E-diagnose, e-consulten, gezondheidsportalen en allerlei vormen van gezondheidszorg via mobiele telefonie nemen explosief toe. Deze toename vereist veel meer aandacht voor de beveiliging van persoonsgegevens. Er bestaan verschillende normen voor de digitale vastlegging van patiëntgegevens. Maar zijn die voldoende?

door: NATASCHA VAN DUUREN **beeld:** ISTOCKPHOTO

Voor IT-managers in de zorg is een adequaat beveiligingsniveau prioriteit nummer één

E-HEALTH DWINGT BEVEILIGING AF

Het is onontkoombaar dat e-health de komende jaren een hoge vlucht neemt. In haar Kamerbrief van 7 juni jl. onderstreept minister Schippers het belang van een brede toepassing van IT in de zorg. Dit onder meer met het oog op de kostenstijging in de zorg en het dreigend personeelstekort. De minister gebruikt in haar brief de definitie van e-health die de Raad voor Volksgezondheid en Zorg (RVZ) in haar studie 'Inzicht in e-health' (2002) heeft gehanteerd: 'Het gebruik van ICT om gezondheid en gezondheidszorg te ondersteunen of te verbeteren.' Daarbij valt te denken aan een EPD, maar ook aan oplossingen voor het maken van online-afspraken, toepassingen op het gebied van e-diagnose, e-consulten, gezondheidsportalen et cetera. Onder de definitie vallen ook vormen van gezondheidszorg via mobiele telefonie, zoals apps die patiënten digitaal ondersteunen bij het managen van hun eigen zorg (zogenaamde 'm-health-toepassingen').

De Geestelijke Gezondheidszorg (GGZ) is koploper in het gebruik van e-health-toepassingen, onder meer door het aanbieden van (anonieme) e-mental-healthdiensten. Door de opkomst van e-health wordt de noodzaak van adequate beveiliging steeds groter. Het zorg dragen voor een adequaat beveiligingsniveau om het beroepsgeheim van artsen te kunnen garanderen, zal de komende jaren dan ook prioriteit nummer één zijn voor IT-managers in de zorg. De wet- en regelgeving houdt helaas geen gelijke tred met de vlucht van e-health. De afgelopen periode zijn diverse initiatieven bovendien gestagneerd door de val van het kabinet. Nu de verkiezingen voorbij zijn, is het aan de politiek de zaken weer op te pakken.

Normen

Alle wet- en regelgeving die voor een zorgproces van toepassing is, geldt ook voor e-health als onderdeel van dat zorgproces. Verantwoordelijken in de zorg dienen op grond van artikel 12 Wbp 'passende technische en organisatorische maatregelen' te nemen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.

Er zijn verschillende normen en criteria voor digitale vastlegging en uitwisseling van patiëntgegevens, waaronder NEN-normen (zie kader). NEN-normen dienen echter beschouwd te worden als een set 'best practices'. Recentelijk heeft de Hoge Raad bevestigd dat NEN-normen geen algemeen bindende voorschriften zijn, maar de betekenis hebben van een wettelijk vermoeden: wie aan de normalisatienorm voldoet, wordt geacht aan de wettelijke prestatie-eisen te hebben voldaan. De vraag is echter of hiermee – gezien het vertrouwelijke karakter van medische gegevens – voldoende tegemoet wordt gekomen aan de hoge eisen die aan informatiebeveiliging in de zorg worden gesteld. Het staat de verantwoordelijken immers vrij om te bepalen hoe ver zij willen gaan met de invoering en handhaving van deze maatregelen. Dit stelt IT-managers in de zorg voor lastige keuzes. De normen zijn immers generiek. IT-managers dienen deze (generieke) norm toe te passen, terwijl er grote diversiteit bestaat in de aard en de omvang van zorginstellingen. Dit betekent dat de IT-manager keuzes zal moeten maken om te komen tot een geslaagde beveiliging in zijn (specifieke) organisatie. Bovendien plaatst de eis dat de beveiligingsmaatregelen 'proportioneel' dienen te zijn, IT-managers voor moeilijke afwegingen. Welke verhouding tussen de mogelijke risico's en schade en de kosten van beveiligingsmaatregelen kan als proportioneel worden aangemerkt? De grote tekorten in de zorg maken deze afweging er niet makkelijker op. Last but not least, is commitment van de bestuurder noodzakelijk. Ook dit blijkt in de praktijk een uitdaging te zijn voor IT-managers. Een bijkomende complexiteit is dat binnen de zorg veel IT wordt uitbesteed en vaak een complexe keten vormt. De verwachting is dat deze trend zich verder doorzet. Op grond van artikel 14 van de Wbp heeft de zorginstelling de verplichting erop toe te zien dat de leverancier voldoende waarborgen biedt voor beveiliging.

Worsteling

In 2008 hebben het College Bescherming Persoonsgegevens (CBP) en de Inspectie voor de Gezondheidszorg (IGZ) onderzoek gedaan naar informatiebeveiliging in ziekenhuizen. Informatiebeveiliging bleek nog te weinig omgezet naar uitgewerkt beleid; te veel was 'in de praktijk' geregeld. Bovendien bleek bij medewerkers het bewustzijn van het belang van informatiebeveiliging te ontbreken.

Dit betekent dat er nog veel werk aan de winkel is. Opmerkelijk is dan ook dat de minister in haar wetsvoorstel voor de 'Wet Cliëntenrechten Zorg' (Wcz), aan informatiebeveiliging weinig aandacht heeft besteed. De minister wil dat alle patiënten op basis van deze nieuwe wet de mogelijkheid hebben hun eigen medisch dossier elektronisch in te zien. Het is dan uiteraard van essentieel belang dat voor alle zorgverleners helder is waaraan informatiebeveiliging moet voldoen en dat dit vervolgens wordt gehandhaafd. Vastgesteld dient te kunnen worden dat de informatie betrouwbaar is en wie informatie heeft toegevoegd.

