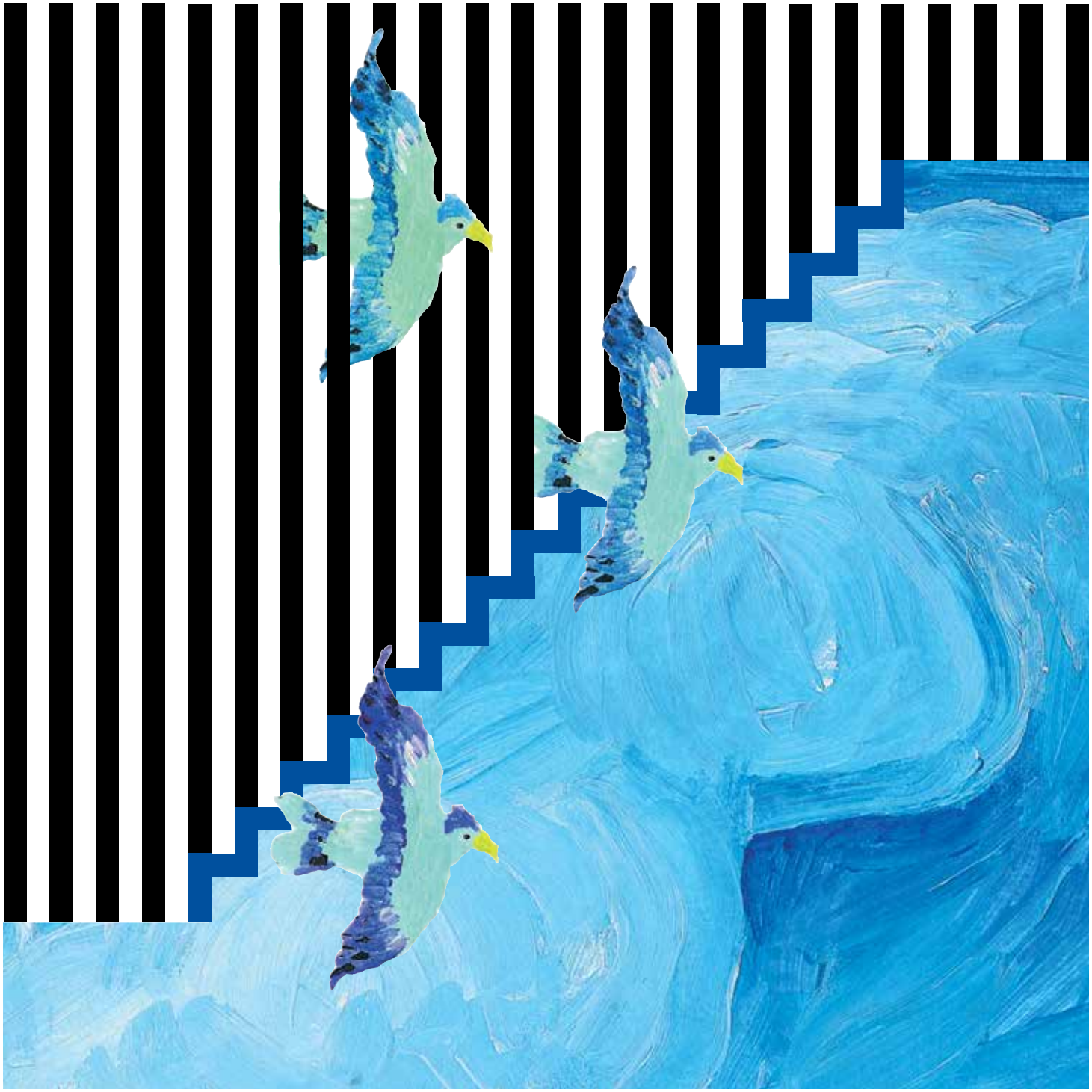

Beveiliging van medische gegevens bij zorginstellingen in België en Nederland

Kennedy Van der Laan

Opgesteld door (laatste update: 22 april 2015)

Kennedy Van der Laan
www.kvdl.nl

Fenna van Dijk (fenna.van.dijk@kvdl.nl)
Hester de Vries (hester.de.vries@kvdl.nl)
Maarten Goudsmit (maarten.goudsmit@kvdl.nl)
Femke Leopold (femke.leopold@kvdl.nl)
Esther Pans (esther.pans@kvdl.nl)

in samenwerking met

Lorenz
www.lorenz-law.com

Jan Dhont (j.dhont@lorenz-law.com)
David Dumont (d.dumont@lorenz-law.com)
Antoine Druetz (a.druetz@lorenz-law.com)
Evelyne Kerkdijk (e.kerkdijk@lorenz-law.com)

In opdracht van:
Imprivata
www.imprivata.com

Inhoud

Voor de verwerking van medische persoonsgegevens gelden strenge beveiligingsverplichtingen. Zorginstellingen moeten technische en organisatorische maatregelen treffen om daaraan invulling te geven. In deze white paper worden de beveiligingsverplichtingen toegelicht en wordt uitgelegd welke risico's een zorginstelling loopt als zij niet aan die verplichtingen voldoet.

Europa

Binnen de Europese Unie geldt geharmoniseerde wetgeving voor de verwerking van persoonsgegevens. Deze wetgeving schrijft voor dat persoonsgegevens worden beveiligd met technische en organisatorische maatregelen. Medische gegevens zijn vanwege hun gevoelige aard onderworpen aan strengere regels en vereisen derhalve ook verdergaande beveiligingsmaatregelen. Op Europees niveau zijn alle privacytoezichthouders verenigd in de Artikel 29 Werkgroep, die het standpunt heeft ingenomen dat het gebruik van een EPD door een zorginstelling slechts aanvaardbaar is indien "toegang voor onbevoegden vrijwel onmogelijk is en voorkomen wordt". Dit moet worden gewaarborgd door beveiligingsmaatregelen die "om de toepassing ervan te bevorderen, op gebruikersvriendelijke wijze worden opgezet"

Sinds 1995 kent de Europese Unie één Richtlijn die de regels stelt voor de bescherming van persoonsgegevens.
Persoonsgegevens is een breed begrip dat alle informatie omvat die betrekking heeft op een geïdentificeerd of identificeerbaar persoon. De gegevens in een medisch dossier zijn (vrijwel) altijd persoonsgegevens en dus onderworpen aan deze regels.
Medische persoonsgegevens worden in de EU - en dus ook in de lidstaten - beschouwd als bijzondere persoonsgegevens en kennen als zodanig een strenger beschermingsregime. Dat vertaalt zich niet alleen in strengere eisen aan de hulpverlener, bijvoorbeeld omtrent het verkrijgen van informed consent voor de verwerking, maar ook aan de informatietechnologie die door een zorginstelling wordt gebruikt.

Persoonsgegevens dienen te worden beveiligd door middel van technische en organisatorische maatregelen. Deze maatregelen moeten onder meer voorkomen dat iemand onrechtmatig toegang kan krijgen tot de persoonsgegevens in het dossier van een patiënt. Uiteraard is het onmogelijk om absolute beveiliging te garanderen. De Richtlijn stelt daarom dat die maatregelen, rekening houdend met de stand van de techniek en de kosten van tenuitvoerlegging, een passend beveiligingsniveau moeten garanderen gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich brengen.

De Europese Richtlijn schrijft geen concrete maatregelen voor, maar geeft wel aan dat de aard van de gegevens een rol speelt. In het geval van medische persoonsgegevens gaat het om "bijzondere" - en daarmee zeer gevoelige - gegevens. Hoe effectief de beveiligingsmaatregelen moeten zijn blijkt bijvoorbeeld uit een advies van de zogenaamde Artikel 29 Werkgroep, de groep waarin alle Europese privacytoezichthouders verenigd zijn. Deze werkgroep schrijft in haar advies over het gebruik van een EPD systeem: "Uit het oogpunt van gegevensbescherming is het systeem slechts aanvaardbaar indien de toegang voor onbevoegden vrijwel onmogelijk is en voorkomen wordt. (…) De integriteit van het systeem moet worden gewaarborgd door toepassing van kennis en instrumenten volgens de laatste stand van de techniek op het gebied van informatica en informatietechnologie."

