wikkeling van een meer algemeen EPD. Daarbij is het zinvol om goed na te denken over de prioriteiten voor de volgende onderdelen, zoals hierboven ook aangegeven. En bij dit alles blijft natuurlijk gelden, dat een intensieve betrokkenheid van de zorgverleners essentieel is.

Literatuur

1. Relevante EU-projecten: GEHR, Synapses, RICHE, NUCLEUS, 14C, STAR; Relevante ontwerpnormen: CEN ENV 13606: Electronic Health Record Communication ISO 18308: Requirements for an Electronic Health Record Reference Architecture.
2. Lloyd D, Kalra D. EHR Requirements, in: Blobel B, Pharow P (Eds.): "Advanced Health Telematics and Telemedicine", IO Press 2003, Amsterdam.
3. Zwetsloot-Schonk B, et al.: Patiëntgegevens te Kijk; de verantwoordelijkheid van de behandelaar en toegankelijkheid tot het EPD; in Proceedings MIC 2001 en Proceedings MIC 2003 (VMBI, Zeist, www.vmbi.nl).
4. Zie bijvoorbeeld: www.hl7.org
5. Zie bijvoorbeeld: www.nictiz.nl

Ned Tijdschr Klin Chem Labgeneesk 2004; 29: 219-225

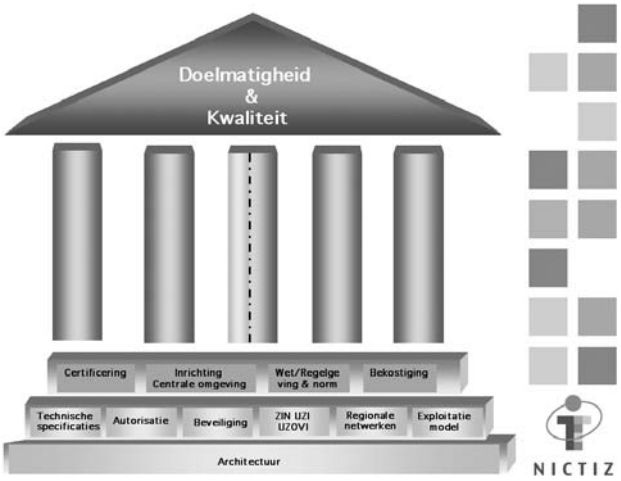
Juridische aspecten van het EPD

T.F.M. HOOGHIEMSTRA

Bij het uitwisselen van laboratoriumuitslagen worden persoonsgegevens verwerkt waardoor de bepalingen en beginselen van privacywetgeving en patiëntenrecht gelden. In dit artikel worden deze bepalingen en beginselen in het perspectief van het EPD geplaatst. Betoogd wordt dat de klinisch chemicus door een medische behandelaar rechtstreeks bij de behandeling betrokken kan worden. Ook wordt een praktische oplossing gegeven voor het toestemmingsvraagstuk bij cumulatieve rapportage. De auteur beveelt de beroepsgroep aan om concreet invulling te geven aan de algemene normen in de privacywetgeving en de patiëntenrechten voor het verantwoord omgaan met (medische) persoonsgegevens door klinisch chemici.

Inleiding

Bij laboratoriumautomatisering is sprake van een informatieverwerkend proces. Voor de verwerking van (laboratorium)gegevens geldt wet- en regelgeving. In het bijzonder wetgeving ter bescherming van persoonsgegevens, zoals de Wet bescherming persoonsgegevens (WBP) en patiëntenrecht, zoals de Wet geneeskundige behandelingsovereenkomst (WGBO). Recente veranderingen in de zorg hebben veel grotere gevolgen voor laboratoriumautomatisering dan de recente veranderingen in wet- en regelgeving. Belangrijke veranderingen in de zorg zijn schaalvergroting, transmuralisering, vraaggestuurde zorg, hogere kwaliteitseisen en hogere doelmatigheidseisen. Deze veranderingen kunnen worden ondersteund door ICT, onder andere via de totstandkoming van een (landelijk) elektronisch patiëntendossier (EPD). Zo stelt het Nationaal ICT Instituut in de Zorg (NICTIZ) zich, namens vrijwel alle zorgpartijen, ten doel om als eerste stap op weg naar het EPD een landelijk medicatiedossier te realiseren. Daarbij gaat het overigens dus ook over labautomatisering, aangezien medicatiegegevens en laboratoriumgegevens een grote verwantschap vertonen. Uitgaande van het gezamenlijke streven naar kwaliteit en doelmatigheid in de zorg bestaat het werkveld van NICTIZ de komende jaren uit hetgeen in onderstaande tempel is weergegeven.