Door de worsteling van de overheid om beveiliging juridisch handen en voeten te geven en de stagnatie die dit tot gevolg heeft, zal informatiebeveiliging voorlopig door IT-managers in de zorg langs contractuele weg moeten worden geregeld, bijvoorbeeld door beveiligingsnormen onderdeel te laten zijn van de SLA. Dit blijkt echter in de praktijk niet altijd even makkelijk. Naast onduidelijkheid over het vereiste beveiligingsniveau, brengt cloudcomputing een extra complexiteit met zich mee. Bij cloudcomputing kunnen veel partijen bij de verwerking van persoonsgegevens betrokken zijn en is vaak onduidelijkheid of de cloudserviceprovider naast de cloudcustomer zich kwalificeert als (mede) verantwoordelijke of als bewerker. De verschillende rollen en verantwoordelijkheden bij beveiliging dienen contractueel nauwkeurig te worden afgebakend.

De praktijk leert dat, terwijl beveiliging van de gegevens tegen verlies of schending van vertrouwelijkheid een van de grootste risico's van cloudcomputing is, beveiligingsverplichtingen contractueel vaak grotendeels worden doorgeschoven naar de cloudcustomers. Voorts worden door cloudserviceproviders, bij gebrek aan specifieke wet- en regelgeving, naar eigen goeddunken bepaalde normen en standaarden gehanteerd.

Audits

Gebruikers trachten dikwijls comfort te zoeken bij een contractueel overeengekomen recht een beveiligingsaudit te laten uitvoeren. Praktisch probleem hierbij is dat de locatie van de gegevens niet altijd met zekerheid is vast te stellen. Voor deze problematiek dient bij het opstellen van de betreffende contracten een oplossing te worden gezocht. Een alternatief is een clausule op basis waarvan de leverancier de verplichting heeft zelf periodiek beveiligingsaudits door een onafhankelijke partij te laten uitvoeren. Er kan echter frictie ontstaan indien elke ketenpartner een eigen (deel)audit laat uitvoeren met eigen normenkaders.

Verdere ontwikkeling van regelgeving omtrent informatiebeveiliging lijkt dan ook noodzakelijk. Op die manier kan door de overheid de gewenste duidelijkheid worden geschapen over de eisen die aan informatiebeveiliging in de zorg dienen te worden gesteld. De ontwikkelingen in de praktijk zijn door de regelgever echter niet bij te benen. Normen met aandacht voor kaderstelling dienen de betrokken partijen dan ook de ruimte te geven om in de praktijk praktische maatregelen te treffen. Het is dan wel zaak dat aan de hand van audits of zelfassessments en bijpassende rapportages de normen toetsbaar zijn. Bij gebrek daaraan is het vooralsnog aan de (private) partijen om de risico's zoveel mogelijk in de contractonderhandelingen te ondervangen en contractueel in te perken. «

NORMEN EN STANDAARDEN

Er zijn verschillende normen en criteria voor digitale vastlegging en uitwisseling van patiëntgegevens, waaronder de nationale NEN-norm 7510 en de diverse uitwerkingen van deze norm. De Europese norm EN 13606 speelt een rol in het uitwisselingsdomein. Internationaal zal de ISO 13131 voor e-health en telemedicine van kracht worden. Deze zal inhoudelijk voor een groot deel gelijk zijn aan de NEN 7510.

Reactie minister

Minister Schippers heeft op 7 juni jl. een Kamerbrief verzonden waarin zij haar visie geeft op het gebruik van e-health in de zorg. In deze brief reageert zij onder meer op de 'Nationale implementatieagenda e-health' (NIA): 'Uiteraard dienen portalen en apps te voldoen aan strenge eisen op het gebied van veiligheid, kwaliteit en patiëntgerichtheid.'.
De minister pleit voor zorgbrede normen en standaarden: over welke informatie nodig is, op welke manier deze wordt opgeslagen, in welke terminologie en hoe uitwisseling van deze informatie technisch kan plaatsvinden. Het door het ministerie van VWS beoogde nationale Kwaliteitsinstituut zal een toetsingskader ontwikkelen dat eisen stelt aan de ontwikkeling van deze standaarden. Het instituut zal hierbij worden ondersteund door Nictiz. Volgens de minister gaat het er niet (alleen) om de standaarden te definiëren, te ontwikkelen, te ontsluiten en te accepteren, maar ook om een ondersteunende rol te spelen bij de implementatie van deze standaarden. Speciale aandacht zal uitgaan naar het voorkomen dat zorgverzekeraars toegang hebben tot elektronische uitwisselingssystemen. De minister heeft aangekondigd dat zij een forse sanctie zal opleggen bij overtreding van dit verbod.

IT-MANAGERS IN DE ZORG STAAN VOOR LASTIGE KEUZES

ag

Voor reacties en nieuwe bijdragen van IT-experts:
Henk Ester,
070 3780397
h.ester@sdu.nl

Natascha van Duuren (n.vanduuren@declercq.com) is advocaat-partner bij De Clercq Advocaten Notarissen te Leiden.
Met dank aan Kees Zwinkels, docent-onderzoeker aan de Vrije Universiteit Amsterdam, vakgebied recht en e-overheid, en werkzaam als advocaat bij De Clercq Advocaten Notarissen.