Het is echter onvoldoende om technische beveiligingsmaatregelen te nemen, zonder daarbij ook passende organisatorische maatregelen te treffen. Hulpverleners moeten immers ook daadwerkelijk gebruik maken van de beschikbare techniek. Het enkele verplicht stellen is daarvoor onvoldoende. "Alle beveiligingsmaatregelen moeten, om de toepassing ervan te bevorderen, op gebruikersvriendelijke wijze worden opgezet", aldus de Artikel 29 Werkgroep. Kortom, goed gedrag moet ook gefaciliteerd worden, zoals wordt beoogd met de producten van Imprivata.

In 2012 is door de Europese Commissie een voorstel gedaan voor een nieuw raamwerk van regels op het gebied van de bescherming van persoonsgegevens. Het voorstel van de Commissie is om een algemene Verordening gegevensbescherming in te voeren, die rechtstreeks geldt in alle lidstaten van de EU. Het voorstel voor deze Verordening omvat aangescherpte regels voor bescherming van (bijzondere) persoonsgegevens en hoge boetes voor niet naleving daarvan. Het huidige voorstel voorziet in boetes tot 1 miljoen Euro of 2% van de wereldwijde omzet van de overtreder. Het Europees parlement is voorstander van veel hogere boetes, namelijk tot 100 miljoen Euro of 5% van de wereldwijde

Nederland

In Nederland zijn deze Europese regels over de bescherming van persoonsgegevens geïmplementeerd in de Wet bescherming persoonsgegevens. Bovendien kent het nationale recht ook voorschriften omtrent de medische vertrouwelijkheid. Die bepalen dat een zorginstelling alleen toegang tot een EPD mag geven aan zorgmedewerkers die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst. Dit moet door middel van technische en organisatorische maatregelen worden geborgd. Deze maatregelen zijn onder meer terug te vinden in de standaard NEN 7510. Daarin wordt onder meer benadrukt dat het enkele gebruik van wachtwoordbeveiliging niet altijd beantwoordt aan de eisen van de medische praktijk. Het gebruik van alternatieven als biometrie en smartcards is vaak sneller en veiliger, aldus NEN 7510. Bovendien rust op elke zorginstelling de verplichting om van elke individuele gebruiker bij te houden wanneer en van welke patiënt hij/zij een dossier heeft bekeken (logging).

Toegangs-beveiliging

In Nederland is de Europese Richtlijn geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp). Daarin zijn dezelfde regels voor de beveiliging van persoonsgegevens vastgelegd als hiervoor besproken voor Europa. Het College Bescherming Persoonsgegevens (CBP) ziet erop toe dat Wbp deugdelijk wordt nageleefd.

De regels omtrent de beveiliging van de toegang tot patiëntgegevens zijn in Nederland nader uitgewerkt. Op basis van de Wet inzake de geneeskundige behandelingsovereenkomst, is het de hulpverlener verboden om informatie over zijn of haar patiënt met anderen te delen. De hulpverlener mag gegevens wel delen met personen die "rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst". Rechtstreekse betrokkenheid wil zeggen dat een zorginstelling waarborgen moet bieden om veilig te stellen dat alleen toegang tot patiëntgegevens wordt verleend aan een hulpverlener die daadwerkelijk bij de behandeling van de patiënt betrokken is. Dat betekent dat de technische en organisatorische maatregelen van een zorginstelling erop gericht moeten zijn om te voorkomen dat hulpverleners toegang hebben tot de informatie van een patiënt waarmee ze geen behandelrelatie hebben. Een van de risico's is dat hulpverleners niet daadwerkelijk gebruik maken van de beschikbare beveiligingsmiddelen en niet consequent uitloggen na elk gebruik van een werkstation. Aldus kunnen anderen meekijken in de dossiers van patiënten van deze hulpverlener. Dat is in strijd met de wet.

Bij veel zorginstellingen blijkt dit mis te gaan. De Inspectie Gezondheidszorg (IGZ) en het CBP concludeerden in een gezamenlijk onderzoek in 2007: "Bij ruim tweederde van de ziekenhuizen waren nog groepsaccounts aanwezig, waarbij meerdere mensen onder één inlognaam en wachtwoord werkten. (…) Veelal was dit om praktische redenen ingesteld, namelijk zodat medewerkers niet voortdurend apart hoefden in te loggen." Met anderen woorden, het was gemakkelijk om in strijd met de regels te handelen.

Deze observatie herhaalde het CBP in het verslag van zijn onderzoek naar de toegangsbeveiliging bij zorginstellingen in 2013. Het CBP merkte op weliswaar positief te zijn "over maatregelen van zorginstellingen voor bewustwording van het personeel met gedragscodes, personeelsbeleid en sancties", maar "dat hiermee geen compensatie kan worden geboden voor het niet inzetten van voldoende technologische maatregelen waarmee 'beheersing vooraf' in voldoende mate kan worden gerealiseerd. Het succes van maatregelen mag niet grotendeels afhankelijk zijn van de zelfbeheersing van de medewerkers." Kortom, iedere zorginstelling heeft een verplichting om door middel van technische en organisatorische maatregelen effectief af te dwingen dat de verplichte toegangsbeveiliging daadwerkelijk gebruikt wordt.

Het CBP legt in zijn Richtsnoeren beveiliging van persoonsgegevens uit hoe het de beveiliging van persoonsgegevens beoordeelt bij zorginstellingen die door de toezichthouder worden bezocht. Daarin noemt het CBP de norm NEN 7510 een gezaghebbende, sectorale uitwerking van de beveiligingsverplichting op grond van de Wbp. "Als een ziekenhuis voldoet aan NEN 7510, mag ervan uit worden gegaan dat het ook voldoet aan bovengenoemde wettelijke bepaling", aldus het CBP. De Regeling gebruik burgerservicenummer in de zorg stelt de norm NEN 7510 verplicht voor alle zorginstellingen.

Ook uit deze NEN norm blijkt dat het louter implementeren van (technische)

beveiligingsmaatregelen niet voldoende is. Op grond van paragraaf 11.6.1 moet bijvoorbeeld bij de toegangsbeheersing rekening worden gehouden met spoedeisende situaties voor patiënten waarbij goede uitvoering van de zorg niet mag worden ingeperkt door te strikte regels." Paragraaf 11.2.3 schrijft het gebruik van wachtwoorden voor, maar geeft blijk van daaraan verbonden risico's "Wachtwoorden zijn een gebruikelijk middel om de identiteit van een gebruiker te verifiëren voordat toegang wordt verleend tot een informatiesysteem (…). Bijvoorbeeld tijdsdruk en steriliteitseisen kunnen het gebruik van wachtwoorden echter lastig maken. Alternatieve technologieën voor gebruikersidentificatie en -authenticatie zijn te overwegen, zoals biometrie (…) en het gebruik van 'hardware tokens', bijvoorbeeld smartcards."

Eerder kwam aan bod dat beveiligingsmaatregelen gebruikersvriendelijk moeten zijn om werkelijk effectief te zijn. De NEN 7510 norm voegt daaraan toe dat ook het zorgbelang een rol speelt bij het kiezen van de juiste techniek voor toegangsbeveiliging: "Gebruik waar krachtige authenticatie en verificatie van de identiteit nodig zijn, andere authenticatiemethoden dan wachtwoorden, zoals cryptografische hulpmiddelen, smartcards, 'tokens' of biometrische hulpmiddelen." De zorginstelling staat dus voor de uitdaging om een hoog beveiligingsniveau te verenigen met het zorgbelang, tijdsdruk en gebruikersvriendelijkheid. Imprivata beoogt met haar product daaraan een bijdrage te leveren.

Toezicht op toegangsbeveiliging: logging en controle

Op grond van NEN 7510 zijn zorginstellingen verplicht om raadplegingen door hulpverleners van patiëntgegevens vast te leggen in logbestanden (logging). In de woorden van het CBP:
"Zorginstellingen waar geen logging plaatsvindt van alle acties, voldoen niet aan [de] Wbp." Dit is verder uitgewerkt in de norm NEN 7513, die specifiek over logging gaat: "Zorginformatiesystemen behoren telkens wanneer een gebruiker via het systeem toegang krijgt tot patiëntgegevens, nieuwe patiëntgegevens invoert, bijwerkt of archiveert een beveiligde logregel aan te maken. In de logging behoort minimaal de identiteit van de gebruiker en van de patiënt uniek vast te liggen, samen met de uitgevoerde actie (invoeren, raadplegen enz.) en datum en tijd van de actie."