De juridische aspecten van het omgaan met medische gegevens zijn minder aan verandering onderhevig. Het medisch beroepsgeheim is al zo oud als de eed van Hippocrates en de wetgeving ter bescherming van persoonsgegevens draait nationaal en Europees al decennia om transparantie, doelbinding, veiligheid en rechten van de betrokkene c.q. de patiënt/cliënt. De komst van het EPD vergt een paradigmashift in denken en doen. Thans is het uitgangspunt nog veelal dat

Manager Juridische Zaken bij het Nationaal ICT Instituut in de Zorg (NICTIZ)

Correspondentie: Mr. Drs. T.F.M. Hooghiemstra, NICTIZ, Postbus 262, 2260 AG Leidschendam.
E-mail: hooghiemstra@nictiz.nl

de zorgverlener een in beginsel gesloten dossier beheert waarbij hij zelf een grote mate van vrijheid heeft hoe hij de gegevens bijhoudt en aan wie hij, op verzoek, gegevens uit dat dossier verstrekt. Na realisatie van het (virtueel) EPD is het uitgangspunt een in beginsel open dossier waar alle bij de behandeling van de patiënt betrokken zorgverleners toegang toe kunnen hebben, mits aan een aantal voorwaarden is voldaan. Gegevens kunnen bij een EPD niet alleen meer worden verstrekt, maar ook op afstand door een andere zorgverlener worden opgehaald. Ondanks deze paradigmashift blijven de juridische spelregels vrijwel gelijk. Door de veranderde omstandigheden vergen die spelregels zo nu en dan echter wel een vernieuwde interpretatie. Bijvoorbeeld ten aanzien van: de rechten van de patiënt; de plichten van de zorgverlener; identificatie; authenticatie; autorisatie; aansprakelijkheid en beveiliging. Dergelijke juridische aspecten van het EPD zijn onderzocht door het Juridisch Laboratorium van Zorgonderzoek Nederland (ZON). De resultaten zijn in de volgende paragraaf samengevat.

Resultaten Juridisch Laboratorium EPD

Tussen 2000 en 2002 heeft het Juridisch Laboratorium in het kader van het programma Informatie- en Communicatietechnologie in de Zorg van ZON aandacht besteed aan de juridische aspecten van het EPD en tegelijkertijd juridische ondersteuning geboden aan de professionals die op door ZON ingestelde proefsites EPD's in de praktijk ontwikkelden.
Het Juridisch Laboratorium heeft naast een algemene rapportage, een vijftal rapporten gepubliceerd over verschillende juridische aspecten van het EPD, te weten patiënten- en zorgverlenersidentificatie, verwijsindexen, de positie van de patiënt bij raadpleging van patiëntengegevens, aansprakelijkheid en verantwoordelijkheid en beveiliging. Deze publicaties kunt u vinden via de website van NICTIZ: www.nictiz.nl. door rechts onderaan op de website het logo van ZonMw aan te klikken.

Patiënten- en zorgverlenersidentificatie

Voor een goede zorgverlening is van belang dat gegevens over één en dezelfde patiënt met elkaar in verband kunnen worden gebracht, zonder dat verwarring optreedt met de gegevens van een ander. Daarnaast moet vastgesteld kunnen worden of de hulpverlener op het bewuste moment wel bevoegd is om toegang te krijgen tot de patiëntengegevens. Veel gebruikte middelen hiertoe zijn een nummer voor de patiënt en een pasje of gebruikersnaam/wachtwoordcombinatie voor de hulpverlener. Biometrie is een nieuwe mogelijkheid om op basis van unieke lichaamskenmerken de authenticiteit vast te stellen.
Patiëntennummers zijn persoonsnummers en persoonsnummers zijn persoonsgegevens, waarop de WBP van toepassing is. Patiëntennummers zijn in vijf soorten te onderscheiden: 1. bestaande wettelijk voorgeschreven nummers (sociaal-fiscaal-nummer, Gemeentelijke Basis Administratienummer) en in de toekomst (1-1-2006) het Burger Service Nummer, 2. versleuteld bestaand wettelijk nummer, 3. een willekeurig eigen nummer voor de gezondheidszorg. 4. lokale of regionale zorgnummers, en 5. ketennummers. Biometrische gegevens zijn ook persoonsgegevens. Patiëntennummers en biometrische gegevens moeten te allen tijde voldoen aan de beginselen voor gegevensverwerking die in paragraaf 5 nader worden uitgewerkt. Toetsing aan deze beginselen leidt tot de conclusie dat naarmate het bereik van het patiëntenidentificatienummer groter is, het risico voor schending van (een van) deze beginselen toeneemt. Biometrie kan enerzijds leiden tot een betere beveiliging van persoonsgegevens, maar kan een bedreiging voor de genoemde beginselen worden wanneer de biometrische kenmerken worden gebruikt voor verschillende handelingen, zodat iemands levensloop kan worden gereconstrueerd. Bovendien kunnen biometrische gegevens meer informatie bevatten dan noodzakelijk is voor identificatie of authenticatie.

