

NEN norm informatiebeveiliging als houvast bij ICT-inkoop door Huisartsen

Carinke Buiting
Jaap van der Wel

HISsen zijn handig maar voordat de software werkt, moet men soms weerbarstige problemen overwinnen. En als het dan werkt, wordt men toch met onaangename verrassingen geconfronteerd. Dan blijkt, ofschoon er iedere dag trouw een back-up is gemaakt, er niets op de tape te staan op het moment dat die nodig is voor systeemberstel. Een fout met een instelling, een vinkje ergens wel of niet, met grote gevolgen.

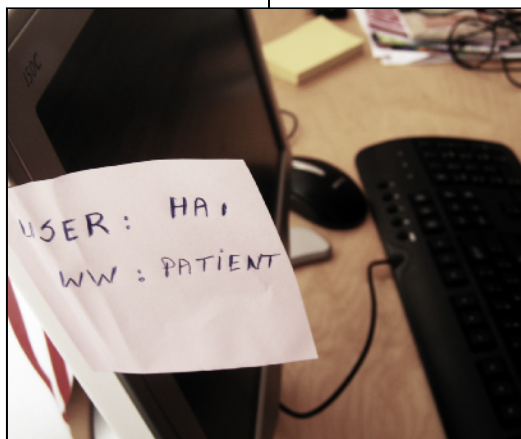
Waarom een norm

ICT is ingewikkeld, staat ver af staat van het werk van de huisarts en veroorzaakt geregeld problemen. Tal van huisartsen zijn dan ook in samenwerkingsverbanden hun ICT gaan uitbesteden. De patiëntgegevens staan dan niet meer op de praktijk-PC maar op een centrale computer die wordt beheerd door een professioneel bedrijf: een Application Service Provider (ASP). Internet levert de verbinding tussen de ASP en de huisartsen, tegen betaalbare prijzen en door encryptie zeer veilig. Zo ontstaan ook de oplossingen om tijdens waarnemingen de patiëntendossiers van collega's te kunnen inzien. Bovendien wordt ingespeeld op de toekomst als de Landelijke Verwijsindex gaat functioneren. Dan zullen medicatiegegevens rond de klok en alle zeven dagen van de week beschikbaar moeten zijn. Dat kan een ASP beter dan dat een individuele huisarts.

Tot zover de bedoeling.

In de praktijk blijken ook ASP's echter voor vervelende problemen te kunnen zorgen. Al menig huisarts heeft overleden patiënten uitgenodigd voor een griep prik omdat er iets mis was gegaan bij de overgang van het oude Elias naar een nieuw, gezamenlijk HIS. Dompers zijn ook de nog te frequent voorkomende storingen in

de beschikbaarheid van HISsen. Kortom, de overgang naar een professionele partij bleek een oplossing met haken en ogen. Overigens klagen ASP-leveranciers ook en soms terecht over hun klanten, bijvoorbeeld dat die niet altijd de cursus volgen voor het HIS-pakket maar vervolgens wel de helpdesk platbellen met triviale vragen.



De aanzet voor een oplossing van deze problemen is op 18 mei 2005 in conceptvorm wereldkundig gemaakt door het Nederlands Normalisatie-instituut (NEN) met de publicatie van de 'toetsbare voorschriften' voor de eerste en tweede lijnszorg. Voor de huisartsen betreft dit de norm NEN7511-3. Deze norm zet de maatregelen op een rijtje die nodig zijn om zeker te stellen dat patiënt- en praktijkgegevens beschikbaar, juist en vertrouwelijk zijn en blijven. Deze normen kunnen

huisartsen gebruiken bij het maken van afspraken met hun ICT-dienstverleners zoals de ASP en eventueel ook de HIS-leverancier. Het taalgebruik van deze normen verraadt de herkomst uit de ICT-hoek en is daardoor lastig toegankelijk voor menig huisarts. Toch zijn deze normen belangrijk voor de huisarts en met dit artikel maken wij u wegwijs in deze materie.

De inhoud van de norm

De norm beschrijft met bijna tweehonderd maatregelen hoe de informatiebeveiliging kan worden ingericht in de praktijk. Die maatregelen zijn ondergebracht in elf hoofdstukken, zie kader 2. De norm geeft ook een handige opstap met de suggestie om de beveiliging in stappen op te bouwen, te beginnen met tien maatregelen die weerstand bieden aan de grootste risico's. Die maatregelen zijn beschreven in bijlage B van de norm.