Alleen wanneer van elke gebruiker individueel kan worden vastgelegd welke gegevens hij raadpleegt, kan er dus worden gezegd dat een zorginstelling aan de wet voldoet. Dat dit bij veel zorginstellingen misgaat kwam duidelijk naar voren in het hiervoor al genoemde gezamenlijk onderzoek van de IGZ en het CBP in 2007. Er waren immers bij ruim tweederde van de ziekenhuizen groepsaccounts, waarbij meerdere mensen onder één inlognaam en wachtwoord werkten. Dit betrof vooral verpleegafdelingen en de eerste hulp. De groepsaccounts waren om praktische redenen ingesteld, namelijk zodat medewerkers niet voortdurend apart hoefden in te loggen. Daardoor was echter niet inzichtelijk wie nu precies welke gegevens heeft geraadpleegd.

In 2013 kwam het CBP tot de conclusie dat veel zorginstellingen nog steeds niet aan deze eis kunnen voldoen: "Het CBP constateert dat de meeste onderzochte zorginstellingen niet structureel bijhouden wie wanneer welk patiëntendossier heeft geraadpleegd (logging). Soms ontbreken daartoe de technische mogelijkheden."

Risico's op handhaving bij onvoldoende beveiliging

Uit onderzoeken van het College bescherming persoonsgegevens (CBP) blijkt dat veel zorginstellingen weliswaar beveiligingsmaatregelen nemen, maar dat deze maatregelen vaak onvoldoende zijn of in de praktijk onvoldoende door zorgmedewerkers worden toegepast. In dat geval handelt de zorginstelling in strijd met de wet en kan het CBP een last onder dwangsom opleggen. Op nationaal niveau wordt er over gesproken om het CBP de bevoegdheid te geven boetes van enkele honderdduizenden euro's op te leggen. Op Europees niveau spreekt men over nieuwe wetgeving voor gegevensbescherming waarbij maximale boetes zijn voorgesteld van 100 miljoen euro of 5% van de wereldwijde omzet van de overtreder.

In Nederland is het CBP bevoegd schendingen van de regels ter bescherming van persoonsgegevens op te sporen, te onderzoeken en te bestraffen. Daarnaast kunnen ook individuele patienten optreden tegen overtreders, door zich te beroepen op hun rechten op grond van de behandelingsovereenkomst of op een overtreding van hun privacyrechten.

Het CBP kan momenteel op een aantal manieren handhaven. Wanneer het CBP constateert dat er een overtreding plaatsvindt, kan het CBP een last onder dwangsom opleggen. Dat is een besluit waarbij het CBP een bevel geeft om die overtreding te beëindigen (de last) en indien zulks niet is gebeurd binnen een bepaalde termijn, een boete per dag of week kan invorderen (de dwangsom). Zolang de dwangsom in proportie staat tot de overtreding is er geen bovengrens aan de maximale dwangsom. Bij een handhavingsactie van het CBP tegen een ziekenhuis werd in 2010 bijvoorbeeld een dwangsom van €120.000 verbeurd.

Momenteel heeft een overtreder altijd nog de gelegenheid om de overtreding te beëindigen voordat hij de dwangsom moet betalen. Daarin komt verandering. De regering werkt aan een wet die het CBP de bevoegdheid geeft om boetes op te leggen. Hoewel de tekst van het wetsvoorstel nog niet vaststaat, is vrijwel zeker dat het uiteindelijke maximale boetebedrag enkele honderdduizenden euro's zal bedragen. In voorkomende gevallen kan naast de zorginstelling ook de natuurlijke persoon die feitelijk leiding gaf aan de overtreding een boete worden opgelegd.

Ook de aankomende Europese Verordening gegevensbescherming zal bij inwerkingtreding het risico van hoge boetes vergroten. Het huidige voorstel voorziet in boetes tot 1 miljoen Euro of 2% van de wereldwijde omzet van de overtreder. Het Europees parlement is voorstander van veel hogere boetes, namelijk tot 100 miljoen Euro of 5% van de wereldwijde omzet van de overtreder.

Medische aansprakelijkheid

De arts/verpleegkundige dient bij zijn werkzaamheden de zorg van een goed hulpverlener in acht te nemen en moet daarbij handelen volgens de medisch-professionele standaard. Deze open norm wordt per geval 'ingevuld' door toetsing van het handelen van de hulpverlener aan de ten tijde van het handelen geldende richtlijnen, protocollen en gebruiken (best practices) in het licht van de individuele situatie. De zorginstelling kan aansprakelijk zijn, indien binnen de zorginstelling wordt gehandeld in strijd met NEN-normen en overige technische en organisatorische (beveiligings)verplichtingen. Onvoldoende beveiliging van medische gegevens kan daarmee leiden tot medische aansprakelijkheid, met name als daardoor een medische fout wordt veroorzaakt.

De kern van medische aansprakelijkheid wordt gevormd door artikel 7:453 BW, dat bepaalt dat de arts/verpleegkundige bij zijn werkzaamheden de zorg van een goed hulpverlener in acht moet nemen en daarbij moet handelen volgens de medisch-professionele standaard. Deze open norm wordt per geval 'ingevuld' door toetsing van het handelen van de hulpverlener aan de ten tijde van het handelen geldende richtlijnen, protocollen en gebruiken (best practices) in het licht van de individuele situatie.

Op grond van de centrale aansprakelijkheid ex art. 7:462 BW is de zorginstelling aansprakelijk voor een tekortkoming binnen de muren van de instelling 'als ware het zelf partij' bij de medische behandelingsovereenkomst. Op de zorginstelling rust voorts de verplichting om de geldende normen en regels voor de beveiliging van de toegang tot medische persoonsgegevens in acht te nemen en tevens om er zorg voor te dragen dat die normen en regels in acht (kunnen) worden genomen door de aldaar werkzame personen. Met andere woorden: de zorginstelling dient goed gedrag te faciliteren en erop toe te zien dat de nodige technische en organisatorische beveiligingsmaatregelen worden ten aanzien van medische gegevens worden genomen. Onvoldoende beveiliging van medische gegevens kan leiden tot medische aansprakelijkheid van de arts en/of de zorginstelling op grond van de hiervoor genoemde grondslagen en tevens op grond van onrechtmatige daad (art. 6:162 BW) en/of wanprestatie, met name als daardoor een medische fout wordt veroorzaakt waardoor een patiënt schade lijdt. Een voorbeeld daarvan is een tekortkoming in de 'TOP' (Time-Out Procedure). Per 1 januari 2011 dienen ziekenhuizen voorafgaand aan operatieve ingrepen een checklist te hanteren om de laatste details voor een operatie door te nemen. Dit is een cruciale veiligheidsnorm die door de IGZ wordt gekwalificeerd als 'de onderkant van verantwoorde medische zorg'. Het is derhalve aannemelijk dat de arts/zorginstelling die niet voldoet aan de TOP niet voldoet aan de medisch-professionele standaard en dus privaat-, tucht- en zelfs strafrechtelijk kan worden aangesproken voor fouten die daardoor zijn veroorzaakt. Daardoor is het van belang op betrouwbare wijze vast te leggen wie wanneer over welke medische gegevens beschikte en wie wanneer daadwerkelijk betrokken was bij de medische behandeling van de patiënt.

Een ander voorbeeld waarbij medische aansprakelijkheid voor onvoldoende beveiliging van medische gegevens aan de orde kan zijn, is in het kader van het vereiste van 'Closed Loop'. Daaronder wordt verstaan een gesloten (digitaal) systeem van medicatievoorschrijving, -uitzetting en –toediening, waarin interne controles door alle betrokken disciplines (artsen, verpleegkundigen, apothekers) zijn ingebouwd om zo de

kans op fouten te verkleinen. Er zijn diverse richtlijnen van (medische) beroepsverenigingen en van de IGZ verschenen die zien op medicatieveiligheid die op bepaalde beslismomenten in de ketenzorg de beschikbaarheid van een actueel medicatieoverzicht eisen. Net als bij TOP, is het aannemelijk dat de zorginstelling die niet voldoet aan de Closed Loop-voorwaarden (waardoor bijvoorbeeld een patiënt een verkeerd medicijn krijgt voorgeschreven, of te laat, en daardoor schade oploopt) aansprakelijk is op grond van art. 7:453 BW en/of onrechtmatige daad ex art. 6:162 BW.
Voorts is beveiliging van medische gegevens van belang omdat de patiënt op grond van de Wgbo geïnformeerd en voorgelicht moet worden over gewijzigde medicatie en vanwege het voor zorgverleners geldende wettelijke vereiste om een goed dossier bij te houden (art. 7:454 BW). Ten slotte geldt dat het medisch dossier voor de bewijspositie van de arts/zorginstelling doorgaans van cruciaal belang is, mochten zij juridisch worden aangesproken (op welke juridisch-inhoudelijke grond ook).