Verwijsindexen

Een verwijsindex is een hulpmiddel bij het uitwisselen van gegevens via verwijsinformatie. Verwijsinformatie wijst de weg naar de plaats waar een gegeven te vinden is. Bij een EPD bestaat verwijsinformatie bijvoorbeeld uit een identificerend gegeven van een patiënt en een verwijzing naar een hulpverlener.
Verwijsindexen kennen we in verschillende varianten: landelijke, regionale, lokale verwijsindexen of een verwijsindex op een zorgpas of behorende bij een bepaalde zorgketen. Bestaande voorbeelden van verwijsindexen zijn de Landelijke Centrale Middelen Registratie en het Pathologisch Landelijk Geautomatiseerd Archief (PALGA).
Vanuit juridisch oogpunt is eerst de vraag van belang of het gebruik van een verwijsindex noodzakelijk is: kan het beoogde doel niet zonder het gebruik van een verwijsindex worden gerealiseerd, bijvoorbeeld doordat de patiënt zelf zijn arts informeert? Om een virtueel EPD (landelijk) te laten functioneren zal in de praktijk echter al snel een verwijsindex noodzakelijk zijn. Mogelijke problemen zullen dan zo goed mogelijk moeten worden opgelost, zoals: zeggenschapsverlies voor hulpverleners; onduidelijke verantwoordelijkheidstoedeling; ongerechtvaardigde schendingen van het beroepsgeheim, e.d.
Wanneer een verwijsindex wordt gebruikt zijn in elk geval de WBP en de regels van het medisch beroepsgeheim van toepassing. De vraag welke gegevens vervolgens in de verwijsindex moeten worden opgenomen, kan worden beantwoord in drie stappen. (1) Is er sprake van een gerechtvaardigde inbreuk op het (medisch) beroepsgeheim? (2) Is er sprake van gezondheidsgegevens? (3) Is er sprake van een rechtmatige grondslag? Tenslotte dienen ook voldoende technische en organisatorische maatregelen getroffen te worden ter beveiliging van de patiëntengegevens die via een verwijsindex toegankelijk zijn.

De positie van de patiënt

Het rapport over de positie van de patiënt gaat over de vraag hoe in de elektronische omgeving van een

EPD vorm kan worden gegeven aan het beroepsgeheim van hulpverleners en met name hoe de zeggenschap van de patiënt over de toegankelijkheid van diens gegevens voor derden gestalte kan krijgen.
In het kader van de medische hulpverlening worden patiënten geconfronteerd met hulpverleners die (1) bepaalde informatie vragen of medewerking vragen om bepaalde informatie te genereren, (2) gevraagde en gegenereerd informatie vastleggen en (3) informatie uitwisselen met andere hulpverleners en eventuele derden. Het beroepsgeheim (de zorgplicht om vertrouwelijkheid van patiëntengegevens jegens derden te waarborgen) strekt mede ter bescherming van het algemeen belang: de onbelemmerde toegang tot gezondheidszorg. Kern van het beroepsgeheim is dat aan anderen geen herleidbare gegevens over de patiënt worden verstrekt (of anderen toegang hebben tot zulke gegevens), tenzij aan bepaalde voorwaarden is voldaan. Die voorwaarden zijn: overmacht of conflict van plichten in een noodsituatie, een wettelijk voorschrift dat tot gegevensverstrekking verplicht of de gegevensverstrekking onder bepaalde voorwaarden toelaat, of met de toestemming van de patiënt.
De eisen die vanuit een oogpunt van de zeggenschap van de patiënt aan een EPD worden gesteld zijn: (1) structurering en standaardisering van (relevante) gegevens naar gelang de hulpvraag, (2) verschillende toegangsniveaus met bijpassende toegangssleutel naar gelang de aard van de gegevens, (3) een methode om de hulpverlener die voor diagnostiek en behandeling van de patiënt elders informatie nodig heeft, kenbaar te maken waar (bij welke hulpverlener) de voor hem benodigde gegevens berusten, (4) een patiënt identificatiesysteem, (5) een systeem van autorisatie voor hulpverleners waarmee de bevoegdheid toegang te krijgen tot de voor hun taak noodzakelijke patiëntengegevens tot uitdrukking komt en (6) een bewijs van rechtmatigheid van toegang tot de informatie (op basis van 'need-to-know') op het concrete moment dat daar behoefte aan is. Die rechtmatigheid wordt mede door de patiënt bepaald.

