dat de

patiëntengegevens voldoende beveiligd zijn. De hoofdregel voor de omgang met patiëntgegevens vinden we in art. 7:457, eerste en tweede lid, BW: de hulpverlener (arts of instelling) moet er voor zorgen dat zonder toestemming van de patiënt geen inlichtingen over de patiënt, dan wel inzage in of afschrift van diens bescheiden aan anderen wordt verstrekt. Onder 'anderen' wordt niet verstaan: 'degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de hulpverlener, voorzover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden'. Aan deze personen mogen dus wel inlichtingen worden verstrekt zonder toestemming van de patiënt.

Een hulpverlener moet bij al zijn werkzaamheden de 'zorg van een goed hulpverlener' in acht nemen. Deze algemene norm fungeert vooral als vangnet voor gevallen waarin de wet niet duidelijk is. Naast 'de zorg van een goed hulpverlener', moet de hulpverlener ook altijd handelen in overeenstemming met de op hem rustende verantwoordelijkheid die voortvloeit uit de voor hulpverleners geldende professionele standaard (art. 7:453 BW). Hiermee wordt mede bedoeld op de normen, regels en ervaringen uit de beroepsgroep. De professionele standaard omvat het geheel van regels en normen waarmee de hulpverlener bij het uitoefenen van zijn werkzaamheden rekening behoort te houden. Algemeen wordt aangenomen dat de professionele standaard niet alleen de vaktechnische aspecten van de medische beroepsuitoefening omvat, maar ook de normen die gelden voor de relatie met de patiënt en maatschappelijke zorgvuldigheidseisen. Daartoe behoren, naast de wettelijke

normen, ook normen en regels uit de beroepsgroep, zoals de 'Gedragsregels voor artsen' en de 'Richtlijnen inzake het omgaan met medische gegevens' van de KNMG. Het is aannemelijk dat ook NEN Norm 7510 tot de professionele standaard moet worden gerekend. Anders dan de norm 'de zorg van een goed hulpverlener', die ook geldt voor zorginstellingen, geldt de norm 'professionele standaard' enkel voor de individuele hulpverlener (arts, psycholoog, verpleegkundige, etc.).

Onderdeel van de beveiliging tegen onrechtmatige verwerking, in het bijzonder de onrechtmatige toegang tot persoonsgegevens, is het regelen van de toegang tot patiëntgegevens. Daarvoor is van belang dat een toegangsregeling wordt opgesteld. De verantwoordelijke voor de gegevensverwerking dient vervolgens met een zekere regelmaat na te lopen of degenen die op basis daarvan toegang hebben, die toegangsmogelijkheid op een bepaald moment nog steeds nodig hebben. Een voorbeeld van een toegangsregeling is te vinden in het rapport over de implementatie van de WGBO.⁵

Wet BIG en Kwaliteitswet Zorginstellingen

Artikel 2 van de Kwaliteitswet zorginstellingen (KWZ) en art. 40 van de Wet beroepen in de individuele gezondheidszorg (Wet BIG) schrijven voor dat hulpverleners 'verantwoorde zorg' aan patiënten moeten aanbieden. 'Verantwoorde zorg' is zorg van inhoudelijk goed niveau die in ieder geval doeltreffend, doelmatig en patiëntgericht wordt verleend en die voldoet aan de behoefte van de patiënt.

De KWZ geldt voor instellingen die zorg verlenen. Een instelling is een organisatorisch verband waarbinnen zorg wordt verleend.



NEN 7510 geeft mij de meetlat die ik als functionaris voor de gegevensbescherming nodig heb. In combinatie met de implementatievoorschriften heb ik nu een passend toetsingskader voor onze informatievoorziening.

Luuc Posthumus, AMC



Informatiebeveiliging heeft niet zozeer te maken met instrumenten zoals virusscanners en wachtwoorden. Deze zichtbare kenmerken van beveiliging zijn afhankelijk van de stand der techniek op een bepaald moment en worden in de loop der tijd vervangen door andere technologie. Effectieve informatiebeveiliging valt of staat echter met het bewustzijn dat veilig werken zich ook moet uiten in het op verantwoorde wijze met informatie omgaan.

Hans van Vlaanderen, SIVZ

Deze omschrijving dekt in beginsel alle intra- en extramurale voorzieningen voor algemene en geestelijke gezondheidszorg, ouderenzorg en gehandicaptenzorg. Daarnaast geldt ook een samenwerkingsverband van enkele beroepsbeoefenaren in een groepspraktijk als een instelling in de zin van deze wet.

De Wet BIG bevat de pendant van de verplichting om 'verantwoorde zorg' te verlenen voor individuele hulpverleners die als 'echte solisten' kunnen worden beschouwd. Voor hen houdt deze norm in dat zij hun beroepsuitoefening in personeel en materieel opzicht zodanig dienen te organiseren dat dit leidt of redelijkerwijze moet leiden tot 'verantwoorde zorg'.

Een goede beveiliging van patiëntgegevens tegen onbevoegde kennisneming behoort ook tot de plicht om 'verantwoorde zorg' te leveren.

Slot

Beveiliging van persoonsgegevens is een al jarenlang op nationaal en internationaal niveau onbetwist privacybeginsel. Als zodanig is de algemene wettelijke verplichting tot beveiliging van persoonsgegevens te vinden in de WBP. Daarnaast valt de beveiligingsplicht ook uit andere bestaande normen in de gezondheidswetgeving af te leiden. Dat geldt bijvoorbeeld voor de WGBO (geheimhoudingsplicht, zorg van een goed hulpverlener, de professionele standaard), de KWZ en de Wet BIG (verantwoorde zorg).

