LESSEN UIT MISLUKKINGEN

Veilige informatie-uitwisseling zonder de zorg te compliceren

Zorgverleners moeten gegevens van patiënten gemakkelijk kunnen uitwisselen. Informatie moet echter wel worden beveiligd en privacy van patiënten gegarandeerd. Als beveiliging en privacy aan de zorgsector wordt opgelegd met regels en voorschriften, leidt dit slechts tot bureaucratische ballast. Enkele vuistregels bieden perspectief.

Jaap van der Wel

Voor de zorgsector is de ervaring van de overheid met informatiebeveiliging interessant. De overheid wilde de informatiebeveiliging verbeteren met een voorschrift, het 'Voorschrift Informatiebeveiliging Rijksdienst' (VIR) van 1994. Het resultaat viel tegen. Onder druk van het controleorgaan voor de rijksoverheid, de Algemene Rekenkamer, vroegen management en politiek om stipte toepassing. Dat leidde tot veel beveiligingsanalyses, veel documentatiewerk, weerstand bij medewerkers en een alom verguisd VIR. Slechte reclame voor informatiebeveiliging.

Deze bureaucratisering kan ook in de zorgsector toeslaan; alle ingrediënten zijn aanwezig. Er is een aanleiding: de snel in belang groeiende computernetwerken vereisen meer aandacht voor informatiebeveiliging en privacy. Een controleorgaan is er ook: de Inspectie voor de Gezondheidszorg. Inmiddels is er ook een begin van een voorschrift: de norm voor informatiebeveiliging in de zorg.

NUTTIG EN NODIG

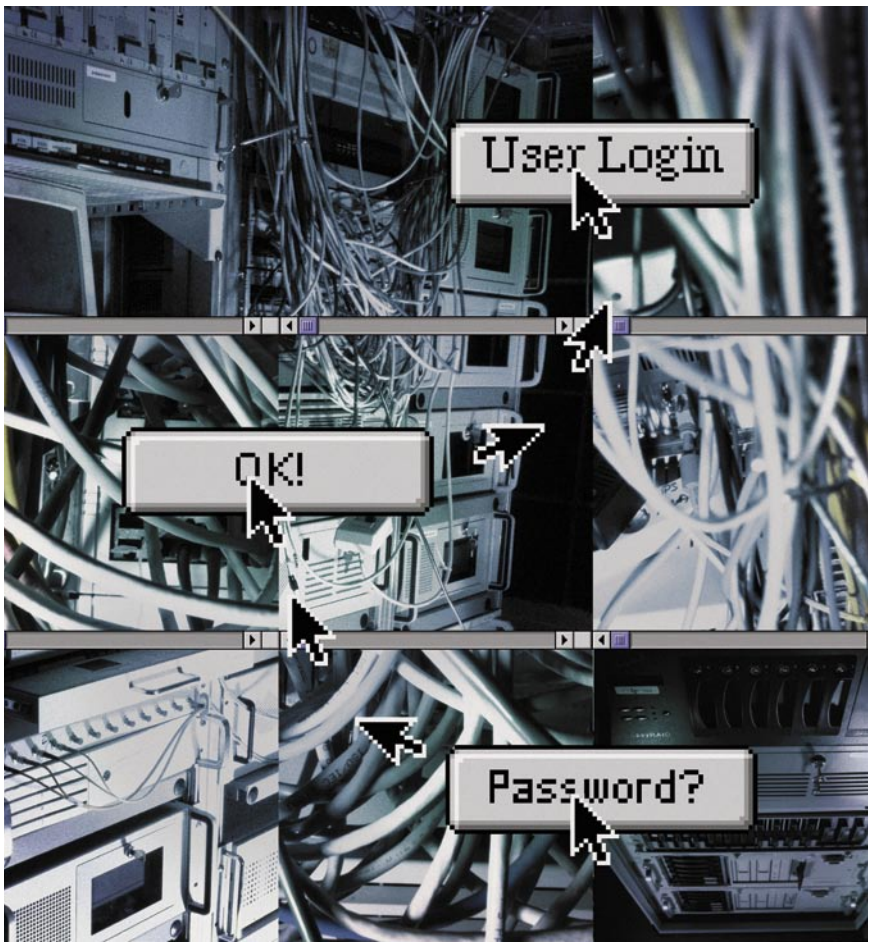
Kan het ook anders? Ja, maar niet door het afschaffen van voorschriften want die zijn nuttig en nodig. Voorschriften blijken echter ongeschikt om de revolutie van informatievoorziening in goede banen te leiden, ze zijn slechts geschikt om toezichthouders te ondersteunen bij het opsporen van uitwassen. Daarnaast kunnen organisaties door aan een voorschrift te voldoen, aantonen dat patiëntgegevens bij hen in goede handen zijn. Ook voor softwarebouwers is een voorschrift nuttig; zij kunnen namelijk de functionaliteit van software, bijvoorbeeld die voor het beheersen van de gegevenstoegang, daarop afstemmen.

