

De staat van de privacybescherming van patiënten en cliënten 2005-2006

mr. dr. J. Nouwt en mr. V.C. Lucieer¹

Samenvatting

Tal van maatschappelijke, economische, technologische en andere hedendaagse ontwikkelingen zijn van invloed op de bescherming van de privacy van patiënten en cliënten in de zorgsector. Enkele voorbeelden zijn de invoering van het nieuwe zorgstelsel, het groeiend aantal samenwerkingsverbanden, de ontwikkelingen rond centrale en decentrale elektronische patiëntendossiers, de identificatieplicht voor patiënten en de fraudebestrijding in de zorg, mede in het licht van de invoering van het burgerservicenummer in de zorg. Deze bijdrage gaat in op deze ontwikkelingen in het licht van de volgende drie thema's: het medisch beroepsgeheim (par. 2), patiëntendossiers (par. 3) en patiëntenidentificatie en fraudebestrijding (par. 4). Dit artikel wordt afgesloten met een analyse (par. 5).

1. Inleiding

Verschillende maatschappelijke, economische, technologische en andere ontwikkelingen van vandaag de dag zijn van invloed op de bescherming van de privacy van patiënten en cliënten. Privacy van patiënten en cliënten is een ruim begrip, dat zich niet alleen beperkt tot de vertrouwelijkheid van en de omgang met gezondheidsgegevens uit medische dossiers, maar zich tevens uitstrekt tot het grondrecht op bescherming van de lichamelijke integriteit. Met het oog op het laatste zij gewezen op de bestaande mogelijkheid om RFID chips te implanteren in mensen, bijvoorbeeld in geriatrische patiënten. Hoewel dergelijke toepassingen van geolokatie-systemen zeker voordelen kunnen hebben voor bepaalde patiënten, zal bij de implementatie daarvan zeker rekening moeten worden gehouden met de “verkeersregels” die bestaan ter bescherming van de privacy.

De hierboven bedoelde ontwikkelingen zijn talrijk en gevarieerd. In de vorige “Staat van de privacybescherming van patiënten en cliënten in de zorgsector” werd daar ook al op gewezen. Ook in deze nieuwe “Staat van de privacybescherming” hebben wij daarom een selectie moeten maken van de volgens ons meest belangrijke ontwikkelingen van de laatste twee jaren. Evenals in de vorige aflevering besteden we ook deze keer aandacht aan de stand van zaken met betrekking tot het medisch beroepsgeheim, elektronische patiëntendossiers en patiëntenidentificatie en fraudebestrijding. In dat verband zullen we op een aantal van de bedoelde maatschappelijke, economische, technologische en andere ontwikkelingen ingaan. Daarnaast besteden we ook aandacht aan voor deze drie centrale thema's relevante rechtspraak, casuïstiek en literatuur van de afgelopen twee jaren.

We gaan in onze bijdrage niet in op de privacybescherming voor de zieke werknemer. Daarvoor verwijzen we naar de bijdrage van Hester de Vries in dit nummer.

2. Het medisch beroepsgeheim

2.1 Zorgverzekeringswet en Addendum Zorgverzekeraars

¹ Sjaak Nouwt is Universitair Docent aan de Universiteit van Tilburg en hoofdredacteur van P&I. Victoire Lucieer is werkzaam als beleidsmedewerker bij het College bescherming persoonsgegevens.

Waarschijnlijk de belangrijkste ontwikkeling op het terrein van het gezondheidsrecht de afgelopen jaren was de inwerkingtreding van de Zorgverzekeringswet (Zvw) op 1 januari 2006. Deze wet maakt een belangrijk onderdeel uit van een omvangrijke stelselwijziging. Het publieke ziekenfonds werd vervangen door een privaat uitgevoerde basisverzekering en de introductie van marktwerking in de zorg die al enige tijd gaande was, werd nu nog explicieter en ook wettelijk verankerd. Deze stelselwijziging heeft veel consequenties voor het medisch beroepsgeheim en de privacybescherming van verzekerden. Het College bescherming persoonsgegevens (CBP) heeft blijkens het Jaarverslag 2005 in dat jaar dan ook veel aandacht besteed aan deze stelselwijziging. Als resultaat daarvan zijn afspraken gemaakt met de minister van Volksgezondheid, Welzijn en Sport (VWS) en is met betrekking tot de verwerking van persoonsgegevens onder andere artikel 87 Zvw nader uitgewerkt in een ministeriële regeling, de Regeling Zorgverzekering (zie hierna).²

Volgens Doppegieter en Legemaate hebben de gevolgen van deze stelselwijziging met name betrekking op het declareren van zorg, de controle door de zorgverzekeraars, het onderhoud van de DBC (DiagnoseBehandelingCombinaties) -systematiek en de risicoverevening.³ Binnen de systemen voor DBC-onderhoud en risicoverevening worden de persoonsgegevens versleuteld. Bij de declaratie van zorg en de controle daarop is dat echter niet het geval.

Om marktwerking te kunnen bevorderen is een nieuwe bekostigingssystematiek ingevoerd, waarbij gebruik wordt gemaakt van DBC's. Bij het declareren van aan een patiënt verleende zorg dienen zorgaanbieders gebruik te maken van codes (DBC's) die de ziektekostenverzekeraar onder meer informatie geven over de gestelde diagnose en de behandeling die vervolgens is ingezet. De verzekeraar krijgt daardoor veel meer medische informatie over zijn verzekerden dan ten tijde van de Ziekenfondswet (Zfw) het geval was. Ondanks afspraken die hierover tussen het College bescherming persoonsgegevens (CBP) en de Minister van VWS zijn gemaakt over de vergroving van deze DBC's met als gevolg dat de verzekeraars minder gedetailleerde medische informatie zouden ontvangen, heeft de Minister hier nog altijd geen gehoor aan gegeven. Dit betekent dat de verzekerde nog steeds een privacyrisico loopt als gevolg van de invoering van de DBC-systematiek.⁴