Kader 2 van dit artikel is op deze tien maatregelen gebaseerd. Vier maatregelen (de nummers 1, 2, 3 en 9) betreffen het invoeren van discipline om structureel over informatiebeveiliging na te denken, er een verantwoordelijke voor aan te wijzen, medewerkers te scholen en procedures regelmatig te evalueren. De overige zes hebben met HIS en computers te maken. Maatregel 4 gaat over het weren van virussen. Deze maatregel komt voort uit een groter doel: het garanderen van

correcte en veilige bediening van ICT voorzieningen, waaronder ook het in de lucht houden ervan. Maatregel 5 gaat over het maken van back-ups, en komt voort uit het grotere doel van het treffen van voorbereidingen voor geval van onderbrekingen in bedrijfsactiviteiten en het beschermen van de kritieke bedrijfsprocessen tegen de effecten van grootschalige storingen of calamiteiten. Maatregel 6 t/m 8 hebben te maken met naleving van wetten. Maatregel 6 schrijft voor om uitsluitend geregistreerde software te gebruiken. Maatregel 7 gaat over

het beveiligen van bedrijfsdocumenten: patiëntdossiers moeten beschikbaar blijven gedurende tenminste tien jaar, en dus ook leesbaar en vindbaar (dat vereist soms beschikbaar blijven van oude software!). Maatregel 8 gaat over de omgang met persoonsgegevens. Maatregel 10 heeft te maken met het reageren op beveiligingsincidenten en storingen, met als doel het beperken van de schade veroorzaakt door beveiligingsincidenten en storingen, toezicht op dergelijke incidenten en er lering uit trekken.

Invoeren van de norm in de huisartspraktijk

De praktijkhouder is verantwoordelijk voor de aanwezigheid van alle beveiliging, dit is een centraal punt van de norm. Dat sluit echter niet uit dat de huisarts de realisatie van die maatregelen kan uitbesteden. In de twee laatste kolommen van kader 2 zijn voorbeelden van uitbesteding uitgewerkt voor de tien belangrijkste maatregelen. Het kader geeft ook voorbeelden van wat niet kan worden uitbesteed. Een voorbeeld van een verplichting is het opstellen van beveiligingsbeleid. De formulering oogt wellicht wat zwaar en formeel maar eenmaal opgesteld is het beveiligingsbeleid handig op te nemen in het contract met de ASP-leverancier, gevolgd door een lijst van de maatregelen die de ASP-leverancier treft respectievelijk die de huisartsen treffen. Een dergelijke algemene motivatie als inleiding maakt het contract stevig omdat duidelijker wordt wat de bedoeling is van partijen, ook als in de lijst van maatregelen iets zou zijn vergeten. De maatregelenlijst kan eenvoudig worden gebaseerd op de normregels van de NEN7511-3. Daarmee is gelijk aan een andere verplichting voldaan: de beveiligingsmaatregelen moeten worden gespecificeerd in de contracten (art 14 WBP lid 5 en NEN-norm punt 10.8.2).

Al met al lijkt er toch wel veel werk te ontstaan voordat een contract getekend is. De voordelen van dat werk kunnen echter niet snel worden overschat want op deze manier zijn wel de verwachtingen van partijen beter op elkaar afgestemd. Zo vermindert het risico dat de huisarts ontevreden is ondanks naleven van de afgesproken servicelevels. Ook ontstaat beter inzicht welke kwaliteit de leverancier levert. Dat is een belangrijke verbetering want nog te vaak krijgen huisartsen geen beter inzicht in de kwaliteit van de ASP dan het geloof in de blauwe ogen van de accountmanager. Maar bovenal dwingt het gebruik van de norm om goed na te denken over de contractuele verhoudingen. Op dit moment worden die nog teveel bepaald door gewoonte of simpelweg de ICT-vergoeding in plaats van een rationele 'make or buy' beslissing (kader 3). De norm kan ook goede diensten bewijzen in bestaande contracten waar zaken ongeregeld zijn gebleven. Waar niets is afgesproken kan de rechter ingeval van conflict aannemen dat 'wat in de branche praktijk is' als uitgangspunt geldt. Wat dat is, maakt de norm duidelijk: die is namelijk afgeleid van algemeen geaccepteerde beveiligingsstandaarden en 35 jaar ervaring.