Deze algemene normen bieden echter weinig houvast voor de concrete invulling van de wettelijke beveiligingsplicht in de praktijk. Die houvast kan wel worden gevonden in NEN norm

7510. De minister van VWS is dan ook terecht van mening dat NEN Norm 7510 het uitgangspunt moet zijn voor de naleving van de wettelijke beveiligingsplicht

- 1 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. *Publicatieblad* Nr. L 281 van 23/11/1995 Obz. 003-0050.
- 2 *Kamerstukken II*, 2004/05, 29 800 XVI, nr. 2, p. 134
- 3 Blarkom, G.W. van , Borking, drs. J.J., *Beveiliging van persoonsgegevens*. Registratiekamer, april 2001. Achtergrondstudies en Verkenningen 23. www.cbppweb.nl
- 4 Evenals bijvoorbeeld art. 9, lid 4, art. 12, lid 2 en art. 21, lid 2, WBP en art. 88 Wet Beroepen in de individuele gezondheidszorg (Wet BIG)
- 5 J.M. Witmer, R.P. de Roode (eindred.), *Van wet naar praktijk. Implementatie van de WGBO. Deel 4: Toegang tot patiëntengegevens*. Utrecht: KNMG juni 2004, bijlage 2. www.knmg.nl.wgbo

MEMO

Voor Zorginstellingen

Aan : Directie, hoofd automatisering, hoofd administratie
Van : de specialisten in informatisering
Betreft : inrichten van uw informatievoorziening met NEN 7510
Datum : juni 2005
Urgentie : hoog!



Geachte dames, heren,

In dit blad heeft u bijna alles kunnen lezen over NEN 7510. Dat is mooi. U kunt nu een juiste diagnose stellen over de toegevoegde waarde van deze norm voor uw organisatie. U bent op de hoogte van de beveiligings-eisen die worden gesteld aan alle partijen die medische gegevens uitwisselen. De checklists zijn ingevuld en de implementatiehandboeken liggen klaar en u heeft de informatiebehoefte van alle actoren in kaart gebracht.

Maar er is nog veel te doen, zoals:

- Het inbedden van informatiebeveiliging in uw beleid en organisatiestructuur.
- Een classificatie opstellen voor informatie, en deze koppelen aan beveiligingsniveaus.
- Een uitgebreide risicoanalyse opstellen.
- Het opstellen van beveiligingsmaatregelen op organisatorisch, technisch en procedureel vlak.
- Zorgen voor koppelingen tussen de diverse informatiesystemen, fysiek of digitaal.
- Het regelen van het onderhoud op de procedures en richtlijnen.

U heeft echter ook te maken met de invoering van de HKZ-norm, DBC's en straks de WMO. Allemaal items die ingevoerd moeten worden voor een betere aanpak van de uitvoeringspraktijk van de zorg.

Hoe nu verder?

U bent een ervaren beroepsbeoefenaar of bestuurder en u bent vanuit de praktijk reeds aan het denken over de effecten van de invoering van NEN 7510 en andere relevante thema's. Tegelijkertijd wordt duidelijk hoe moeilijk het is om deze nieuwe koers op te pakken. Innoveren kost immers veel tijd en inspanning. U wilt actief meedoen aan het vinden van de juiste koers. Hiervoor heeft u trendsetters nodig: ervaren en overtuigde professionals die u in de praktijk stap voor stap op het juiste spoor zetten.

HBS informatisering

HBS informatisering wil u daarbij ondersteunen met een gericht offensief, door het aanbieden van haar ervaren en enthousiaste informatieprofessionals. Professionals die dagelijks organisaties, (overheids)instellingen en bedrijven ondersteunen bij het creëren van een gerichte toegang tot kritische bedrijfsinformatie. Informatie die nodig is om producten en/of diensten te optimaliseren, maar ook om organisatieveranderingen te realiseren. Kwaliteit en persoonlijke dienstverlening staan in onze aanpak voorop. Kort en goed: wij leveren u de kennis, de route naar een optimale en veilige informatievoorziening.

Wat levert dat u straks op?

Een organisatie waarin het communiceren van kennis wordt gestimuleerd, waarin informatie toegankelijk en overdraagbaar wordt gemaakt en waar kennisbanken worden gecreëerd. Dit alles met als doel om met behulp van kennis en informatie concurrentievoordelen te kunnen behalen en om te voldoen aan wet- en regelgeving.

ACTIE!

Wij willen onze expertise graag vrijblijvend aan u presenteren zodat u daarin kan delen. Stuur een e-mail of bel op, een afspraak is snel gemaakt. Neem contact op met Veronique Schiefelbusch.

Vriendelijke groet,


HBS Informatisering

HBS INFORMATISERING 

Weena 290 - 3012 NJ ROTTERDAM - Tel. 010 - 282 16 35 - info@hbs-i.nl - www.hbs-i.nl



**EINDELIJK!
ONTDEK, ISOLEER EN VERWIJDER
VIRUSSEN OP DE NETWERKLAAG.**



**De eerste appliance voor uitbraakpreventie –
alleen bij Trend Micro.**

Schadelijke virussen en wormen vallen uw netwerk aan op het netwerkniveau. Bestrijd deze bedreigingen met Trend Micro™ Network VirusWall™ – de eerste en enige appliance die uitbraken op netwerkniveau voorkomt. Ontdek, isoleer en verwijder bedreigingen voordat ze schade kunnen veroorzaken. Ondersteund door onze Enterprise Protection Strategy en beveiligingsexperts blokkeert u virussen en wormen. En blijft u productief. Missie volbracht.

**Voor meer informatie:
kijk op www.trendmicro-europe.com/nvw**