Aansprakelijkheid van bestuurders

Een stap verder gaat de persoonlijke aansprakelijkheid van bestuurders en toezichthouders van zorginstellingen. Die aansprakelijkheid gaat over het privévermogen van de betrokkenen en is om die reden al ingrijpend. Elke bestuurder is jegens de rechtspersoon gehouden tot een behoorlijke vervulling van zijn taak.
Als er sprake is van een tekortkoming die een ernstig verwijt oplevert en aan ten minste één van de bestuurders persoonlijk te wijten is, dan zijn in beginsel alle bestuurders jegens de rechtspersoon voor de gehele schade hoofdelijk aansprakelijk. Of sprake is van een 'ernstig verwijt' moet aan de hand van alle omstandigheden van het geval worden bepaald. Externe bestuurdersaansprakelijkheid kan om de hoek komen kijken indien een bestuurder een wettelijke of statutaire norm heeft overtreden, die het belang van een van de stakeholders – waaronder de patiënt – beoogt te beschermen. Ook regels van zelfregulering, zoals de Zorgbrede Governancecode 2010, waarin wordt bepaald dat "de geleverde zorg voldoet aan eigentijdse kwaliteitseisen", spelen daarbij een rol. Daarnaast is denkbaar dat het bestuur en/of de toezichthouders – naast de instelling – aansprakelijk zijn, wanneer door professionals binnen een zorginstelling wordt gehandeld in strijd met op hen rustende (beveiligings)verplichtingen.

Een stap verder gaat de persoonlijke aansprakelijkheid van bestuurders en toezichthouders van zorginstellingen. Die aansprakelijkheid gaat over het privévermogen van de betrokkenen en is om die reden al ingrijpend. De afgelopen jaren is in de semipublieke sector, waaronder de zorgsector, een toename te zien van de bereidheid om bestuurders en toezichthouders persoonlijk aan te spreken. Hoewel de drempel voor bestuurdersaansprakelijkheid hoog ligt en die aansprakelijkheid niet snel aan de orde is, krijgen deze claims vaak veel media-aandacht en maken zij al snel deel uit van het publieke en politieke debat. Na diverse incidenten die "het vertrouwen van burgers in het functioneren van bestuurders en toezichthouders in semipublieke sectoren hebben geschaad, en daarmee het vertrouwen in de publieke zaak" , is onder meer de Commissie Behoorlijk Bestuur onder leiding van Femke Halsema, in het leven geroepen.

Wet Toezicht en Bestuur Rechtspersonen
Veel zorginstellingen hebben de rechtsvorm van een stichting. Recent is een concept wetsvoorstel gelanceerd dat de rechtspositie van bestuurders en toezichthouders bij verenigingen en stichtingen ingrijpend wijzigt. Het doel van de Wet Toezicht en Bestuur Rechtspersonen is vooral om de nu bestaande verschillen tussen de diverse soorten rechtspersonen op te heffen. Onder meer komt er een wettelijke verankering van het toezichthoudend orgaan en worden de normen voor interne en externe aansprakelijkheid binnen en buiten faillissementssituaties, gelijk getrokken. Zo komt er voor alle rechtspersonen een uniforme regeling inhoudend dat bestuurders en leden van het toezichthoudend orgaan aansprakelijk zijn in geval van onbehoorlijke taakvervulling. Met het wetsvoorstel wordt invulling gegeven aan de aanbevelingen van de Commissie Behoorlijk Bestuur.

Toetsingskader
Belangrijke aansprakelijkheidsgronden voor bestuurders en toezichthouders zijn:
1. De (interne) aansprakelijkheid jegens de zorginstelling (art. 2:9 BW; deze aansprakelijkheid is in het huidige recht niet geregeld voor toezichthouders van stichtingen en verenigingen);
2. De (externe) aansprakelijkheid jegens derden, waaronder patiënten;

3. De aansprakelijkheid jegens de curator in geval van een faillissement (waarbij de aansprakelijkheid ziet op het gehele faillissementstekort. Bij commerciële verenigingen en stichtingen geldt deze aansprakelijkheid thans ook voor toezichthouders).

In algemene termen geldt dat elke bestuurder jegens de rechtspersoon gehouden is tot een behoorlijke vervulling zijn taak (artikel 2:9 BW). Als er sprake is van een tekortkoming die een ernstig verwijt oplevert en aan ten minste één van de bestuurders te wijten is, dan zijn in beginsel alle bestuurders jegens de rechtspersoon voor de gehele schade hoofdelijk aansprakelijk. In voorkomende gevallen kan een bestuurder of toezichthouder op grond van een onrechtmatige daad jegens derden (extern) aansprakelijk zijn. Dit betreft een afgeleide aansprakelijkheid. Het is namelijk in de eerste plaats de rechtspersoon die verbonden wordt, als het bestuur binnen de kring van zijn bevoegdheid optreedt en daardoor schade wordt veroorzaakt. Primair zal het dan ook de zorginstelling zijn die aansprakelijk is, indien bijvoorbeeld niet wordt gehandeld volgens de NEN-normen, of indien anderszins beveiligingsvoorschriften worden geschonden, waardoor een patiënt schade lijdt.

Aansprakelijkheid van de bestuurder of toezichthouder komt pas in beeld indien sprake is van aan de bestuurder of toezichthouder persoonlijk te maken ernstig verwijt. Of sprake is van een 'ernstig verwijt' moet aan de hand van alle omstandigheden van het geval worden bepaald. Volgens vaste rechtspraak speelt daarbij onder meer een rol de aard van de door de rechtspersoon uitgeoefende activiteiten, de in het algemeen daaruit voortvloeiende risico's, de voor het bestuur en/of de toezichthouders geldende voorschriften en het inzicht en de zorgvuldigheid die mogen worden verwacht van een bestuurder/toezichthouder die voor zijn taak berekend is en deze nauwgezet vervult.

Externe bestuurdersaansprakelijkheid komt om de hoek kijken indien een bestuurder een wettelijke of statutaire norm heeft overtreden, die het belang van een van de stakeholders – waaronder de patiënt – beoogt te beschermen. Ook de regels van governance (zelfregulering) zijn daarbij van belang. Blijkens de Zorgbrede Governancecode 2010 (artikel 2) behoort het onder meer tot de verantwoordelijkheid van de zorginstelling dat "de geleverde zorg voldoet aan eigentijdse kwaliteitseisen." Art. 2 lid 3 bepaalt dat het bestuur en de toezichthouders overeenkomstig hun wettelijke en statutaire taakverdeling verantwoordelijk zijn voor de naleving van de Code. Denkbaar is voorts dat het bestuur en/of de toezichthouders aansprakelijk zijn, wanneer door de zorginstelling of professionals binnen die instelling wordt gehandeld in strijd met op hen rustende verplichtingen. Zoals hiervoor aan de orde kwam, is de zorginstelling dan in de eerste plaats zelf aansprakelijk. In uitzonderlijke gevallen kan echter worden 'doorgestoten' naar de bestuurders en toezichthouders persoonlijk. Er moet dan zijn voldaan aan de drempel van een ernstig en persoonlijk verwijt dat de zorginstelling waarvoor de bestuurders en toezichthouders verantwoordelijk zijn, niet aldus in ingericht dat de geldende normen en regels in acht (kunnen) worden genomen door de aldaar werkzame personen. Dit geldt ook voor de wettelijke verplichtingen tot beveiliging van de toegang tot medische persoonsgegevens, de TOP en Closed Loop-voorwaarden. Het faciliteren van goed gedrag binnen de zorginstelling én het toezien op de naleving daarvan, is bij uitstek een verantwoordelijkheid van het bestuur en een schending van die verantwoordelijkheid kan in bijzondere gevallen leiden tot bestuurdersaansprakelijkheid.