Hoewel de inbreuk op het medisch beroepsgeheim onder de Zvw vele malen groter is dan onder de Zfw het geval was, omdat veel meer persoonsgegevens moeten worden verstrekt aan de zorgverzekeraar, is bij en krachtens de Zvw wel veel duidelijker bepaald welke (medische) persoonsgegevens zorgaanbieders aan zorgverzekeraars moeten verstrekken en voor welke doeleinden dit dient te gebeuren. De artikelen 86 tot en met 93 van de Zvw bevatten hiervoor de wettelijke basis. De Regeling Zorgverzekering bepaalt onder meer nader welke gegevens op grond van artikel 87 Zvw moeten worden verstrekt, op welke wijze dit dient te gebeuren en aan welke beveiligingseisen deze gegevensverstrekking dient te voldoen.⁵ Ook bepaalt deze ministeriële regeling dat de zorgverzekeraar deze gegevens moet verwerken in overeenstemming met de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen, die gedragsregels bevat voor banken en verzekeraars.⁶

² College bescherming persoonsgegevens, *Jaarverslag 2005*. Den Haag: CBP juni 2006, p. 9.

³ R.M.S. Doppegieter en J. Legemaate, Het beroepsgeheim van hulpverleners en de nieuwe zorgverzekeringswet. *NJB*, afl. 2005/40

⁴ Zie ook: College bescherming persoonsgegevens, *Jaarverslag 2005*. Den Haag: CBP juni 2006, p. 11 en p. 41.

⁵ Regeling van de Minister van Volksgezondheid, Welzijn en Sport van 1 september 2005, nr. Z/VV-2611957, houdende regels ter zake van de uitvoering van de Zorgverzekeringswet (Regeling zorgverzekering). *Staatscourant* 2005, 171.

⁶ Gedragscode Verwerking Persoonsgegevens Financiële Instellingen van het Verbond van Verzekeraars en de Nederlandse Vereniging van Banken (te vinden op www.cbpweb.nl via 'wetten en zelfregulering' en 'gedragscodes'). Met een 'goedkeurende verklaring' wordt bedoeld op een verklaring van het CBP als bedoeld in artikel 25 van de Wet

Aangezien ziektekostenverzekeraars veel meer dan andere financiële instellingen medische gegevens verwerken, heeft Zorgverzekeraars Nederland (ZN) een aanvulling op de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen gemaakt. Dit Addendum Zorgverzekeraars (het Addendum) is door het CBP van een 'goedkeurende verklaring' voorzien en van kracht vanaf 4 mei 2006.⁷ Sinds die datum zijn alle in Nederland opererende zorgverzekeraars dan ook (krachtens de Regeling Zorgverzekering) gebonden aan het bepaalde in het Addendum.

Ter voorbereiding op het verzoek van ZN, het Verbond van Verzekeraars en de Nederlandse Vereniging van Banken tot goedkeuring van het Addendum heeft het CBP medio 2005 een verkennend onderzoek uitgevoerd bij drie ziektekostenverzekeraars.⁸ Dit onderzoek is verricht om te kunnen beoordelen welke aanvullende regelgeving noodzakelijk was. Uit dit onderzoek kwam naar voren dat er met name onduidelijkheid bestond bij de onderzochte verzekeraars over het inzien van medische dossiers ten behoeve van materiële controle, de reikwijdte van de zogenaamde 'Chinese muren' die het verder verwerken van persoonsgegevens voor een andere (ziekttekosten-)verzekering reguleren, de selectie van groepen verzekerden op basis van declaratiegegevens, de verantwoordelijkheid van de adviserend geneeskundige en het opvragen van medische gegevens bij zorgaanbieders. Deze onderwerpen zijn geadresseerd in het Addendum.

In zijn algemeenheid bepaalt het Addendum of persoonsgegevens mogen worden verwerkt voor de verschillende bedrijfsprocessen van de zorgverzekeraars.⁹ Ten behoeve van de zorginkoop, schadelastbeheersing, algemene zorgbemiddeling, acceptatie (bij een wettelijke acceptatieplicht), maatschappelijke en financiële verantwoording, marketing en premie-inning worden geen gezondheidsgegevens verwerkt. Voor de schadebehandeling, acceptatie voor de aanvullende verzekering, individuele zorgbemiddeling, materiële controle, fraude en geschillenbehandeling worden alleen gezondheidsgegevens verwerkt als dat noodzakelijk is. Als gezondheidsgegevens worden verwerkt rust er op de medewerkers van de zorgverzekeraar een contractuele geheimhoudingsplicht. De beoordeling, taxatie en interpretatie van gezondheidsgegevens vinden plaats onder de verantwoordelijkheid van de medisch adviseur. De verzekeraar is de verantwoordelijke als bedoeld in de Wet bescherming persoonsgegevens (WBP), maar de medisch adviseur is tuchtrechtelijk aansprakelijk voor het gebruik van gezondheidsgegevens.

Tot slot bevat het Addendum Zorgverzekeraars als bijlage een Protocol Materiële Controle. Materiële controles worden door de zorgverzekeraars toegepast om te voldoen aan hun wettelijke verplichtingen en om de schadelast en premies te beperken. Bij een dergelijke controle gaat de verzekeraar na of de door de zorgaanbieder gedeclareerde prestatie is geleverd (rechtmatigheid) en of die prestatie, gelet op de gezondheidstoestand van de verzekerde, wel de meest aangewezen was (doelmatigheid).

bescherming persoonsgegevens.