Verantwoordelijkheid en aansprakelijkheid
Een belangrijke juridische vraag in verband met het EPD luidt: wie is inhoudelijk verantwoordelijk en juridisch aansprakelijk voor het onverhoopt onrechtmatige gebruik van patiëntengegevens in een EPD? Juridische vormen van aansprakelijkheid vloeien voort uit een diversiteit aan wet- en regelgeving. De bescherming tegen onrechtmatig gebruik van patiëntengegevens uit een EPD kan worden gebaseerd op het klachtrecht (Wet klachtrecht cliënten zorgsector), het tuchtrecht (Wet beroepen in de individuele gezondheidszorg), het burgerlijk recht in het algemeen (contractuele aansprakelijkheid, wettelijke aansprakelijkheid, aansprakelijkheid voor hulppersonen, productaansprakelijkheid), het strafrecht (Wetboek van Strafrecht) en het bestuursrecht (Kwaliteitswet zorginstellingen).
In het bijzonder is het mogelijk dat men aansprakelijk wordt gesteld op grond van de WGBO of de WBP. Vaak zal het een ziekenhuis zijn dat juridisch aansprakelijk wordt gesteld voor vermeend onrechtmatig gebruik van patiëntengegevens. Het ziekenhuis is immers veelal het centrale aansprakelijkheidsadres op grond van de WGBO ofwel de 'verantwoordelijke' als bedoeld in de WBP. Zo is een ziekenhuis veelal verantwoordelijk voor de facilitaire voorzieningen, zoals de lokale informatie-infrastructuur. Van een ziekenhuis mag bijvoorbeeld ook worden verwacht dat het zorgt voor een adequate beveiliging (versleuteling) van de uitwisseling van patiëntengegevens per e-mail. Op zijn minst kunnen richtlijnen worden opgesteld voor het gebruik van e-mail bij de uitwisseling van patiëntengegevens.
Hoewel juridisch aansprakelijk, is het mogelijk dat het ziekenhuis de geclaimde schade verhaalt op de individuele hulpverlener die verantwoordelijk is voor de inhoud van de omgang met de patiëntengegevens in het EPD. In de praktijk kunnen gevallen waarin aansprakelijkheid wordt erkend worden afgehandeld tussen de patiënt of diens gemachtigde en de beroepsaansprakelijkheidsverzekeraar van de arts of de instelling. Ook kan het zijn dat de aansprakelijkheid ligt bij de 'bewerker' (een externe organisatie waaraan taken worden uitbesteed). Daarom het advies om goede bewerkerscontracten af te sluiten.

Beveiliging
De plicht tot beveiliging van patiëntengegevens in een EPD komt voort uit een aantal juridische normen. In het kader van de geneeskundige behandeling gaat het om de algemene normen die nopen tot de inachtneming van 'de zorg van een goed hulpverlener', 'de professionele standaard' en het aanbieden van 'verantwoorde zorg'. Elementen die aan deze 'open normen' nadere invulling geven zijn bijvoorbeeld het medisch beroepsgeheim en de juridische verplichting tot het beveiligen van persoonsgegevens (zie artikel 13 WBP). Ter beveiliging van patiëntengegevens in een EPD dienen technische en organisatorische maatregelen te worden genomen. Deze maatregelen zijn bijvoorbeeld te vinden in de voornorm van het Europese normalisatie instituut Comité Européen de Normalisation (CEN) uit 1997, de Code voor informatiebeveiliging, opgesteld door het Ministerie van Economische Zaken en het Nederlandse Normalisatie Instituut (NEN) en het rapport Beveiliging van persoonsgegevens, opgesteld door het College Bescherming Persoonsgegevens (CBP), zie www.cbpweb.nl). Inmiddels is door het NEN de Nederlandse norm voor Informatiebeveiliging in de zorg gepubliceerd (NEN 7510). Het betreft een 'paraplu-norm' die op onderdelen (zoals authenticatie en autorisatie) nog nader uitgewerkt gaat worden.
De maatregelen ter beveiliging van patiëntengegevens in een EPD dienen onderdeel te zijn van een algemeen beveiligingsbeleid dat door een (groep van) organisatie(s) is vastgesteld. In die zin staat het beveiligen van medische persoonsgegevens niet op zichzelf, maar maakt het deel uit van het beleid van een instelling. Ter beveiliging van patiëntengegevens in een EPD is het tevens van belang voldoende aandacht te schenken aan technische maatregelen waar-

mee het normatieve kader kan worden versterkt. Gedacht moet worden aan biometrie, cryptografie, beveiligingsprotocollen, de elektronische handtekening, 'Privacy Enhancing Technologies' en 'Trusted Third Parties'.

Algemene rapportage
Het Juridisch Laboratorium heeft bij haar activiteiten vanuit de praktijk diverse vragen voorgelegd gekregen. Deze zijn beantwoord in de algemene rapportage van het juridisch laboratorium.

Verhouding WBP-WGBO
Uit het voorgaande blijkt dat met name de WBP en de WGBO van belang zijn om de juridische aspecten van het EPD te doorgronden. Hoe verhouden die twee wetten zich tot elkaar? Beide vullen elkaar aan. Waarbij in geval van een vermeend conflict tussen bepalingen van beide wetten als uitgangspunt geldt dat de bepaling die de patiënt de meest bescherming biedt voor gaat. Bovendien geldt op grond van artikel 9, vierde lid, WBP dat in het geval het beroepsgeheim aan de orde is, eerst naar de wetgeving gekeken moet worden die over het beroepsgeheim gaat. In casu meestal de geheimhoudingsbepaling in de WGBO. Dit onderwerp krijgt speciale aandacht in paragraaf 6. Zodra het beroepsgeheim geen probleem (meer) vormt gelden aanvullend nog de bepalingen van de WBP. Bijvoorbeeld bepalingen inzake de verantwoordelijke, de bewerker, beveiligingsverplichting, informatie aan patiënt; juistheid; volledigheid; melding en inzagerecht (inclusief bijbehorende prijs).