België

De digitalisering van het medische dossier heeft het leven van de beroepsbeoefenaars in de gezondheidszorg op verschillende vlakken vergemakkelijkt. Zo is alle informatie betreffende het medische verleden van een patiënt, eventuele allergieën en andere belangrijke informatie voor het stellen van een correcte diagnose en bepalen van een gepaste behandeling nu met enkele klikken beschikbaar. De digitalisering van het medisch dossier heeft dan ook een positieve invloed op de kwaliteit en efficiëntie van de zorgverlening.

Inleiding

De digitalisering van het medische dossier heeft het leven van de beroepsbeoefenaars in de gezondheidszorg op verschillende vlakken vergemakkelijkt. Zo is alle informatie betreffende het medische verleden van een patiënt, eventuele allergieën en andere belangrijke informatie voor het stellen van een correcte diagnose en bepalen van een gepaste behandeling nu met enkele klikken beschikbaar. De digitalisering van het medisch dossier heeft dan ook een positieve invloed op de kwaliteit en efficiëntie van de zorgverlening.

Aan de andere kant brengt deze evolutie echter enkele nieuwe vragen en problemen met zich mee. Naarmate meer medische gegevens worden gedigitaliseerd wordt de noodzaak van een goede beveiliging van deze gegevens almaar groter.

Er is dus steeds een tweestrijd tussen enerzijds de kwaliteit van de zorgverlening, die gebaat is bij een zo efficiënt mogelijke beschikbaarheid van de gegevens uit medische dossiers, en anderzijds de noodzaak aan beperking van de toegang tot deze gegevens met het oog op de bescherming van de privacy van de betrokken patiënten.

Een illustratie van deze tweestrijd vindt men onder andere in het kader van de closed loop medicatie- en time-out systemen/procedures. Beide systemen verbeteren de patiëntenveiligheid en dienstverlening door een betere uitwisseling en/of een grotere toegankelijkheid tot informatie uit het medisch dossier te bewerkstelligen. Deze grotere toegankelijkheid tot patiëntengegevens vergroot echter de kans op schending van de privacy van de betrokken patient. Strikte toegangsbeveiligingsmethodes zijn dan ook van groot belang. Voor het bereiken van het doel van deze procedures moet men immers kunnen garanderen dat (i) enkel geautoriseerde personen toegang krijgen, (ii) de informatie ingegeven werd door een bevoegd persoon, en (ii) men achteraf kan nagaan wie welke informatie heeft toegevoegd. Deze beveiligingsmethodes mogen echter de toegang tot de informatie niet zodanig bemoeilijken dat zorgverleners er van afzien om de systemen consequent te gebruiken. Een consequent en correct gebruik van de systemen beperkt immers de kans op medische fouten en dus de aansprakelijkheid van het ziekenhuis.

Vereisten beveiliging informatie & JCI/ NIAZ Quality-Accreditatie

Ziekenhuizen en beroepsbeoefenaars in de gezondheidszorg zijn verplicht bepaalde informatie betreffende hun patiënten bij te houden in zogenaamde patiëntendossiers. Aangezien de informatie in deze dossiers de gezondheidstoestand van de betrokken patiënt betreft, gelden er strenge regels betreffende de beveiliging van deze gegevens, inclusief de maatregelen ter voorkoming van ongeoorloofde toegang tot deze gegevens.

Zorginstellingen en beroepsbeoefenaars in de gezondheidszorg zijn van oudsher verplicht dossiers bij te houden betreffende hun patiënten. Dit wordt onder andere bepaald in het koninklijk besluit van 23.10.1964 tot bepaling van de normen die door de ziekenhuizen en hun diensten moeten worden nageleefd; de gecoördineerde wet op de ziekenhuizen van 10.07.2008 (m.b. artikel 20 voor wat het medisch dossier betreft en artikel 25 voor wat het verpleegkundig dossier betreft, verder uitgevoerd door het koninklijk besluit van 3.05.1999 betreffende het Algemeen Medisch Dossier, het koninklijk besluit van 3.05.1999 houdende bepaling van de algemene minimumvoorwaarden waarvan het medisch dossier, bedoeld in artikel 15 van de wet op de ziekenhuizen, gecoördineerd op 7.08.1987, moet voldoen en het koninklijk besluit van 28.12.2006 houdende bepaling van de algemene minimumvoorwaarden waaraan het verpleegkundig dossier, bedoeld in artikel 17quater van de wet op de ziekenhuizen, gecoördineerd op 7.08.1987, moet voldoen); en artikel 9 van de wet van 22.08.2002 betreffende de rechten van de patiënt (hierna: "Patiëntenrechtenwet").

Uit al deze wettelijke bepalingen blijkt duidelijk dat zorginstellingen en beroepsbeoefenaars in de gezondheidszorg (en meer in het bijzonder voor ziekenhuizen, de hoofdgeneesheer van het ziekenhuis) ervoor moet zorgen dat voor alle patiënten een medisch dossier wordt aangelegd. De wettelijke regels laten toe dat deze patiëntendossiers elektronisch dan wel in papier worden bijgehouden. In beide gevallen moeten de beroepsbeoefenaars in de gezondheidszorg er echter over waken dat de gezondheidsgegevens van de betrokken patiënten op een veilige manier worden verwerkt. Één van de deelaspecten van deze veilige bewaring is de implementatie van maatregelen om ongeoorloofde toegang tot gegevens in het patiëntendossier te voorkomen.

Zo bepaalt artikel 9 van de Patiëntenrechtenwet dat iedere patiënt recht heeft op een zorgvuldige bijgehouden en veilig bewaard patiëntendossier. Wat terminologie "veilig bewaard" wordt niet nader bepaald in de wet.

Het bijhouden van patiëntengegevens in een elektronisch (of logisch gestructureerd manueel) dossier valt verder onder de toepassing van de wet van 8.12.1992 op de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna: "Privacywet"). De Privacywet vormt de omzetting van de hierboven besproken Europese Richtlijn 95/46 in het Belgische recht. De Privacywet is van toepassing op elke geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op elke niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand (zijnde elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn) zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Hieruit volgt dat het verwerken van patiëntengegevens in (elektronische) patiëntendossiers vrijwel altijd binnen het toepassingsgebied van de Privacywet zal vallen. De zorginstelling of beroeps-

beoefenaar in de gezondheidszorg in het kader van wiens activiteiten de patiëntendossiers worden aangemaakt en bijgehouden zijn verantwoordelijk voor de verwerking van de persoonsgegevens die in het kader daarvan plaatsvindt. Op de verantwoordelijke voor de verwerking rusten een aantal belangrijke verplichtingen. Zo moet hij of zij ervoor zorgen dat (i) de verwerking van persoonsgegevens legitiem en proportioneel is, (ii) de betrokken patiënten voldoende worden geïnformeerd betreffende de verwerking van hun persoonsgegevens, (iii) verzoeken van de patiënten voor toegang, wijziging en vernietiging van hun persoonsgegevens worden nageleefd, (iv) aangifte van de gegevensverwerking wordt gedaan bij de Privacycommissie, enz…

Naast de hierboven vermelde verplichtingen legt de Privacywet ook verplichtingen op naar beveiliging van de verwerkte persoonsgegevens. De verantwoordelijke voor de gegevensverwerking (in dit geval de zorginstelling of beroepsbeoefenaar in de gezondheidszorg die de elektronisch patiëntendossiers aanmaakt en bijhoudt) moet meer bepaald gepaste technische en organisatorische maatregelen implementeren om de verwerkte gegevens te beveiligen tegen toevallige of ongeoorloofde vernietiging, verlies, wijziging of toegang, en iedere andere niet toegelaten verwerking. Om te bepalen welk niveau van beveiligingsmaatregelen gepast zijn moet enerzijds rekening gehouden worden met de stand van de techniek en de kosten van het implementeren van dergelijke maatregelen en anderzijds met de aard van de verwerkte gegevens en de hieraan verbonden risico's.
Aangezien de gegevens opgenomen in een patiëntendossier hoofdzakelijk gegevens zijn die de gezondheidstoestand van de betrokken patiënt betreffen, moeten er in dit kader robuuste beveiligingsmaatregelen worden geïmplementeerd. Gezondheidsgegevens worden immers als bijzonder gevoelig beschouwd. Het is voor het ziekenhuis en de beoefenaars in de gezondheidszorg, verantwoordelijk voor deze patiëntendossiers, dan ook erg belangrijk om het systeem voor het beheren van de elektronische patiëntendossiers zo op te stellen dat het voldoende waarborgen biedt voor de beveiliging van de gegevens die in dit systeem zijn opgeslagen.
Een deelaspect van de algemene beveiligingsplicht is dat de verantwoordelijke zorginstelling of beroepsbeoefenaar in de gezondheidszorg ervoor moet zorgen dat de personen die onder zijn of haar gezag handelen enkel toegang hebben tot hetgeen deze personen nodig hebben voor de uitoefening van hun taken of de behoefte van de dienst. Zij moeten bovendien verzekeren dat er geen wederrechtelijk gebruik wordt gemaakt van de gegevens in de patiëntendossiers.