⁷ Een 'goedkeurende verklaring' is geldig vanaf de dag na publicatie in de Staatscourant. Deze verklaring is gepubliceerd in de Staatscourant van 3 mei 2006 ('Goedkeuring Addendum Zorgverzekeraars bij de bestaande Gedragscode Persoonsgegevens Financiële Instellingen', *Staatscourant* 2006, 85) en geldig tot 4 februari 2008. 'Addendum Zorgverzekeraars van goedkeurende verklaring voorzien'. Persbericht College bescherming persoonsgegevens, 27 april 2006. Zie ook College bescherming persoonsgegevens, *Jaarverslag 2005*. Den Haag: CBP juni 2006, p. 11 en p. 41.

⁸ 'Zorgverzekeraars, gezondheidsgegevens en privacy. Verkennend onderzoek bij drie zorgverzekeraars in relatie tot het Addendum en het Protocol materiële controle', CBP, mei 2006. Het rapport is te vinden op www.cbpreweb.nl.

⁹ Vgl. M. Kooijman, Nieuwe privacycode zorgverzekeraars. *JPG* 2006/46.

Ten behoeve van de materiële controle is het in bepaalde gevallen mogelijk dat een verzekeraar toegang krijgt tot een medisch dossier van een patiënt c.q. verzekerde. Daarbij gelden nadrukkelijk de beginselen van proportionaliteit en subsidiariteit als uitgangspunten. De hoofdregel luidt dat de ziektekostenverzekeraar voor de materiële controle geen gebruik maakt van tot personen herleidbare gegevens, tenzij onderzoek daarmee aanwijzingen oplevert voor een redelijk vermoeden van onrechtmatig of ondoelmatig handelen.¹⁰ Voor de materiële controle is inzage in medische dossiers alleen gerechtvaardigd als het nader onderzoek is gericht op het vaststellen van fraude of oneigenlijk gebruik en inzage de toets van proportionaliteit en subsidiariteit doorstaat. Voor de doelmatigheidsvraag is het opvragen van alle medische dossiers disproportioneel.¹¹

2.2 Samenwerkingsverbanden

Samenwerkingsverbanden zijn meer en meer in opkomst, ook in de zorgsector. Een van de meest privacygevoelige samenwerkingsverbanden is de samenwerking in het kader van bemoeizorg (vaak een ‘vangnetoverleg’ genoemd). Bij bemoeizorg – actieve en ‘outreachinge’ hulpverlening aan mensen met ernstige psychische of psychosociale problemen die hulp afwijzen, maar die hulp wel dringend nodig hebben – is het vaak noodzakelijk dat niet alleen zorgaanbieders samenwerken, maar dat daarbij ook organisaties zoals de politie, woningbouwcorporaties en de sociale dienst worden betrokken. Hoewel in steeds meer steden en regio’s vorm werd gegeven aan deze samenwerkingsverbanden, merkten het CBP en de Inspectie voor de Gezondheidszorg (de Inspectie) dat er met name bij hulpverleners veel vragen bestonden over de verhouding tussen het uitwisselen van informatie en hun medisch beroepsgeheim.¹² Daarom zijn in 2004 GGZ Nederland, GGD Nederland en de Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst (KNMG) gevraagd richtlijnen op te stellen voor hulpverleners. Deze handreiking ‘Gegevensuitwisseling in het kader van bemoeizorg’ (de ‘Handreiking voor bemoeizorg’) was in april 2005 een feit. De handreiking gaat uit van het onderscheid tussen kernpartners, organisaties die primair hulpverlening tot doel hebben, en schilpartners, zoals de politie, woningbouwcorporaties en de sociale dienst. Schilpartners dienen in beginsel geen informatie over de lichamelijke of psychische toestand van een cliënt te ontvangen. Een ander belangrijk uitgangspunt van de handreiking is dat steeds moet worden gestreefd naar toestemming van de cliënt. Het verstrekken van gegevens zonder toestemming van de cliënt is immers een inbreuk op zijn rechten. De handreiking bevat tien richtlijnen waarin de uitgangspunten worden opgesomd.

Naast vangnetoverleggen worden er meer samenwerkingsverbanden aangegaan in de zorg. Een voorbeeld is de samenwerking tussen energieleverancier Nuon en de GGD in Amsterdam. Zij hebben een samenwerkingsprotocol opgesteld met als doel de afsluiting van energie bij mensen die zich in een fysieke of psychische noodsituatie bevinden te voorkomen. Het CBP heeft in 2005 advies uitgebracht over het voornemen tot samenwerking en daarbij aangegeven dat Nuon NAW-gegevens mag doorgeven aan de GGD als de gezondheidstoestand van de betrokkene dat noodzakelijk maakt, waarna de GGD contact kan opnemen met deze persoon. In verband met het medisch beroepsgeheim mag de GGD slechts informatie doorgeven aan Nuon indien de betrokkene daarvoor toestemming heeft gegeven.¹³

¹⁰ Protocol Materiële Controle, hoofdstuk 2.

¹¹ Idem.

¹² Zie ook: College bescherming persoonsgegevens, *Jaarverslag 2005*. Den Haag: CBP juni 2006, p. 43.

¹³ College bescherming persoonsgegevens, ‘Samenwerking Nuon en GGD om afsluiting van energie te voorkomen’, 12 september 2005; zie www.cbpweb.nl.