WGBO en EPD
In de WGBO zijn de patiëntenrechten vastgelegd. Welke invloed hebben deze rechten op het EPD? De belangrijkste rechten worden hier met het betreffende artikel opgesomd en voorzien van commentaar in het licht van het EPD:

Artikel 7:453 BW: "*De hulpverlener moet bij zijn werkzaamheden de zorg van een goed hulpverlener in acht nemen en handelt daarbij in overeenstemming met de op hem rustende verantwoordelijkheid, voortvloeiende uit de voor hulpverleners geldende professionele standaard."* Bij een EPD is het pleitbaar dat wanneer het met behulp van ICT redelijkerwijs mogelijk is om bij een andere zorgverlener elektronisch gegevens te verkrijgen die noodzakelijk zijn voor een goede hulpverlening het tegelijkertijd de plicht inhoudt om van die mogelijkheid gebruik te maken c.q. mee te werken, tenzij de patiënt kenbaar heeft gemaakt hier geen prijs op te stellen.

Artikel 7:454 BW*:*
1. *De hulpverlener richt een dossier in met betrekking tot de behandeling van de patiënt. Hij houdt in het dossier aantekening van de gegevens omtrent de gezondheid van de patiënt en de te diens aanzien uitgevoerde verrichtingen en neemt andere stukken, bevattende zodanige gegevens, daarin op, een en ander voor zover dit voor een goede hulpverlening aan de patiënt noodzakelijk is.*
2. *De hulpverlener voegt desgevraagd een door de patiënt afgegeven verklaring met betrekking tot de in het dossier opgenomen stukken aan het dossier toe.*
3. *Onverminderd het bepaalde in artikel 455, bewaart de hulpverlener de bescheiden, bedoeld in de vorige leden, gedurende tien jaren, te rekenen vanaf het tijdstip waarop zij zijn vervaardigd, of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit.*
Lid 1 gaat over de dossierplicht van de zorgverlener**.** Wat precies onder het dossier moet worden verstaan en wat er precies in moet zitten staat niet in de wet. Bij een virtueel EPD is de vraag wat allemaal tot het dossier gerekend zou moeten worden. Volgens deze bepaling alles wat voor een goede hulpverlening noodzakelijk is. Het is wenselijk dat de beroepsgroep aangeeft wat noodzakelijk is.
Lid 2 gaat over het aanvullingsrecht van de patiënt. Ook een EPD zal die mogelijkheid moeten bieden.
Lid 3 gaat over de bewaartermijn. ICT maakt het mogelijk gegevens veel compacter op te slaan, zodat ruimtegebrek geen problemen meer hoeft op te leveren. Vroeg of laat zal echter toch een keuze gemaakt moeten worden of en zo ja welke gegevens bewaard moeten worden. Ook zal men de gegevens te zijner tijd willen kunnen selecteren. Dat kan de computer alleen als van te voren bijgehouden wordt hoe lang gegevens en welke soorten gegevens bewaard worden. Tot op heden is de software van ICT in de zorg daar nog niet op ingesteld.

Artikel 7:455 BW:
1. *De hulpverlener vernietigt de door hem bewaarde bescheiden, bedoeld in artikel 454, binnen drie maanden na een daartoe strekkend verzoek van de patiënt.*
2. *Lid 1 geldt niet voor zover het verzoek bescheiden betreft waarvan redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de patiënt, alsmede voor zover het bepaalde bij of krachtens de wet zich tegen vernietiging verzet.*
Bij artikel 7:454 lid 1 was de vraag wat allemaal tot het dossier behoort, met name bij een virtueel EPD. In het verlengde daarvan is hier de vraag wat er allemaal vernietigd moet worden als een patiënt om vernietiging van zijn elektronisch dossier vraagt. Bovendien moet de software van ICT in de zorg het mogelijk (gaan) maken om aan het vernietigingsrecht te voldoen.

7:456 BW:
De hulpverlener verstrekt aan de patiënt desgevraagd zo spoedig mogelijk inzage in en afschrift van de bescheiden, bedoeld in artikel 454. De verstrekking blijft achterwege voor zover dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander. De hulpverlener mag voor de verstrekking van het afschrift een redelijke vergoeding in rekening brengen. Inzage kan ook elek-

tronisch vorm gegeven worden, bijvoorbeeld via een publiekszuil in een ziekenhuis en, zodra de identiteit van patiënten op afstand betrouwbaar te verifiëren is, ook thuis vanuit de luie stoel. Zodra dat redelijkerwijs kan, zal dit recht van de patiënt ook technisch en organisatorisch vormgegeven moeten worden.

Een ander belangrijk recht in de WGBO betreft het beroepsgeheim. Dit wordt als speciaal onderwerp in paragraaf 6 behandeld. Alvorens het beroepsgeheim te behandelen komen eerst de relevante begrippen en beginselen uit de WBP aan bod.