Deze algemene wettelijke beveiligingsplicht wordt verder geconcretiseerd in aanbevelingen van de Privacycommissie (de instantie die waakt over de naleving van de Privacywet). Specifiek met betrekking tot toegangsbeveiliging heeft de Privacycommissie, onder andere, de volgende richtsnoeren vooropgesteld:
- Databanken die persoonsgegevens bevatten, mogen slechts toegankelijk zijn vanaf hiervoor bestemde, beveiligde toepassingen.
- De verantwoordelijke organisatie moet zich ervan vergewissen dat persoonsgegevens slechts toegankelijk zijn voor personen die hiertoe uitdrukkelijk gemachtigd zijn. De toegangsmachtigingen moeten vertaald worden in technische voorzieningen en toegangscontroles tot de verschillende informaticaonderdelen. Bovendien moet de identificatie vervolledigd worden met authenticatie van diegene die toegang neemt tot de gegevens, aangezien het om gevoelige gegevens gaat.
- Er moeten zogenaamde loggings- en opsporingsmechanismen worden geïm-

plementeerd. Dit zijn mechanismen die toelaten om achteraf na te gaan wie op een bepaald moment toegang heeft gehad tot gegevens en deze al dan niet heeft bewerkt.
- De organisatie moet een goedgekeurd en geactualiseerd toegangscontrolebeleid hebben met betrekking tot het toekennen, veranderen en verwijderen van toegangsrechten tot systemen waarin persoonsgegevens worden verwerkt en een verantwoordelijke aanstellen die op de naleving hiervan toekijkt.
- De organisatie moet alle gepaste maatregelen nemen om te verhinderen dat persoonsgegevens ongecontroleerd de organisatie verlaten, meer bepaald onder andere door bedrijfsmiddelen te beschermen tegen ongeoorloofde toegang, openbaarmaking, wijziging, vernietiging of verstoring.
- Per systeem moet aan de hand van de beveiligingseisen, de nodige beveiligingsmaatregelen worden genomen om de toegang tot de persoonsgegevens te beperken. Dit dient te gebeuren aan de hand van een: (i) identificatiesysteem, (ii) authenticatiesysteem, en (iii) authorisatiesysteem.

Ook al zijn de richtsnoeren van de Privacycommissie strikt genomen niet bindend, kan hun belang niet worden onderschat. Rechtbanken nemen deze immers in acht bij het bepalen of er al dan niet een fout is begaan bij de beveiliging van de toegang tot de gegevens, die eventueel tot strafrechtelijke dan wel burgerrechtelijke aansprakelijkheid van de instelling of de beroepsbeoefenaar in de gezondheidszorg kan leiden.

Voor het opstellen van deze richtsnoeren heeft de Privacycommissie zich trouwens grotendeels gebaseerd op de internationale ISO/IEC 27002 norm. Deze norm is verder uitgewerkt voor medische informatica in de ISO 277799:2008. Net zoals de richtsnoeren van de Privacycommissie bevat deze norm enkele specifieke vereisten met betrekking tot de beveiliging van toegang tot de verwerkte gegevens. Zo moeten organisaties, actief in de gezondheidszorg, maatregelen nemen om ervoor te zorgen dat de gezondheidsgegevens van een patiënt enkel toegankelijk zijn (i) voor personen met wie een arts-patiënt relatie bestaat, (ii) wanneer de gebruiker een handeling stelt ten behoeve van de patiënt, en (iii) wanneer de gegevens noodzakelijk zijn voor het stellen van deze handeling. Verder wordt bepaald dat "Healthcare organizations are encouraged to consider the implementation of a federated identity and access management solution in recognition of the potential additional support, and reduced administration costs, that this will provide to the access control policy. Additionally, this will support a higher level security access processes, such as smart-card-based access and single-sign-on capability". Net zoals de richtsnoeren van de Privacycommissie, is deze norm niet-bindend, maar door deze norm te respecteren ontstaat er wel een vermoeden ten voordele van de betrokken instelling of beroepsbeoefenaar in de gezondheidszorg dat er afdoende beveiligingsmaatregelen werden geïmplementeerd in het geval er iets mis gaat.

Ook kan worden vastgesteld dat toenemend specifieke wetgeving wordt uitgevaardigd dat voorschrijft dat hospitalen afdoende maatregelen dienen te nemen om toegang tot gezondheidsgegevens te beschermen. Ingevolge een decreet van het Vlaamse Parlement van 23.04.2014 (betreffende de organisatie van een netwerk voor gegevensdeling tussen actoren in de zorg), moeten zorginstellingen bepalen in welke mate en op welke wijze gegevens van hun patienten toegankelijk zijn voor personen die betrokken zijn bij de zorg rekening houden met de (i) functie van de zorgverleners, (ii) aard van de gegevens en (iii) potentiële risico's die aan toegang verbonden zijn. Deze toegangsregels

moeten worden opgenomen in het veiligheidsbeleid van de zorginstelling. Daarnaast dienen zorginstellingen ook een veiligheidsconsulent aan te stellen die toekijkt op de naleving van dit veiligheidsbeleid. Sancties voor het niet naleven van deze vereisten lopen op tot (i) schorsing of intrekking van de werkingsvergunning van de zorginstelling; (ii) inhouding of terugvordering van subsidies; (iii) administratieve geldboetes voor de zorginstelling tot 600.000 Euro (en tot 240.000 Euro voor de zorgverleners); en (iv) ontzegging van toegang tot het netwerk voor gegevensdeling.

Specifiek in de sector van de gezondheidszorg moeten ook de verplichtingen uit de Code van geneeskundige plichtenleer betreffende het medische dossier en de aanbevelingen van de Nationale Raad van de Orde van Geneesheren hieromtrent in acht genomen worden. Op het vlak van elektronische medische dossiers heeft de Nationale Raad verschillende aanbevelingen en adviezen uitgevaardigd. Deze identificeren, kort samengevat, de volgende spelregels voor de beveiliging van informatie in medische dossiers:
- Het toegangsrecht tot patiëntengegevens moet beperkt worden tot de gegevens waarvan de kennis noodzakelijk is voor de verzorging en tijdens de duur ervan.
- Er moet een hiërarchische volgorde opgesteld worden in functie van de bekwaamheden en specialisaties van de toegangsgerechtigden, evenals een selectie van de gegevens onderling. De toegangsbeperkingen dienen gedefinieerd te worden op basis van de volgende criteria: (i) de identiteit en kwalificatie van diegene die toegang wenst (bv. behandelende arts, vertrouwens arts, enz…); (ii) het soort van gegevens (bv. spoedgegevens, gedocumenteerde hypotheses, genetische informatie, enz…); (iii) de vertrouwelijkheidsgraad die de arts, auteur van de gegevens of patiënt aan de betrokken gegevens heeft toegekend; (iv) het doel van de toegang; en (v) beperking van de duur waarvoor de toegang wordt verleend (bv. voor artsen die de patiënt behandelen dient de toegang te worden beperkt tot de periode tijdens welke de desbetreffende artsen de patiënt behandelden).
- Het toegangsrecht van verpleegkundigen dient beperkt te zijn tot bepaalde gegevens in het medisch dossier, voor de periode gedurende dewelke de patient in het hospitaal verblijft en tot de verpleegkundigen die de patiënt effectief verzorgen.