Een ander voorbeeld van een samenwerkingsverband is het Justitieel CasusOverleg-Jeugd (CJO-Jeugd) dat op 1 mei 2003 in alle arrondissementen in het land is ingevoerd. In dat overleg bespreken vertegenwoordigers van het Openbaar Ministerie, de politie en de Raad voor de Kinderbescherming individuele zaken van jongeren tussen de 12 en 18 jaar die in aanraking zijn gekomen met de politie. In veel arrondissementen doen ook nog andere deelnemers mee aan het overleg, zoals Bureau HALT, Bureau Jeugdzorg en de gemeente. In dat verband kunnen wij ook wijzen op de ontwikkelingen rondom de invoering van het Elektronisch Kinddossier (2008), dat wellicht nog eens een rol gaat spelen in het samenwerkingsverband CJO-Jeugd. Sinds september 2006 is een Modelconvenant Justitieel CasusOverleg Jeugd beschikbaar dat de bestaande mogelijkheden aangeeft voor de uitwisseling van persoonsgegevens tussen bij het CJO-Jeugd betrokken partijen.¹⁴

2.3 Casuïstiek

Een medisch adviseur van een verzekeraar mag alleen met toestemming van de cliënt gezondheidsgegevens over die cliënt verstrekken aan een neuroloog. Een neuroloog die door een medisch adviseur van een verzekeraar wordt gevraagd om een aantal vragen te beantwoorden op basis van een patiëntendossier, mag erop vertrouwen dat de medisch adviseur daarvoor toestemming heeft gekregen van de patiënt, maar moet dat eigenlijk wel even checken. Deze uitspraak deed het Centraal Tuchtcollege voor de Gezondheidszorg op 31 augustus 2004.¹⁵ Hoewel de medisch adviseur had nagelaten om de cliënt om toestemming voor de gegevensverstrekking te vragen, legde het Centraal Tuchtcollege opmerkelijk genoeg geen maatregel op. Waarschijnlijk omdat de cliënt nadien liet weten dat hij toch wel toestemming daarvoor had gegeven.

Op grond van art. 7:457 BW mag een hulpverlener (zorgaanbieder) aan een andere hulpverlener persoonsgegevens verstrekken zonder toestemming van de patiënt als die andere hulpverlener rechtstreeks betrokken is bij de uitvoering van de behandelingsovereenkomst. Het Centraal Tuchtcollege voor de Gezondheidszorg bepaalde in een uitspraak op 12 augustus 2004 dat de informatie verstreckende hulpverlener de kring van “rechtstreeks bij de uitvoering betrokkenen” in bepaalde omstandigheden ruim mag uitleggen, om overbodige ingrepen te voorkomen die schade voor de patiënt kunnen opleveren.¹⁶ In dit geval had een revalidatie-arts een kopie van zijn brief aan de huisarts van een patiënt aan 17 specialisten gestuurd die volgens het dossier van de huisarts van de patiënt (ooit) bij de behandeling betrokken zijn geweest. De patiënt is daarover niet geïnformeerd. Het Centraal Tuchtcollege is van mening dat de revalidatiearts in redelijkheid kon menen dat het versturen van de kopieën van de brief aan diverse specialisten in het belang van de patiënt was. Een belangrijke overweging daarbij is dat de revalidatiegeneeskunde een inter- en multidisciplinair specialisme is, waarbij het van belang kan zijn dat een revalidatiearts andere bij de behandeling betrokken hulpverleners informeert over zijn bevindingen, ter vermijding van het gevaar van overbodige, voor de patiënt schadelijke ingrepen of behandelingen.

Bij een vermoeden van kindermishandeling mag een hulpverlener de geheimhoudingsplicht doorbreken als sprake is van een conflict van plichten. Maar ook dan geldt dat zorgvuldigheid

¹⁴ Zie ook: M.R. Bruning, *Over sommige kinderen moet je praten. Gegevensuitwisseling in de jeugdzorg*. Rede uitgesproken bij de aanvaarding van het ambt van bijzonder hoogleraar vanwege het Leids Universiteits Fonds op het gebied van het Jeugdrecht aan de Universiteit Leiden op dinsdag 11 april 2006.

¹⁵ Medisch adviseur verstrekt patiëntengegevens zonder toestemming aan neuroloog. *P&I* 2005, p. 42.

¹⁶ Centraal Tuchtcollege voor de Gezondheidszorg, 12 augustus 2004, *P&I* 2005, p. 88-89.

in acht genomen moet worden. Een jeugdarts die in een brief aan het Advies- en Meldpunt Kindermishandeling (AMK) partij kiest door zich positief uit te laten over de moeder, maar negatief over de vader, gaat daarmee te ver. Hij had zich moeten beperken tot het vermoeden van Parental Alienation Syndrome. De jeugdarts krijgt hiervoor een waarschuwing.¹⁷ Wel zorgvuldig handelde een kinderarts door een vermoeden van kindermishandeling te melden bij het AMK nadat een leerlingverpleegkundige had gezien dat een moeder tijdens het baden het hoofdje van haar kind onder water hield. Op grond van een aantal feiten en omstandigheden kon de kinderarts vermoeden dat sprake was van Münchhausen-by-proxy syndroom (MBP). Door dit vermoeden te melden aan de huisarts, de vertrouwensarts en het AMK, handelde de kinderarts niet onzorgvuldig omdat hij op dat moment in redelijkheid van de juistheid van de feiten mocht uitgaan.¹⁸

In een commentaar op beide uitspraken wijst De Roode erop dat het een goede ontwikkeling is dat artsen steeds vaker melding doen van vermoedens van kindermishandeling.¹⁹ De moeilijkheid ligt vooral in de vraag wanneer, hoe en wat er precies moet worden gemeld. Behoedzaamheid en zorgvuldigheid is geboden, aldus De Roode. De “Meldcode voor medici inzake kindermishandeling” biedt hiervoor handvatten. Omdat een arts soms nog de enige is die contact heeft met een gezin, moeten er wel goede redenen zijn om het beroepsgeheim te doorbreken en het (laatste) contact te beschadigen.