WBP en EPD
In deze paragraaf komen eerst vier relevante begrippen uit de WBP aan bod en vervolgens de beginselen die de WBP (en de Europese richtlijn waar de WBP een implementatie van is) samenvatten.

a) Persoonsgegeven: *elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;*
b) Verwerking van persoonsgegevens: *elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens* (kort gezegd: alles van verzamelen tot en met vernietigen);
c) Verantwoordelijke: *de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt* (bijvoorbeeld de directie van een ziekenhuis);
d) Bewerker: *degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.* Per definitie werkt de bewerker buiten de organisatie van de verantwoordelijke die de persoonsgegevens onder zijn verantwoordelijkheid heeft en de bewerker een opdracht heeft gegeven, bijvoorbeeld een ICT-onderhoudsbureau, een extern archief of een salarisadministratiebureau).

De Europese en (toekomstige) nationale spelregels voor de omgang met persoonsgegevens zijn vervolgens samen te vatten in de volgende zes beginselen.

1. Transparantie van de gegevensverwerking
Het gaat hierbij om het principe dat iemand op de hoogte hoort te zijn van het feit dat gegevens over hem worden verwerkt en voor welk doel. Dit raakt de verzameling en het gebruik van de gegevens en de mogelijkheden tot kennisneming daarvan door de patiënt.

2. Doelbinding
Het beginsel van doelbinding vereist dat de persoonsgegevens slechts worden verzameld voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden, dat niet meer gegevens worden verwerkt dan voor die doeleinden noodzakelijk zijn en dat deze gegevens niet worden gebruikt voor doeleinden die daarmee niet verenigbaar zijn. Het is belangrijk dat niet meer gegevens verwerkt worden dan noodzakelijk. Niet alleen vanwege de bescherming van de patiënt, maar ook voor de beheersbaarheid van de gegevensstromen.

3. Rechtmatige grondslag
Een rechtmatige grondslag voor de verwerking van persoonsgegevens kan zijn:
- toestemming van de patiënt. Bij toestemming gaat het steeds om een vrije gerichte toestemming die op toereikende informatie berust;
- de uitvoering van een overeenkomst waarbij de patiënt partij is. Bij het medisch dossier zal het meestal gaan om overeenkomst in de zin van de WGBO. Klinisch chemici vallen niet rechtstreeks onder de WGBO, maar kunnen daarbij wel betrokken worden door huisartsen en medisch specialisten.
- de nakoming van een wettelijke verplichting, zoals de WGBO;
- een vitaal belang (bijvoorbeeld zwaarwegende geneeskundige redenen);
- de uitvoering van een publiekrechtelijke taak door een bestuursorgaan;
- een gerechtvaardigd belang, terwijl het belang van de patiënt niet wordt geschaad

4. Kwaliteit van gegevens
De gegevens moeten toereikend, ter zake dienend en niet overmatig zijn in relatie tot het doel waarvoor ze worden verwerkt. De gegevens dienen ook nauwkeurig te zijn en zonodig te worden bijgewerkt. In dit verband dienen alle redelijke maatregelen te worden getroffen om tekortkomingen te herstellen.

5. Beveiliging en Privacy Enhancing Technologies
Dit beginsel is reeds behandeld in paragraaf 2.5.

6. Verbodsregime bijzondere gegevens
Verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden, tenzij de wetgever daarvoor een ontheffing heeft verleend in de WBP. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
Bij ICT-toepassingen in de gezondheidszorg is er uiteraard een ontheffing op het verbod om gezondheidsgegevens te verwerken voor hulpverleners, instellingen of voorzieningen in de gezondheidszorg. Gezondheidsgegevens zijn alle gegevens die de lichamelijke of geestelijke gezondheid van een persoon betreffen.

Beroepsgeheim en de gevolgen voor laboratoriumautomatisering

In dit artikel ligt de focus op de bepaling inzake beroepsgeheim in de WGBO. Volledigheidshalve zij opgemerkt dat het beroepsgeheim echter ook geregeld is in artikel 272 Wetboek van Strafrecht, artikel 88 Wet Beroepen Individuele Gezondheidszorg, in ongeschreven recht, in jurisprudentie et cetera.

De tekst inzake beroepsgeheim in de WGBO luidt als volgt:
7: 457 BW:
***1**. […] draagt de hulpverlener zorg, dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden, bedoeld in artikel 454, worden verstrekt dan met toestemming van de patiënt. […]De verstrekking kan geschieden zonder inachtneming van de beperkingen, […]indien het bij of krachtens de wet bepaalde daartoe verplicht.*
2. Onder anderen dan de patiënt zijn niet begrepen degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de hulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden. […]

Doorbreken van het beroepsgeheim zonder toestemming van patiënt is gerechtvaardigd als het gaat om verstrekking aan de vervanger van de behandelende zorgverlener; aan een rechtstreeks bij de behandeling betrokkene (indien noodzakelijk) of op basis van een wet. Verder mogen gegevens zonder toestemming verstrekt worden in geval van een noodtoestand in de zin van artikel 40 Wetboek van Strafrecht als de zorgverlener in gewetensnood raakt vanwege een conflict van plichten. Met andere woorden: nood breekt wet.
Overigens is toestemming in de WGBO vormvrij. Volgens de rechtsgeleerde literatuur mag bijvoorbeeld uitgegaan worden van stilzwijgende toestemming als toegang noodzakelijk is voor een andere behandeling.