Voorschriften zijn echter niet meer dan een hulpmiddel. Bepalend of fatsoenlijk met informatie wordt omgegaan, is de professionaliteit van artsen en >>

Voorschriften nuttig bij het opsporen van uitwassen

NORM VOOR INFORMATIEBEVEILIGING

De Nederlandse Norm voor Informatiebeveiliging in de Zorg[1] definieert informatiebeveiliging als 'een stelsel van maatregelen om verstoringen in de zorgvuldige en doelmatige informatievoorziening te voorkomen en eventuele schade als gevolg van desondanks optredende verstoringen te beperken'. Het doel is 'om patiënten het gewenste niveau van dienstverlening te kunnen bieden' en 'om de privacy van de patiënt, de zorgverlener en van de zorginstelling te beschermen.'
De verdere uitwerking is een checklist die beschrijft 'welke soorten maatregelen de leiding binnen organisaties moet treffen'. Bij de huidige norm is al een 'implementatietool' beschikbaar die voor verschillende typen zorgorganisaties een handreiking geeft voor het gebruik. Kleine organisaties zoals HAP's en individuele huisartsen hebben nu eenmaal een andere manier van administreren en dossiergebruik dan grote organisaties zoals een ziekenhuis met duizenden medewerkers. En de manier waarop huisartsen bij weekenddiensten gegevens uitwisselen is bijvoorbeeld in de psychiatrie ondenkbaar. ■



BEELD: IMAGE SOURCE

<< verpleegkundigen en de praktische integratie van de administratie in het dagelijkse werk. En juist hier loopt de zorgsector bepaald niet voorop met vernieuwingen. De academische ziekenhuizen bijvoorbeeld zouden op basis van de bewaartermijn van de Wet inzake de geneeskundige behandelingsovereenkomst (WGBO), veel op hun kilometers archiefplank kunnen besparen. De verslagen van de nachtzuster bijvoorbeeld zijn na dertig jaar nutteloos maar veroorzaken daar wel steeds terugkerende kosten, voor opslag, het zoeken naar nuttige informatie, verhuizen, scannen van patiëntendossiers om die on line te ontsluiten et cetera. De oplossing begint bij artsen die met behulp van richtlijnen voor dossiervorming aangeven welke informatie kan worden afgesplitst van de rest van een dossier om langdurig te worden bewaard.

SUCCES

Het professioneel medisch handelen verandert door de toenemende invloed van ICT. Voor het succes van die verandering is de norm voor informatiebeveiliging in de zorg belangrijk, evenals de handreikingen van de beroepsorganisaties.[2] Bepalend voor het succes zijn deze echter niet. Bepalend is de mate waarin zorgorganisaties informatiebeveiliging en privacy kunnen integreren in medische kwaliteitszorg, ook omdat zij een zwaar stempel drukken op de opleiding van artsen en verpleegkundigen.

Voor deze organisaties heb ik uit mijn ervaring in ICT-, kwaliteitszorg- en informatiebeveiligingsprojecten, zes vuistregels gedestilleerd om effectief het niveau van informatiebeveiliging te verbeteren.

1. Liever concreet dan abstract
Een organisatie kan gewoonlijk meer leren van concrete ervaringen en klachten van patiënten dan van risicoanalyses. Risicoanalyses zijn aanvullend wel nuttig. Ook verantwoorden aan een arts of patiënt wie er inzage heeft gehad in dossiers - door *logging* is dit goed te realiseren - levert een organisatie uiteindelijk meer mogelijkheden om iets te leren van de werkelijkheid dan het stipt opvolgen van voorschriften. Bovendien verschaft het patiënten meer vertrouwen dan abstracte certificaten die zijn behaald na een toets van administratieve processen. Als aanvulling zijn certificaten wel nuttig, zelfs noodzakelijk.

2. Begin met de enthousiastelingen
Niet iedere arts of verpleegkundige staat te trappelen om naar de manier van werken te kijken. Begin daarom met de enthousiastelingen. Na verloop van tijd zal blijken dat klachten en kosten afnemen en dat de medische kwaliteit toeneemt. Anderen kunnen dan niet meer achterblijven.

3. Regel gelijk goed, later verbeteren is duur
Beveiligingsmaatregelen toevoegen aan een bestaande administratie is veel werk; ze vooraf meenemen in het ontwerp van die administratie is aanzienlijk goedko-

STERKE EN ZWAKKE KANTEN

De Nederlandse Norm voor Informatiebeveiliging in de Zorg is afgeleid uit de internationaal geaccepteerde 'Code voor Informatie-beveiliging', waarvan de terminologie is vertaald naar die van de zorg. Deze aanpak van de normcommissie had zowel een voordeel als een nadeel. Het voordeel was dat het brede draagvlak van de Code voor Informatiebeveiliging ook doorwerkte naar de norm voor informatiebeveiliging in de zorg. Nadeel is dat de omissies van het uitgangspunt[3] daarmee werden geïmporteerd in het zorgdomein. Zo bevat de norm voor ieder staforgaan (HRM-afdeling, ICT-afdeling, huishoudelijke dienst) wel één of meerdere hoofdstukken. Maar artsen en verplegend personeel, hebben nog geen eigen hoofdstuk en moeten hun punten maar bij elkaar sprokkelen. Een puntje voor een volgende versie? ■

per. Het is bijvoorbeeld bij ziekenhuisafdelingen met sterk veranderlijke taken, zoals heelkunde, in de hectiek niet altijd gemakkelijk om papieren patiëntendossiers voortdurend volledig bij te houden. ICT moet ook daarvoor een oplossing bieden. Een systeem dat slechts papieren gegevens automatiseert maar extra handelingen vergt doordat artsen op iedere locatie weer opnieuw moeten inloggen, is contraproductief. Zo'n systeem leidt ertoe dat artsen vaker vergeten iets te registreren (lagere medische kwaliteit) of tot hoge kosten om het systeem te herbouwen.