Naast het feit dat deze aanbevelingen net zoals de aanbevelingen van de Privacycommissie in acht zullen worden genomen door de rechtbanken in geval van een geschil omtrent de beveiliging van gegevens, geven deze richtlijnen een nadere invulling van de deontologische verplichtingen van de betrokken beroepsbeoefenaars in de gezondheidszorg.
Verder moet er ook op gewezen worden dat de persoonsgegevens die de patiënt toevertrouwd aan zijn of haar instelling of beroepsbeoefenaar in de gezondheidszorg gedekt zijn door het medisch beroepsgeheim (zoals voorzien in artikel 458 van het Strafwetboek) De Nationale Raad stelt hieromtrent dat een arts geen patiëntengegevens mag toevertrouwen aan een informaticasysteem dat niet of niet voldoende aan de voorwaarden die zij heeft gesteld voor de beveiliging van de informaticasystemen, met inbegrip van het systeem van toegangsbeveiliging, voldoet. Dit impliceert dat dit wel doen mogelijk een schending van het strafrechtelijk gesanctioneerd beroepsgeheim met zich mee kan brengen.

Ook al zijn instellingen en beroepsbeoefenaars in de gezondheidszorg zich meer en meer bewust van de noodzaak om gezondheidsgegevens van hun patiënten op een adequate manier te beveiligen (onder andere ten gevolge van de recente ontwikkelingen op het vlak van

het e-health Platform) en gebruiken zij veelal goed beveiligde softwarepakketen, toch blijkt uit de praktijk dat het bij het eigenlijke gebruik van deze software soms misgaat. De tijdrovende inlog procedures zorgen ervoor dat beroepsbeoefenaars vaak ingelogd blijven in het programma waarin de patiëntendossiers toegankelijk zijn. Zij zijn immers (terecht) van mening dat een snelle en kwaliteitsvolle zorgverlening voorrang heeft op de vereisten naar informatieveiligheid. Zoals hieronder besproken stellen zij zich en/of de instelling waar zij tewerkgesteld zijn, hiermee echter bloot aan verschillende mogelijke sancties en aansprakelijkheden.

Ook al zijn instellingen en beroepsbeoefenaars in de gezondheidszorg zich meer en meer bewust van de noodzaak om gezondheidsgegevens van hun patiënten op een adequate manier te beveiligen (onder andere ten gevolge van de recente ontwikkelingen op het vlak van het e-health Platform) en gebruiken zij veelal goed beveiligde softwarepakketen, toch blijkt uit de praktijk dat het bij het eigenlijke gebruik van deze software soms misgaat. De tijdrovende inlog procedures zorgen ervoor dat beroepsbeoefenaars vaak ingelogd blijven in het programma waarin de patiëntendossiers toegankelijk zijn. Zij zijn immers (terecht) van mening dat een snelle en kwaliteitsvolle zorgverlening voorrang heeft op de vereisten naar informatieveiligheid. Zoals hieronder besproken stellen zij zich en/of de instelling waar zij tewerkgesteld zijn, hiermee echter bloot aan verschillende mogelijke sancties en aansprakelijkheden. De producten en diensten die Imprivata aanbiedt, laten de zorgverlener toe beide belangen, nl. snelle zorgverlening en adequate gegevensbescherming, te combineren.

JCI/NIAZ Quality-Accreditatie

Adequate gegevensbeveiliging maakt tevens deel uit van de internationale accreditatieschemas voor ziekenhuizen zoals ontwikkeld door de "Joint Commission International" (JCI) en het "Nederlands Institutuut voor Accreditatie in de Zorg" (NIAZ). Deze schemas bevatten ziekenhuisbrede kwaliteitsstandaarden. Door deelname aan dergelijke externe accreditatiesystemen worden Vlaamse ziekenhuizen vrijgesteld van systeemtoezicht door de Zorginspectie en zijn zij enkel onderworpen aan een beperkter "nalevingstoezicht" (Omzendbrief 16/200 van Vlaams Minister van Welzijn, Volksgezondheid en Gezin). Momenteel zitten 60 van de 65 Vlaamse Ziekenhuizen in het NIAZ or JCI traject en hebben reeds 4 Vlaamse ziekenhuizen een JCI accreditatie bekomen.

Kwalitatief informatiebeheer is een centrale peiler om accreditatie te bekomen. Ziekenhuizen dienen, ingevolge de NIAZ standaard, een beleid vast te leggen omtrent de beschikbaarheid en beveiliging van informatie dat voldoet aan: (i) vertrouwelijkheid (bescherming tegen onbevoegde kennisname), (ii) integriteit (waarborg tegen verlies of ongecontroleerde wijziging of toevoeging), en (iii) beschikbaarheid (gebruikers kunnen er op elk gewenst moment bij) (Deel 422.02 NIAZ Standaard). Bij het uitvoeren van certificatieaudits inzake informatiebeheer berust het NIAZ zich op de NEN 7510-norm inzake het organiseren en borgen van informatiebeveiliging binnen een zorginstelling. Ziekenhuizen dienen ondermeer toe te zien dat specifieke toegangsmaatregelen worden genomen met betrekking tot informatiesystemen:
- Toegangsrechten van werknemers, ingehuurd personeel en externe gebruikers dient te worden ingetrokken bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na wijziging te worden aangepast (NEN 7510, 8.3.3.).
- Taken en verantwoordelijkheidsgebie-

den behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen (NEN 7510, 10.1.3).
- Onbeheerde gebruikersapparatuur dient passend te worden beschermd: er dient te worden voorzien in technologische beveiliging om actieve sessies automatisch te beveiligen bij beëindiging en apparatuur te vergrendelen tegen onbevoegd gebruik (NEN 7510, 11.3.2. en 11.3.3.).
- Passende authenticatiemethoden dienen te worden gebruikt om toegang van gebruikers op afstand te beheren. Authenticatie van gebruikers op afstand kan worden gerealiseerd door middel van bijvoorbeeld cryptografische technieken, "hardware tokens" of een "challenge/response"-protocol (NEN 7510, 11.4.2)

De JCI standaard bevat analoge vereisten, zoals:
- Het waarborgen van informationele privacy, confidentialiteit en beveiliging – met inbegrip van gegevensintegriteit;
- Het evalueren en testen van technologie ter verwerking van gezondheidsinformatie, bijvoorbeeld aan de hand van privacy impact assessments;
- Het trainingen inzake gegevensbeheer van het management en ander personeel dat in contact komt met gezondheidsinformatie.

Bijzonder is vast te stellen dat er specifiek aandacht dient te worden besteedt aan het nemen van maatregelen ter voorkoming van ongeoorloofde toeging en gebruik van informatie. Meer in het bijzonder wordt van ziekenhuizen vereist dat zij (i) bepalen wie toegang heeft tot specifieke klinische patientendossiers; en (ii) er wordt bijgehouden wanneer deze gerechtigden wijzigingen of "entries" in het dossier hebben geregistreerd, met bijhorende tijdsbepaling (Deel MOI. 11 JCI Standaard).

De producten die Imprivata aanbiedt incorporeren de specifieke vereisten inzake authenticatie en combineren robuste toegangsbeveiliging met gebruiksvriendelijkheid. Hierdoor wordt de drempel tot effectieve gegevensbeveiliging substantieel verlaagd.

Risico's op handhaving bij onvoldoende beveiliging

Wanneer instellingen en beroepsbeoefenaars in de gezondheidszorg hun plicht tot adequate informatiebeveiliging niet naleven, kunnen zij onderworpen worden aan strafsancties en eventueel tuchtsancties. Daarnaast kunnen zij tevens burgerrechtelijk aansprakelijk worden gehouden voor de schade die een patiënt lijdt ten gevolge van ongeoorloofde toegang tot en verwerking van zijn of haar gegevens. Ook bestuurders van zorginstellingen kunnen in bepaalde gevallen burgerrechtelijke en strafrechtelijke aansprakelijkheid oplopen.

Zoals hierboven uiteengezet komen de verplichtingen aangaande beveiliging van patiëntengegevens in patiëntendossiers voort uit verschillende (rechts) bronnen. Dit brengt met zich mee dat er ook een ruim scala van handhavingsacties mogelijk zijn.