Ook de Hoge Raad heeft zich uitgesproken over het medisch beroepsgeheim met betrekking tot het medisch dossier van de Stichting Thuiszorg Groot Rijnland over de peuter Savanna.²⁰ Het dossier was in beslag genomen in opdracht van de rechter-commissaris. De Stichting wil de inbeslagname ongedaan laten maken met een beroep op het verschoningsrecht (medisch beroepsgeheim). De Hoge Raad bevestigt in het arrest van 9 mei 2006 dat aan het verschoningsrecht ten grondslag ligt dat het belang van waarheidsvinding moet wijken voor het maatschappelijk belang dat een ieder zich zonder vrees voor openbaarmaking van het toevertrouwde moet kunnen wenden tot een verschoningsgerechtigde. Volgens de Hoge Raad heeft de rechtbank onvoldoende gemotiveerd dat in dit geval sprake is van zeer uitzonderlijke omstandigheden die de inbreuk op het verschoningsrecht door inbeslagname zou kunnen rechtvaardigen. Bij die afweging moeten de volgende omstandigheden worden meegenomen:

- het moet gaan om een verdenking van de verschoningsgerechtigde;
- de aard en omvang van de gegevens die bij doorbreking van het verschoningsrecht in de strafprocedure worden ingebracht is van belang;
- in dit geval betrof het een verdenking van de misdrijven van art. 307, 308 en 309 Sr (dood of zware mishandeling door schuld, gepleegd in de uitoefening van een beroep), terwijl de rechtbank met name de frequentie en inhoud van de contacten tussen de arts van het consultatiebureau en de verdachte gezinsvoogdes van belang achtte;
- de vraag of de relevante gegevens niet op een andere wijze konden worden verkregen: deze vraag is door de rechtbank onvoldoende onderzocht.

Een psychotherapeut die een verzekeringsarts schriftelijk informeert over de problemen van een patiënt mag die problemen niet als feiten presenteren als het om een subjectieve beleving van de patiënt gaat. De psychotherapeut had woorden moeten gebruiken als “mijn cliënte zegt...”.²¹ De achtergrondinformatie die de psychotherapeute verstreekte was bovendien te

¹⁷ Regionaal Tuchtcollege Eindhoven, 2 juni 2005, *P&I* 2006/108.

¹⁸ Regionaal Tuchtcollege Zwolle, 13 oktober 2005, *P&I* 2005/109.

¹⁹ Noot R.P. de Roode bij Regionaal Tuchtcollege Zwolle, 13 oktober 2005, nr. 93/04. *Gezondheidszorg Jurisprudentie* 2006/6.

²⁰ HR, 9 mei 2006, *P&I* 2006/214.

²¹ Regionaal Tuchtcollege Amsterdam, 10 augustus 2004, *P&I* 2005, p. 42.

uitvoerig. Ook had de psychotherapeut geen prognostische uitspraken moeten doen over arbeidsongeschiktheid. Tevens is er onvoldoende rekening mee gehouden dat de brief gebruikt zou kunnen worden in een rechtszaak over een omgangsregeling. De psychotherapeut kreeg een waarschuwing van het Regionaal Tuchtcollege.

Ook een psychiater die bij wijze van vriendendienst een verklaring afgeeft die als getuigenverklaring wordt gebruikt in een echtscheidingsprocedure schendt zijn beroepsgeheim.²² De 'vriendin' dient een klacht tegen hem in omdat hij zonder haar toestemming in de verklaring zegt dat hij haar antidepressiva (Prozac) heeft voorgeschreven. Het Regionaal Tuchtcollege oordeelt dat, ondanks het feit dat hier sprake zou zijn van een vriendendienst, er wel degelijk een behandelrelatie tussen beide heeft bestaan waardoor sprake is van handelen in het kader van individuele gezondheidszorg. Dat heeft tot gevolg dat het beroepsgeheim op die relatie van toepassing is.

Uit de bovenstaande casuïstiek blijkt wederom dat het medisch beroepsgeheim geen belemmering vormt voor noodzakelijke gegevensverstrekkingen. Een hulpverlener mag bijvoorbeeld de kring van rechtstreeks bij de behandeling betrokkene n (waarmee onder voorwaarden gegevens over de patiënt kunnen worden uitgewisseld) ruim uitleggen, indien de verstrekking noodzakelijk is om overbodige ingrepen te voorkomen die schade voor de patiënt kunnen opleveren.²³ Ook in andere zwaarwegende gevallen zoals bij een vermoeden van kindermishandeling kunnen, in het belang van de patiënt, gegevens worden verstrekt. Zorgvuldigheid is in al deze gevallen wel geboden, met name omdat het medisch beroepsgeheim een essentiële factor is in de vertrouwensrelatie tussen hulpverlener en patiënt.

2.4 Literatuur

In de afgelopen twee jaren is verschillende interessante literatuur verschenen die in meer of minder mate ook gaat over het medisch beroepsgeheim. Hieronder gaan we in op een tweetal interessante proefschriften die zijn verschenen.

Ploem concludeert in haar proefschrift, waarop zij in december 2004 in Amsterdam promoveerde, dat op een aantal punten in de huidige wet- en regelgeving aanpassing of aanvulling wenselijk is met betrekking tot het gebruik van gezondheidsgegevens voor wetenschappelijk onderzoek.²⁴

- de juridische status van gecodeerde gegevens is niet duidelijk;
- het toestemmingsvereiste neemt een te centrale positie in;
- de regels voor het verzamelen en verwerken van gecodeerde gegevens zijn te streng;
- er zijn te weinig waarborgen voor transparantie ;
- een systematisch toezicht op de naleving van de regelgeving ontbreekt; en
- niet langer kan worden volstaan met een regeling voor alleen de verstrekking van patiëntengegevens aan onderzoekers (en niet voor eigen wetenschappelijk onderzoek door de hulpverlener).

Ploem geeft enkele aanbevelingen die betrekking hebben op de materiële normen, de rechten voor betrokkenen en normen voor systematisch toezicht op de naleving van de regelgeving. Voor wetenschappelijk onderzoek moet zoveel mogelijk met anonieme of gecodeerde gegevens worden gewerkt. Dat leidt niet alleen tot een minder grote privacy-inbreuk voor de

²² Regionaal Tuchtcollege Amsterdam, 5 april 2005, *P&I* 2005, p. 233.

²³ Centraal Tuchtcollege voor de Gezondheidszorg, 12 augustus 2004, *P&I* 2005, p. 88-89.