Wat kan mis gaan

Tot slot is wat hierboven aan de orde is gekomen geen panacee voor alle ICT-kwalen. Hierna volgen enkele notoire problemen die nog reesteren.
*Even snel een verbetering aanbrenge*n Niet doen! De NEN norm formuleert restricties op wijzingen in applicaties (punt 12.5.3). Deze eis is zo geformuleerd omdat de ervaring leert dat 'eventjes een kleine wijziging aanbrenge' te vaak resulteert in grote storingen. Zeker in het geval van die leverancier die ongeveer 90 wijzigingen per jaar uitleverde.
Inpassing van het HIS in een centrale server omgeving. Tal van HISsen zijn gemaakt voor lokale PC's maar moeten functioneren op grote centrale servers en dat vermindert de systeemstabiliteit. Een voorbeeld is een HIS die

de printuitvoer nog naar een printerpoort stuurt want dan moet de ASP-leverancier trucjes uithalen om die uitvoer van de centrale server op de PC van de huisarts te krijgen. En trucjes gaan gewoonlijk ten koste van de systeemstabiliteit.
Verplichtingen huisarts. Goede beveiliging vereist inspanningen van leveranciers en huisarts sámen. De huisarts die bijvoorbeeld in zijn HAP de ICT coördineert, moet dat aan zijn collega's duidelijk maken. In de meest volledige ASP-opzet richt de huisarts zijn eigen PC niet meer in. Of het daar op korte termijn van komt valt te betwijfelen maar de huisarts die met een wat oudere PC met Windows '98 of millennium wil doorwerken, moet dan wel afgesloten blijven van internet en e-mail ont-

vangen via een professionele bescherming van de ASP-leverancier. Wil men wel internet, dan zit men vast aan een goede firewall op iedere PC (een betere dan die van Windows XP), een actuele versie van het operating system (2000, XP, Apple), goed bijhouden van updates, actuele viruschecker, uitsluitend software voor de praktijk op de PC, nooit downloaden en installeren van software van het internet, tenzij het om algemeen erkende programma's gaat, spyware checker (een betere dan gratis van het internet!), etc. Natuurlijk nooit internetgames op de praktijkcomputer. Ook is het aan te raden de tekstverwerkerbestanden netjes te back-uppen! Voor alle PC's van de praktijk. We zijn dan weer terug bij het begin: de huisarts als technisch systeembeheerder, alsof hij niet al druk genoeg is!

Uit elkaar gaan. Als de huisarts en zijn ASP leverancier niet meer verder willen, zijn er enkele problemen op te lossen. Niet zelden zijn partijen dan gebrouilleerd maar moet de leverancier toch nog klusjes uitvoeren zoals meewerken aan de gegevensconversie nodig om over te stappen naar een andere leverancier. Bij het afsluiten van contracten denkt men zelden aan het uit elkaar gaan. Toch is het verstandig om in het contract een exitregeling op te nemen. Dat voorkomt chicanes op het moment dat partijen uit elkaar willen.

C.I.C.M. Buiting (buiting@euprax.nl) is managing partner bij Euprax en stafmedewerker automatisering bij het Nederlands Huisartsen Genootschap.

Mr. drs. J.A. van der Wel (jvdwel@comfort-ia.nl) is managing partner van Comfort-IA (www.comfort-ia.nl) en lid van de normcommissie voor Informatiebeveiliging in de zorg van het Nederlands Normalisatie-instituut.

Kader 1 Samenvatting van de inhoud van de norm NEN7511 – 3

De norm is verdeeld in een elftal hoofdstukken die tezamen alle beveiligingsmaatregelen beschrijven:

H5 Informatiebeveiligingsbeleid geeft de maatregelen om informatiebeveiliging structureel aan te pakken: wat doen we aan informatiebeveiliging en hoe controleren we of het werkt. Samen met de evaluatie van de geregistreerde beveiligingsincidenten (H15) vormt dit de as van de informatiebeveiliging.

H6 organiseren van informatiebeveiliging heeft als belangrijkste maatregel het aanwijzen van de verantwoordelijke, tevens aanspreekpunt rond beveiligingszaken.

H7 beheer van middelen voor de informatievoorziening somt de maatregelen op die nodig zijn om overzicht te houden over het geheel van computers, programmatuur, bestanden alsmede de kwetsbaarheid en het belang van elk onderdeel.

H8 beveiligingseisen ten aanzien van personeel geeft de maatregelen voor het verminderen van de risico's van menselijke fouten, diefstal, fraude of misbruik van voorzieningen.