4. Stel niet de procedures maar de mensen centraal
Een sfeer waarin fouten bespreekbaar zijn, draagt meer bij dan een formele procedure voor het rapporteren van beveiligingsincidenten. Een incident is vaak terug te voeren op fouten van collega's. In een open sfeer komen fouten gemakkelijker aan de orde dan in een repressieve sfeer.

5. Laat belangentegenstellingen buiten de discussies, ga voor het resultaat
Belangenstrijd leidt tot patstellingen. Zo pleiten verzekeraars wel voor nauwkeuriger patiëntenidentificatie om zorgfraude te bestrijden. Met alleen dat argument wordt de zorg het toneel van de verzekeraars en resteert de zorginstellingen een figurantenrol. Overigens kan verzekeringsfraude ook tot fouten in patiëntendossiers leiden. Fouten krijgen vaker medische gevolgen naarmate artsen zich door de toenemende rol van zorgnetwerken meer op patiëntengegevens van elders gaan baseren. Dat raakt rechtstreeks aan de kwaliteit van zorg. Op den duur is een betere patiëntenidentificatie dan ook onvermijdelijk.

Informatiebeveiliging en privacy betekent de eed van Hippocrates in praktijk brengen

6. Medici en verplegend personeel bepalen de prioriteiten, de staven (administratie, juristen en ICT) motiveren de kosten, de directie beslist
Nog te vaak worden beveiligingsprogramma's vooral gemotiveerd met financiële, juridische (privacy) of automatiseringsmotieven. Zo zijn het gewoonlijk de automatiseerders, niet de artsen, die beginnen over de briefjes met de toegangscodes die geplakt zijn aan de beeldschermen. Het zijn echter de artsen die belang en kosten moeten afwegen tegen alternatieven. Informatiebeveiliging en privacy betekent namelijk de eed van Hippocrates in praktijk brengen in deze wereld van ICT en internet. Daarvoor is het nodig om procedures te moderniseren en, daarop aansluitend, medewerkers op te voeden. Dat begint met concreet omgaan met problemen waarop alle andere punten volgen die ik hiervoor heb genoemd. ■

mr. drs. J.A. van der Wel,
directeur Comfort-IA, lid van de NEN-normcommissie voor informatiebeveiliging in de zorg

Correspondentieadres: jvdwel@comfort-ia.nl.

Het artikel is geschreven op persoonlijke titel.

SAMENVATTING

- *Het belang van ICT in de zorg groeit. Om de ruimere mogelijkheden met informatievoorziening in goede banen te leiden is de inzet van beveiligings- en privacydeskundigen nodig.*
- *De zorg kan te maken krijgen met meer dwingende voorschriften en uitgebreide verantwoordingsverplichtingen.*
- *Door de groeiende uitwisseling van patiëntgegevens is meer aandacht nodig voor risicobestrijding en privacybescherming.*
- *Voor een gestroomlijnde en effectieve beveiliging is het nodig dat medici en zorgdirecties de regie houden over het verbeteren van informatiebeveiliging en privacy. Informatiebeveiliging en privacy zijn namelijk onderdeel van medische kwaliteitszorg.*

Kijk voor meer informatie over het implementatieprogramma WGBO op onze website. Ga naar ***www.medischcontact.nl/dezeweek*** *en bij dit artikel vindt u de desbetreffende informatie.*

Referenties
1. *De norm voor Informatiebeveiliging in de Zorg is te bestellen op de website van het NEN,* ***www.nen.nl****.* ***2.*** *Van wet naar praktijk: Implementatieprogramma WGBO van de KNMG,* ***www.knmg/wgbo****.* ***3.*** *Informatiebeveiliging 4/2001, Ontstijgt Informatie-beveiliging de techniek? J.A. van der Wel.*

TOEKOMSTIGE ONTWIKKELINGEN

Het ministerie van VWS wil het 'implementatietool' bij de norm ombouwen naar een voorschrift per type zorgorganisatie of clusters van zorgorganisaties. Het is de bedoeling van het Nederlands Normalisatie Instituut dat dit gebeurt in nauwe samenwerking met de koepelorganisaties. In deze stap ligt een uitgelezen kans voor de zorgsector om te komen tot een praktische implementatie van de norm. Als deze aanpak slaagt, neemt de kans toe dat het geschetste bureaucratiseringsproblee m wordt vermeden. ■