²⁴ M.C. Ploem, *Tussen privacy en wetenschapsvrijheid. Regulering van gegevensverwerking voor medisch-wetenschappelijk onderzoek*. Den Haag: Sdu uitgevers 2004.

betrokkenen, maar ook tot minder belasting voor de onderzoekers (toestemming vragen, informatieplicht, andere rechten betrokkenen). Voorts kan volgens Ploem worden volstaan met een bezwaarmogelijkheid voor betrokkenen in plaats van expliciete toestemming vooraf als het onderzoek plaats vindt met gecodeerde gegevens. Het CBP, de rechter en de medisch-ethische toetsingscommissies moeten zorgen voor voldoende toezicht en handhaving.

Een ander in dit verband interessant proefschrift is getiteld “Boeven in het ziekenhuis” en werd op 19 september 2005 in Nijmegen verdedigd door Duijst-Heesters.²⁵ Zoals de subtitel vermeldt, bevat het boek een juridische beschouwing over de verhouding tussen het medisch beroepsgeheim en de opsporing van strafbare feiten. In haar boek staan twee vragen centraal:

- In welke situaties kan het opsporingsbelang prevaleren boven het belang van het medisch beroepsgeheim?
- Kan met behulp van convenanten tussen politie en ziekenhuizen vorm gegeven worden aan de verhouding tussen het medisch beroepsgeheim en de opsporing?

Duijst-Heesters concludeert dat de wetgever het medisch beroepsgeheim duidelijk laat prevaleren boven het belang van opsporing. Dat volgt met name uit het verschoningsrecht dat in het Wetboek van Strafvordering is opgenomen. Om het medisch beroepsgeheim (zwijgplicht of verschoningsrecht) te mogen doorbreken in het belang van opsporing, zal daarom een wettelijke grondslag moeten bestaan. Om aan dit uitgangspunt te voldoen zijn wettelijke aanpassingen nodig op de volgende punten:

- Algemene wet op het binnentreden: toegang tot behandelkamer van de arts en kamer van verschoningsgerechtigde moet slechts mogelijk zijn met toestemming van de verschoningsgerechtigde of met een machtiging van de rechter-commissaris;
- Artikel 98 WvSv moet worden aangepast omdat de huidige formulering niet duidelijk is: niet alleen brieven en geschriften, maar alle voorwerpen die onder het verschoningsrecht vallen moeten uitgesloten worden van inbeslagneming. Inbeslagneming moet wel mogelijk zijn wanneer de verschoningsgerechtigde zelf verdachte is van een strafbaar feit;
- Aftappen van de telefoon van een verschoningsgerechtigde moet bij wet worden uitgesloten. Onder de bestaande regeling komen de gegevens eerst ter beschikking van het Openbaar Ministerie voordat wordt besloten of zij onder het verschoningsrecht vallen;
- Wetgeving die verplicht tot het verstrekken van gegevens voor opsporing of controle moet duidelijk maken welke weg die gegevens gaan afleggen;
- Een wettelijke regeling moet een arts verplichten om het overlijden van minderjarigen te melden bij een gemeentelijk lijkschouwer, waardoor de vaststelling of sprake is van een al dan niet natuurlijke dood niet langer door de behandelende arts (veelal tevens de huisarts van het gezin) plaats vindt;
- Een wettelijke regeling moet het gebruik van DNA-materiaal uit hielprikbloed zonder toestemming van de ouders mogelijk maken voor de identificatie van een lijk, zoals bijvoorbeeld in gevallen als dat van “het meisje van Nulde”.

Met betrekking tot de convenanten tussen politie en ziekenhuizen concludeert Duijst-Heesters dat in dergelijke convenanten meestal afspraken worden vastgelegd over het door de politie betreden van het ziekenhuis, doorzoeking en inbeslagneming, beroepsgeheim en niet-natuurlijke dood. Er lijkt consensus te bestaan bij de NVZ (vereniging van ziekenhuizen), de artsenorganisatie KNMG, het Expertisecentrum medische zaken en bij individuele

²⁵ W.L.J.M. Duijst-Heesters, *Boeven in het ziekenhuis. Een juridische beschouwing over de verhouding tussen het medisch beroepsgeheim en de opsporing van strafbare feiten*. Diss. Nijmegen. Den Haag: Sdu uitgevers 2005.

ziekenhuizen over de wens dat dergelijke convenanten tussen politie en ziekenhuizen op landelijk niveau moeten worden gesloten.

3. Patiëntendossiers

3.1 Bewaartermijn medische dossiers

Op 1 april 2004 publiceerde de Gezondheidsraad het rapport 'Bewaartermijn patiëntengegevens'.²⁶ In dat rapport doet de Gezondheidsraad voorstellen voor verschillende bewaartermijnen voor de verlening van zorg, erfelijke gegevens en medisch-wetenschappelijk onderzoek, die alle langer zijn dan de op dat moment geldende bewaartermijn van 10 jaar voor patiëntendossiers waarop de WGBO van toepassing is.

In verband met een overgangsbepaling uit de WGBO ging de bewaartermijn voor bestaande dossiers pas lopen bij inwerkingtreding van de wet. Vanaf 1 april 2005 zouden veel dossiers worden vernietigd, tenzij uit de zorg van een goed hulpverlener voortvloeide dat deze gegevens langer zouden moeten worden bewaard. In verband met de korte periode die nog restte tot 1 april 2005 en om te voorkomen dat hulpverleners medische dossiers zouden gaan vernietigen, terwijl nader onderzoek door de regering wellicht zou uitwijzen dat het wenselijk zou zijn dossiers langer te bewaren, heeft de overheid vervolgens 'in eerste instantie en als voorlopige maatregel' (wat overigens niet uit de wettekst blijkt) besloten de bewaartermijn te verlengen tot 15 jaar.²⁷ De komende jaren zal nader worden bekeken in hoeverre men de adviezen van de Gezondheidsraad wil opvolgen.