De niet-naleving van de hierboven geschetste verplichtingen inzake het implementeren van gepaste technische en organisatorische beveiligingsmaatregelen uit de Privacywet kan leiden tot strafrechtelijke sancties. Meer bepaald kan, naast een aantal bijkomende strafmaatregelen, een strafrechtelijke geldboete worden opgelegd van 600 euro tot 120.000 euro. In geval van een tweede veroordeling kan er zelfs een boete van 600 euro tot 600.000 euro worden opgelegd en/of een gevangenisstraf van 3 maanden tot twee jaar. De Privacycommissie heeft de bevoegdheid om bij het vaststellen van een inbreuk op de Privacywet hiervan aangifte te doen bij de bevoegde procureur des Konings. De aankomende Europese Verordening gegevensbescherming zal bij inwerkingtreding bovendien het risico van hoge boetes vergroten. Het huidige voorstel voorziet in boetes tot 1 miljoen euro of 2% van de wereldwijde omzet van de overtreder. Het Europees parlement is voorstander van veel hogere boetes, namelijk tot 100 miljoen euro of 5% van de wereldwijde omzet van de overtreder.

Daarnaast kan het toevertrouwen van gegevens die beschermd zijn door het beroepsgeheim aan informaticasystemen dat niet of niet voldoende aan de voorwaarden betreffende de beveiliging van de informaticasystemen voldoet, mogelijk een schending van het beroepsgeheim vormen. Schending van het beroepsgeheim kan gesanctioneerd worden met gevangenisstraf van acht dagen tot zes maanden en met een geldboete van 600 euro tot 3.000 euro.

Naast het mogelijk oplopen van strafrechtelijke sancties zijn bepaalde beroepsbeoefenaars in de gezondheidszorg ook onderworpen aan mogelijke tuchtrechtelijke sancties wanneer zij patiëntengegevens niet op een zorgvuldige en veilige manier bewaren.

Verder kan de instelling of beroepsbeoefenaar van de gezondheidszorg ook burgerrechtelijk aansprakelijk worden gehouden voor de schade die iemand heeft geleden ten gevolge van het niet-naleven van wettelijke voorschriften aangaande informatiebeveiliging opgelegd door of krachten de Privacywet. De instelling of beroepsbeoefenaar in de gezondheidszorg die verantwoordelijk is voor de verwerking van de patiëntengegevens is enkel van deze aansprakelijkheid ontheven indien hij of zij het bewijs kan leveren dat het feit waaruit de schade is ontstaan niet aan hem of haar kan worden toegerekend. Het implementeren van een adequate techniek voor toegangsbeveiliging kan het voeren van dit bewijs vergemakkelijken. Naast de algemene burgerrechtelijke aansprakelijkheid die een instelling of beroepsbeoefenaar heeft voor schade berokkend door personen die zij aangesteld heeft, veroorzaakt tijdens de

uitvoering van hun werk, voorziet de Patiëntenrechtenwet specifiek dat een ziekenhuis aansprakelijk is voor de tekortkomingen begaan door beroepsbeoefenaars die er werkzaam zijn, ook wanneer deze er niet op basis van een arbeidsovereenkomst of statutaire benoeming werkzaam zijn (tenzij de patiënt voorafgaandelijk van het tegendeel werd geïnformeerd). Naast deze specifieke aansprakelijkheidsregels blijven de algemene regels van contractuele en buitencontractuele aansprakelijkheid onverkort gelden.

Naast de mogelijke handhavingsacties in geval van niet adequate bescherming van patiëntendossiers, dient men ook rekening te houden met de reputatieschade die uit berichtgeving hieromtrent (bv. in het geval van een gegevenslek) kan voortvloeien. Vertrouwen tussen de patiënt en de instelling of beroepsbeoefenaar in de gezondheidszorg is essentieel. Schending van dit vertrouwen kan dan ook verstrekkende gevolgen hebben.

Aansprakelijkheid bestuurders

Naast de aansprakelijkheid van de zorginstelling als rechtspersoon, kunnen bestuurders in bepaalde gevallen persoonlijk aansprakelijk worden gesteld voor het al dan niet correct uitvoeren van hun bevoegdheden met betrekking tot het organiseren van de informatiebeveiliging in de zorginstelling. De straf- en/of burgerrechtelijke aansprakelijkheid treft dus niet noodzakelijk enkel de zorginstelling, maar eveneens de persoon en het vermogen van de bestuurder zelf.

Statuut zorginstellingen
De rechtsvorm van zorginstellingen is niet wettelijk bepaald in België. In de praktijk nemen echter de meeste zorginstellingen de rechtsvorm van een vereniging zonder winstoogmerk (hierna: "vzw") aan.

Bij gebrek aan enige specifieke regelgeving omtrent aansprakelijkheid van bestuurders van zorginstellingen gelden de algemene regels voor de aansprakelijkheid van de bestuurders van een vzw.

Algemeen
Ook al is de zorginstelling in principe aansprakelijk voor de handelingen van haar bestuurders voor zover deze binnen de grenzen van hun mandaat handelen, kunnen bestuurders in bepaalde gevallen persoonlijk burgerrechtelijk en strafrechtelijk aansprakelijk gesteld worden voor hun fouten. Het gaat hier dan in principe om een individuele aansprakelijkheid (dit is geen vermoeden van solidariteit).

Bestuurders kunnen zowel burgerrechtelijk als strafrechtelijk persoonlijk aansprakelijk worden gesteld voor een tekortkoming inzake de voornoemde vereisten inzake gegevensbeveiliging en de daaruit voortvloeinde schade.

Burgerrechtelijke aansprakelijkheid van de bestuurder
Zowel de zorginstelling als iedere derde (in casu bv. een patiënt) die schade heeft geleden ten gevolge van een foutief (niet) handelen van een bestuurder, kan onder bepaalde voorwaarden de door hem of haar geleden schade rechtstreeks op het persoonlijke vermogen van de bestuurder verhalen. In sommige gevallen zal het feit dat een derde kan aantonen dat de wettelijk vereiste beveiligingsmaatregelen niet werden genomen tot de vaststelling van aansprakelijk leiden. De overige voorwaarden verschillen naargelang het gaat om contractuele dan wel buitencontractuele aansprakelijkheid:

- Buitencontractuele aansprakelijkheid
Wanneer een bestuurder van de zorginstelling buiten zijn mandaat handelt en hierbij niet handelt zoals een normaal en redelijke bestuurder in dezelfde omstandigheden of een wettelijke verplichting schendt, kan eender welke persoon (bv. een patiënt) die ten gevolge van dit handelen schade heeft geleden, deze schade verhalen op het persoonlijk vermogen van de bestuurder.

De zorginstelling kan bovendien de bestuurder ook burgerrechtelijk aansprakelijk stellen wanneer deze zijn mandaat foutief uitoefent en handelingen stelt die een redelijke bestuurder niet zou stellen of die niet in overeenstemming zijn met de wet.

- Contractuele aansprakelijkheid
Naast de hierboven beschreven mogelijkheid voor de zorginstelling om de bestuurder, los van enig contract, aan te spreken voor schade die de instelling heeft geleden ten gevolge van zijn of haar persoonlijke fout, heeft de zorginstelling tevens de mogelijkheid om haar bestuurder persoonlijk contractueel aansprakelijk te stellen indien de betrokken bestuurder zijn of haar mandaat

niet correct heeft vervuld en de zorginstelling hierdoor schade heeft geleden.

Strafrechtelijke aansprakelijkheid
Naast burgerrechtelijke aansprakelijkheid, kan een bestuurder persoonlijk strafrechtelijke aansprakelijkheid oplopen wanneer hij persoonlijk een strafrechtelijke inbreuk begaat tijdens het uitoefenen van zijn mandaat bij de zorginstelling. Hiertoe dient het openbaar ministerie aan te tonen dat de strafrechtelijke inbreuk persoonlijk en individueel aan de bestuurder toegerekend kan worden.

In de praktijk zullen bestuurders vaak aansprakelijk worden gesteld voor handelingen waartoe zij het bevel hebben gegeven, zonder dat zij de strafrechtelijke inbreuk persoonlijk gesteld hebben. De persoon die persoonlijk de strafrechtelijke inbreuk gepleegd heeft, wordt hierdoor vaak gevrijwaard. Zoals hierboven in het stuk omtrent de risico's op handhaving werd uiteengezet, kan de zorginstelling vanzelfsprekend ook zelf strafrechtelijke aansprakelijkheid oplopen wanneer de voorschriften betreffende de beveiliging van patiëntendossiers niet worden nageleefd.