H9 fysieke beveiliging en beveiliging van de omgeving geeft alle maatregelen voor het voorkomen van ongeautoriseerde toegang tot, schade aan of verstoring van de gebouwen en informatie van de organisatie.

H10 operationeel beheer van informatie en communicatievoorzieningen geeft de maatregelen voor het garanderen van een correcte en veilige bediening van IT voorzieningen.

H11 toegangsbeveiliging regelt de toegang tot informatie.

H12 aanschaf, ontwikkeling en onderhoud van systemen waarborgt dat beveiliging wordt ingebouwd in informatiesystemen.

H13 continuïteitsbeheer geeft maatregelen voor het treffen van voorbereidingen voor geval van onderbrekingen in bedrijfsactiviteiten en het beschermen van de kritieke bedrijfsprocessen tegen de effecten van grootschalige storingen of calamiteiten.

H14 naleving beschrijft het voorkómen van schending van straf- of civielrechtelijke wetgeving, statutaire, wettelijke of contractuele verplichtingen of beveiligingseisen.

H15 (reageren op) beveiligingsincidenten (en storingen) geeft maatregelen die de schade moeten beperken die wordt veroorzaakt door beveiligingsincidenten en storingen, en voor toezicht op dergelijke incidenten. Net zo belangrijk is er lering uit te trekken. Zoals gezegd dient de registratie van de incidenten als input voor evaluatie en bijstelling van het beleid.

De conceptversie van de norm kan worden aangevraagd bij Shirin Golyardi [Shirin.golyardi@nen.nl] van het Nederlands Normalisatie-Instituut. De definitieve versie komt waarschijnlijk uit op 17 november en kan worden gedownload vanaf de website www.nen.nl

Kader 2 Mogelijkheden van zelf doen of laten doen bij de eerste 10 maatregelen¹

De eerste klap is een daalder waard (in modernere termen: de 20/80 regel). Met over de hele breedte een aantal relatief eenvoudige maatregelen is al heel wat gevaar te weren. De eerste tien maatregelen moeten worden gezien als uitgangspunt voor het ontwikkelen van richtlijnen specifiek toegesneden op uw organisatie. Het kan zijn dat voor uw praktijk een elfde en een twaalfde maatregel nodig zijn. Overigens zijn deze maatregelen een eerste begin, laat het daar niet bij.

Wat de norm vraagt (maatregel 1 t/m 10)	Voorbeelden van aanpak	Zelf doen of ASP laten doen?
1 Beleidsdocument voor informatiebeveiliging	Gebruik NEN of andere voorbeelden en vul in voor de eigen situatie. Analyseer jaarlijks de rapportage van de beveiligingsincidenten van maatregel 10 Bundel de ervaring van huisartsen met hun gezamenlijke leverancier of binnen een waarneminggroep. Selecteer de actiepunten voor het komend jaar.	Zelf doen
2 Toewijzing en vastlegging van verantwoordelijkheden voor informatiebeveiliging	Wijs een verantwoordelijke aan binnen de praktijk. Bedenk welke maatregelen u gezamenlijk met andere kunt regelen, of kunt beleggen bij uw (ASP-)leverancier. Bewaak zelf de contracten.	Zelf doen
3 Bewustwording, opleiding en training voor informatiebeveiliging	Draag het informatiebeveiligingsbeleid uit. Ga na welke opleidingen er zijn voor het eigen systeem wat betreft back-up procedures, beveiliging tegen diefstal e.d. Heeft iedereen die cursussen gevolgd?	1) Zelf doen, wel eisen stellen aan de leverancier dat deze een adequate opleiding heeft (duidelijk, praktisch, terzake) 2) Afspraken maken binnen de huisartsengroep. Gedisciplineerd volgen v opleiding stelt ook in staat om professionele eisen te stellen aan de leverancier.
4 Maatregelen tegen kwaadaardige programmatuur	Virusscanner, firewall, wie neemt dit voor zijn rekening? Bij elke nieuwe component aan software en (mobiele) hardware zijn er nieuwe risico's.	Praktijk nog vaak: zelf doen (vereist ICT-kennis!). Professional: ASP laten doen.
5 Ontwikkelen en implementeren van continuïteitsvoorzieningen en –plannen	Welke afspraken zijn er met de ASP leverancier? Heeft u zich laten rondleiden langs de apparatuur en voor de hand liggende vragen gesteld?	Zelf doen: backups maken (gaat niet altijd goed!!!) Beter: uitbesteden aan ASP Uitwijk: contractueel regelen, met sancties voor leverancier.
6 Intellectueel eigendom	Worden alle plekken van kantoorautomatisering afgerekend? Worden licenties van tabellen ed afgerekend?	Zelf doen en uitbesteden zijn mogelijk.
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 mee geconverteerd, zo niet, blijven de gegevens uit het oude systeem gemakkelijk beschikbaar de komende jaren?	Papier: zelf doen Automatisering: afspraken met ASP maken over 'schoningsprocedures' Conversie: laten doen Resultaten goed controleren (proefconversies uitvoeren, pas als deze foutloos zijn na grondige controle, overgaan op het nieuwe systeem)
8 Bescherming van persoonsgegevens		Zelf doen. Selecteren systeem met goede mogelijkheden voor toegangsbeveiliging.
9 Naleving beveiligingsbeleid	Wordt de naleving af en toe geëvalueerd en onafhankelijk gecontroleerd? Geeft u het goede voorbeeld?	Kan zelf, beter is peer-review binnen de beroepsgroep onder begeleiding van een beveiligingsprofessional.
10 Het rapporteren van beveiligingsincidenten	Leg problemen overzichtelijk vast met tijdstip, apparaat, software, probleem, schade, oplossing, persoon (spreadsheet, nog mooier: storingsadministratie van de ASP leverancier)	Storingsadministratie bijhouden: zelf doen