Na verloop van de bewaartermijn van 15 jaar vervalt de verplichting voor de hulpverlener om de gegevens uit het medisch dossier nog langer te bewaren, tenzij langer bewaren nodig is omdat het voortvloeit uit de zorg van een goed hulpverlener. Wanneer een hulpverlener na verloop van de bewaartermijn de gegevens wil vernietigen, zouden de betreffende patiënten wel de mogelijkheid moeten hebben om daartegen op te komen. Een mogelijkheid is dan om het dossier aan de patiënten mee naar huis te geven. De patiënten zouden dan wel op de consequentie moeten worden gewezen dat het medisch beroepsgeheim van de hulpverlener er dan niet langer op van toepassing is. Tevens is het van belang dat men zich realiseert wat er kan gebeuren met het dossier na het overlijden van de patiënt.

3.2 Elektronisch patiëntendossier

Het landelijke elektronisch patiëntendossier (EPD) wordt op zijn vroegst in 2007 verwacht. Het EPD is geen dossier dat alle gegevens van een patiënt bevat op een centrale plek. Feitelijk is het slechts een virtueel dossier. Een Landelijk Schakel Punt (LSP) functioneert als 'verkeerstoren' die veilige, landelijke elektronische uitwisseling van patiëntgegevens mogelijk maakt. Via het Landelijk Schakel Punt kunnen hulpverleners gegevens over hun patiënten opvragen bij andere ziekenhuizen, apotheken en huisartsen.

Het EPD wordt gefaseerd ingevoerd. De eerste onderdelen zijn het Elektronisch Medicatie Dossier (EMD), het elektronische Waarneem Dossier Huisartsen (WDH) en het Elektronisch Kinddossier (EKD). Het ministerie van VWS werkt samen met het Nationaal ICT Instituut in de Zorg (NICTIZ), het Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG) en betrokken branche- en koepelorganisaties aan de invoering van deze hoofdstukken. Belangrijke onderdelen bij de invoering van het EPD zijn:

²⁶ Gezondheidsraad, *Bewaartermijn patiëntengegevens*. Den Haag: Gezondheidsraad, 2004; publicatie nr. 2004/08.

²⁷ Wijziging van enige bepalingen van het Burgerlijk Wetboek omtrent de overeenkomst inzake geneeskundige behandeling en van artikel IV van de wet van 17 november 1994, *Stb.* 837, Tweede Kamer 2004-2005, 30 049, nr.3, p.1.

- het identificeren van patiënten met het toekomstige burgerservicenummer (BSN);
- het identificeren en authenticeren van zorgverleners met de Unieke Zorgverlener Identificatie (UZI);
- het veilig en betrouwbaar uitwisselen van informatie via het Landelijk Schakel Punt (LSP);
- het stapsgewijs en zorgvuldig invoeren van de eerste hoofdstukken van het EPD: het Elektronisch Medicatie Dossier (EMD) en het Waarneemdossier Huisartsen (WDH) via een koploperprogramma.

Over het Elektronisch Medicatie Dossier en het Waarneem Dossier Huisartsen is de film 'Veilige en landelijke gegevensuitwisseling in de zorg' te downloaden.²⁸ Deze film geeft een beeld van het nut, noodzaak, werking en invoering van het EPD.

De minister heeft in zijn brief aan de Kamer van 7 november 2005 aangekondigd dat hij voornemens is een wet voor het landelijk EPD (Wet EPD) in te voeren. Deze wet zal bevatten: waarborgen voor veilig gebruik, kwaliteit van de gegevens, autorisatie en toegang (van onder meer de patiënt), standaardiseren en normeren en het daadwerkelijk gebruik van het EPD. De Wet EPD regelt vervolgens:

- (verplichte) aansluiting van zorgaanbieders op het landelijk schakelpunt;
- het elektronisch beschikbaar stellen van patiëntgegevens via het landelijk schakelpunt;
- de gegevens op veilige en betrouwbare wijze via het Landelijk Schakel Punt uitwisselen.

De wettelijke verplichting geldt in het begin alleen voor zorgaanbieders die mee dienen te werken aan het goed functioneren van het Elektronisch Medicatie Dossier en het Waarneem Dossier Huisartsen. Later zal de verplichting worden uitgebreid naar andere zorgaanbieders. De verplichte aansluiting van zorgaanbieders op het Landelijk Schakel Punt moet waarborgen dat de zorgaanbieders hun systemen aanpassen aan het landelijk EPD-systeem. Daarnaast zal de Wet EPD wettelijke waarborgen bevatten om te zorgen dat de gegevens veilig én betrouwbaar via het Landelijk Schakel Punt worden uitgewisseld. Daarmee moet worden voorkomen dat patiëntgegevens die door zorgaanbieders zijn aangeleverd – en die daar zelf verantwoordelijk voor blijven – in handen van niet-gerechtigden vallen. De Wet EPD wordt een kaderwet en zal sober van opzet zijn.²⁹ De minister heeft voorts laten weten dat de Wet EPD niet zal zijn bedoeld om de wettelijke bepaling van het medisch beroepsgeheim te doorbreken als gevolg van meer ICT-verkeer, maar dat deze juist zal aangeven wat de waarborgen zijn voor het medisch beroepsgeheim in verband met de mogelijkheden van ICT.³⁰ Er wordt vooralsnog echter onvoldoende aandacht besteed aan onder meer de autorisaties; daardoor is de kring van personen die toegang kunnen krijgen tot de gegevens breder dan noodzakelijk.