Voor autorisatie bij EPD's is het gevolg van bovenstaande bepaling dat er drie cumulatieve voorwaarden zijn: 1) bevoegdheid (op basis van een bevoegdheidsprofiel); 2) rechtmatigheid (bijvoorbeeld op basis van toestemming van de patiënt); 3) noodzakelijkheid. Daarnaast is het van belang dat eventueel onrechtmatige toegang te traceren is via logging, met name als gebruik gemaakt wordt van het noodprotocol.

Gevolgen voor labsystemen
Het voorgaande leidt voor labsystemen ten minste tot de volgende twee vragen:
1. Kan de klinisch chemicus beschouwd worden als rechtstreeks bij de behandeling betrokken zorgverlener?
2. Is voor (cumulatieve) opslag in labsystemen toestemming van de patiënt nodig en zo ja in welke vorm?

Ad 1) Het feit dat de klinisch chemicus geen behandelingsovereenkomst in zin van de WGBO kan sluiten betekent nog niet dat een huisarts of een medisch specialist een klinisch chemicus nooit in consult kan roepen bij de behandeling van een patiënt.
Een klinisch chemicus kan betrokken worden bij de uitvoering van de behandelingsovereenkomst die de huisarts of de specialist met de patiënt heeft gesloten voorzover het de klinisch chemische handelingen betreft. Dit mag als aan bepaalde voorwaarden wordt voldaan. Naar analogie van de randvoorwaarden die de Registratiekamer (thans CBP) destijds stelde bij medicatiebewaking door centrale patiëntenadministraties om een apotheker als rechtstreeks bij de behandeling betrokkene te kunnen worden aangemerkt zijn de volgende randvoorwaarden geformuleerd:
- is het gebruikelijk in de beroepsgroep van huisartsen, respectievelijk medisch specialisten, om de klinisch chemicus op deze wijze bij de behandelingsovereenkomst te betrekken?
- zijn er redelijke alternatieven voor de huisartsen en medisch specialisten?
- heeft de huisarts of medisch specialist voldoende zeggenschap?
- zijn er privacybeschermende maatregelen getroffen?
- is deze werkwijze kenbaar voor de patiënt en bezwaar mogelijk?
- is deze werkwijze in het belang van de patiënt?
- is de omvang van de gegevensuitwisseling beheersbaar?

Pleitbaar is het om te stellen dat bij direct aan de behandeling gerelateerde informatie de hiervoor genoemde randvoorwaarden bevestigend beantwoord kunnen worden.
In dat geval is geen voorafgaande toestemming van de patiënt vereist, wel kan de patiënt desgewenst bezwaar maken.

Ad 2) De toestemmingsvraag is in het voorgaande reeds ten dele beantwoord. Maar in de praktijk wordt bij labsystemen ook vaak gebruik gemaakt van zogenaamde cumulatieve rapportages waar ook informatie in zit die meestal niet noodzakelijk is voor de betreffende behandelaar bij de behandeling van zijn patiënt. Strikt genomen zou in dat geval de betreffende behandelaar (die is in eerste instantie verantwoordelijk en aansprakelijk te stellen!) er voor moeten zorgen dat de patiënt vooraf toestemming geeft voor het verwerken van eerdere gegevens die opgeslagen liggen in het laboratorium. Bij de parlementaire behandeling van de WGBO (met name in relatie tot de privacywetgeving) is over het toestemmingsvereiste bij gegevens verstrekking door de regering gewaarschuwd om onnodige formalisering te voorkomen en voorliggende vragen genuanceerd te behandelen. Gelet op het feit dat cumulatieve rapportages (gedeeltelijk) voor de behandelaar van belang kunnen zijn om tot een goede diagnose te komen en het ook gebruikelijk is hiervan gebruik te maken is het verdedigbaar om er voor te kiezen dat bij de verwijzer en/of bij het laboratorium foldermateriaal voor de patiënt ligt met heldere en relevante informatie. Daarin moet dan ook

staan dat gebruik gemaakt wordt van cumulatieve rapportages van de laboratoria, tenzij de patiënt hiervoor geen toestemming geeft en dit kenbaar maakt bij de behandelaar. Een richtlijn voor de behandelaren zou verder moeten zijn dat zij, als dat redelijkerwijs mogelijk is, ook mondeling moeten informeren en om toestemming moeten vragen.

Recente en toekomstige wet- en regelgeving rond het EPD

Volledigheidshalve wordt aan het einde van dit artikel over juridische aspecten van EPD's ook even vooruit geblikt naar juridische ontwikkelingen die relevant kunnen zijn voor klinisch chemici.

In mei 2003 is de Wet elektronische handtekening van kracht geworden. Deze wet is met name van belang zodra in de nabije toekomst zorgverleners betrouwbaar en onweerlegbaar gegevens via internet willen c.q. moeten uitwisselen. De wet beschrijft aan welke voorwaarden certificaten voor zorgverleners moeten doen alvorens ze door de OPTA gekwalificeerd worden.