¹ In de definitieve versie van de NEN-norm zal aan de gepresenteerde 10 maatregelen nog een tweetal worden toegevoegd.

Kader 3 Make or buy?

De praktijk kent talloze varianten van afspraken tussen huisartsen en hun ICT-leveranciers. Vaak is sprake van een traject van groeien, kleerscheuren oplopen en dan maar weer verder proberen. Kort door de bocht kun je de bestaande contractverhoudingen met ICT-leveranciers in drie categorieën onderverdelen:

1. *Do it yourself*. De huisarts selecteert zelf zijn HIS, koopt computers, printers e.d. bij een ander (vaak op basis van advies van de softwareleverancier) en laat de boel aanleggen door nog weer een ander. Bij storingen zijn er meerdere kandidaten die veroorzakers kunnen zijn en niet zelden verwijzen die naar elkaar, met overtuigend klinkende maar voor de huisarts niet op legitimiteit te beoordelen argumenten. Bij deze oplossing moet de huisarts zelf veel beveiligen wat veel werk en kennis vereist.
2. *Tussenvorm*. Ontstaat in de praktijk vaak als een huisartspraktijk van de ICT-rompslomp af wil en een partij aantrekt die het beheer gaat uitvoeren zoals hiervoor beschreven. Die partij zorgt dan ook voor de contacten naar weer andere leveranciers: bijvoorbeeld KPN voor de internetverbinding, Dell of HP voor de centrale server en dergelijke. De huisarts blijft in deze vorm ook nog zaken zelf doen, bijvoorbeeld het beheer van zijn lokale computers of overleg met de leverancier van het HIS. De huisarts kan nog te maken krijgen met gekibbel over ICT-problemen maar in beperktere mate dan bij punt 1.
3. *ASP*: één leverancier neemt alle verantwoordelijkheid voor alle ICT aspecten, ook de hardware bij de huisarts, ook de contacten met de HIS leverancier. Alle ICT-problemen zijn nu belegd bij een partij die er verstand van heeft. Het ligt voor de hand dat in de laatste situatie de uitbestedende partij niet ontslagen is van alle verantwoordelijkheid. Ook in de wet is deze regel te vinden, zo stelt artikel 14 van de Wet Bescherming Persoonsgegevens 'Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke ziet toe op de naleving van die maatregelen.'

Kader 4 Afkortingen

ASP = Application Service Provider

Concept waarbij een huisarts het HIS en vaak ook de hardware voor een vast bedrag per maand least van een provider. Het HIS staat dan bij de provider, de huisarts heeft op de werkplek een browser. Communicatie met andere modules of systemen – denk aan controle verzekering, medicatiebewaking, wachtlijsten, postbusdiensten – regelt de provider.

SLA = Service Level Agreement

Overeenkomst tussen opdrachtgever (huisarts) en provider die in een zekere mate van detail aangeeft welke werkzaamheden de provider in opdracht van de huisarts verricht, en wanneer, hoe en waar deze werkzaamheden worden uitgevoerd (naar Gartner 1996).