Er is een wet op het Zorg Identificatie Nummer (ZIN) in voorbereiding die vermoedelijk in de tweede helft van dit jaar in de Tweede Kamer zal worden behandeld. Deze wet gaat niet alleen het zorgnummer regelen, maar ook voorwaarden stellen aan de gebruikers van dat nummer. Voor zorgverleners is daarbij het unieke zorgverlenersidentificatie (UZI-)-register van belang. En voor zorgverzekeraars het unieke zorgverzekeraars (UZOVI)-register. In de hiervoor geschetste 'tempel van NICTIZ' is te zien dat deze nummers (en daarmee de ZIN-wet) randvoorwaardelijk zijn voor een EPD. Verder zal de wet verwijzen naar beveiligingsnormen en autorisatieregelingen, zoals die nu juridisch al grotendeels in de WGBO staan en zijn toegelicht in het onderhavige artikel.

Bovendien zij verwezen naar de (deels hiervoor genoemde) ontwikkelingen rond zelfregulering), zoals de nadere uitwerking van de NEN Norm voor informatiebeveiliging in de zorg (7510) en ontwikkelingen rond wereldwijde standaarden voor EPD's (zoals HL7).

Tenslotte merk ik op dat in dit artikel het algemene normatieve kader voor EPD's is geschetst en toegepast op de praktijk van labsystemen. Helaas heeft uw beroepsgroep nog geen specifieke beroepsregels (bijvoorbeeld in de vorm van een door het CBP goedgekeurde gedragscode) opgesteld die een concrete invulling geven aan de algemene normen in de WBP, WGBO en andere relavante wet- en regelgeving rond labsystemen c.q. EPD's. Van harte beveel ik uw beroepsgroep aan concrete invulling aan deze algemene normen te gaan geven. Zolang die concrete invulling er niet is, hoop ik met dit artikel enig houvast te bieden.

Literatuur

1. Gevers JKM., Hooghiemstra TFM, Nouwt S, Roscam Abbing HDC. Algemene rapportage van het juridisch laboratorium. Den Haag: ZonMw, oktober 2002.
2. Gevers JKM, Roscam Abbing HDC. Het EPD en de positie van de patiënt bij raadpleging van patiëntengegevens. Den Haag: ZonMw, oktober 2002.
3. Hooghiemstra TFM. Laboratoriumuitslagen en privacy, Ned Tijdschr Klin Chem 2000; 25: 259-262.
4. Hooghiemstra TFM. Patiënten- en zorgverlenersidentificatie; een weergave van de juridische 'state of the art'. Den Haag, oktober 2002.
5. Hooghiemstra TFM. *Verwijsindexen*. Den Haag: ZonMw, oktober 2002.
6. Hooghiemstra TFM. Privacy bij ICT in de zorg, CBP, Den Haag, november 2002.
7. Hooghiemstra TFM. Tekst en toelichting Wet bescherming persoonsgevens, 2e editie, Koninklijke Vermande, 2003.
8. Nouwt S. Verantwoordelijkheid en aansprakelijkheid bij het EPD. Den Haag: ZonMw, oktober 2002.
9. Nouwt S.Beveiliging van het EPD. Rapportage van het juridisch laboratorium. Den Haag: ZonMw, oktober 2002.
10. Wijmen FCB van, Swilders PH. De expertise van de klinisch chemicus. Medisch Contact, 10 mei 2002, p.80.

Ned Tijdschr Klin Chem Labgeneesk 2004; 29: 225-227

Het bloed gevolgd van voor- tot achterdeur

G. COUNOTTE

De Gezondheidsdienst voor Dieren levert kennis over landbouwhuisdieren en hun kwaliteitskenmerken in relatie tot hun gezondheid en productie van veilig voedsel. Met andere woorden: zorg dat het dier traceerbaar gezond is tijdens de productieve periode (ei, melk) en dat het dier gezond wordt geëxporteerd (levend) of geslacht (vlees).

Het doel van 'tracking / tracing' is te zorgen dat het product veilig en traceerbaar bij de consument komt waarbij het dier vanaf geboorte (vader/moeder = stamboek), tijdens zijn verblijf op het bedrijf en vervolgens tijdens transport wordt gevolgd. De gezondheid moet op ieder moment traceerbaar zijn, liefst ook op afstand (bijv. intranet). De Gezondheidsdienst ondersteunt daarbij maar moet er dan ook voor zorgen dat binnen het laboratorium geen verwisselingen van monsters, inzendingen of uitslagen kunnen voorkomen en dat alle processen en resultaten traceerbaar zijn en via webfunctionaliteit beschikbaar komen. De onderzoeksmaterialen (1 tot 500 monsters) komen bij de voordeur van het laboratorium voorzien van een inzendformulier. Op het formulier staan gemiddeld 1 tot 20 onderzoeken aangekruist. De monsters kunnen

Gezondheidsdienst voor Dieren in Deventer