3.3 Casuïstiek

3.3.1 Registratie patiënten met crisisindicatie door huisartsenposten

Personen die psychiatrische hulp nodig hebben dienen in beginsel een verwijzing van hun huisarts te hebben. Dat geldt ook voor degenen die al onder behandeling staan bij een RIAGG of Regionaal Centrum voor Geestelijke Gezondheidszorg en crisisgeïndiceerd zijn. Regelmatig kloppen dergelijke patiënten in een crisistoestand aan bij huisartsenposten. Om te voorkomen dat in deze situaties de tussenkomst van de huisarts van de patiënt nodig is, vroeg

²⁸ Unieke Zorgverleners Identificatie Register, <http://www.uzi-register.nl/> (laatst geraadpleegd op 13 oktober 2006).

²⁹ *Kamerstukken II*, 2005/06, 27 529, nr. 18.

³⁰ Schriftelijke beantwoording vragen Algemeen Overleg ICT in de zorg van 23-11-2005. Kenmerk IBE/I-2653523, 25-01-2006.

een huisartsenpost (HAP) het CBP of deze een registratie van patiënten met een crisisindicatie mocht aanleggen. Hiervoor was het echter wel nodig dat zij de RIAGG en het Regionaal Centrum GGz zouden kunnen benaderen in dergelijke situaties, en dat zij deze gegevens aan de huisartsenposten zouden verstrekken. Het CBP was van oordeel dat in een aantal van deze gevallen mag worden uitgegaan van de veronderstelde toestemming van de patiënt. Het gaat daarbij om patiënten die tijdelijk niet in beeld zijn bij de GGz-instelling of huisarts, of patiënten waarbij de eigen huisarts wel op de hoogte is van de crisisindicatie, maar de crisistoestand zich voordoet tijdens de openingstijden van de huisartsenpost. Hierbij moet echter wel in het oog worden gehouden dat het verstrekken van de informatie slechts mogelijk is, indien en voor zover dit geacht kan worden in het belang van de patiënt te zijn.³¹

3.3.2 *Online afsprakensysteem in Flevoziekenhuis*

Het Flevoziekenhuis te Almere biedt de mogelijkheid aan om afspraken te maken via internet. In een uitspraak naar aanleiding van een klacht erkent het CBP dat een online afsprakensysteem gemakkelijk en klantvriendelijk is.³² Tegelijkertijd wijst het CBP erop dat het niet noodzakelijk is om diagnose-informatie te verwerken om een afspraak te kunnen maken. Dergelijke informatie hoort daarom niet thuis in een online afsprakensysteem. Daarnaast wijst het CBP erop dat de informatie in het online afsprakensysteem beter beveiligd moet worden. Dat kan al worden gerealiseerd door gebruik te maken van individuele wachtwoorden.

De bovenstaande casussen met betrekking tot de registratie van bepaalde crisisgeïndiceerde patiënten en het online afsprakensysteem zijn zeer verschillend van aard. Wel blijkt uit beide zaken dat het CBP nadrukkelijk een rol toekent aan het belang van de patiënt bij een verwerking, maar ook blijkt nogmaals dat verantwoordelijken zich moeten beperken tot het verwerken van de strikt noodzakelijke informatie. Met name elektronische systemen dienen daarbij zeer goed te worden beveiligd.

3.4 *Literatuur*

3.4.1 *CBP rapport landelijke zorgregistraties*

In maart 2005 publiceerde het College bescherming persoonsgegevens het rapport "Landelijke zorgregistraties". Het rapport bevat een verslag van oriënterend feitenonderzoek bij vijf grote landelijke registraties in de zorg. Deze registraties zijn: PALGA (Pathologisch Anatomisch Landelijk Geautomatiseerd Archief), PRN (Perinatale Registratie Nederland), het landelijke ZRS (Zorg Registratiesysteem), ZORGIS (de landelijke GGZ-registratie) en het LINH (Landelijk Informatienetwerk Huisartsen). De centrale vraag was in hoeverre de registraties gegevens bevatten die herleidbaar zijn tot individuele patiënten, in relatie tot de vraag naar de rechtmatigheid van dit soort gegevensverzamelingen en de rechtmatigheid van de verstrekking van gegevens daaruit voor onder meer onderzoek en beleid. De belangrijkste aanbevelingen uit het rapport zijn:

- de registraties dienen zo min mogelijk te werken met gegevens die direct of indirect herleidbaar zijn tot individuele personen;

³¹ College bescherming persoonsgegevens, uitspraak 'Registratie huisartsenposten van patiënten met crisisindicatie', 26 februari 2004, z2003-1597.

³² College bescherming persoonsgegevens, Online afsprakensysteem Flevoziekenhuis moet worden aangepast. Uitspraak 9 mei 2006, z2005-1372, P&I2006/215.

- herleidbaarheid van gegevens kan verregaand beperkt worden door het toepassen van Privacy-Enhancing Technologies (PET) zonder nadelig gevolg voor de onderzoekswaarde van de gegevens;
- patiënten van wie gegevens in de registraties worden opgenomen, dienen over het algemeen meer en beter geïnformeerd te worden;
- de beveiliging van de gegevens dient verbeterd te worden.

3.4.2 'Medische geheimen'

In haar boek 'Medische geheimen. Risico's van het elektronisch patiëntendossier' (2005) besteedt Karin Spaink aandacht aan de vraag of het medisch beroepsgeheim wel bewaard kan blijven in het elektronische tijdperk. Zij gaat in op de risico's die invoering van een landelijk elektronisch patiëntendossier (EPD) naar haar mening met zich brengt, zoals het risico op virussen. Bovenal werpt zij echter een kritische blik op het proces dat moet leiden tot de totstandkoming van het EPD. Ze merkt onder meer op dat de randvoorwaarden, zoals de beveiliging van de computers van hulpverleners, onvoldoende worden doordacht. Ook stelt ze dat het accent in de plannen de laatste jaren meer op de mogelijke kostenbesparingen en minder op de mogelijke kwaliteitsverbetering ligt. Daarnaast vraagt ze zich af hoe realistisch de hooggespannen verwachtingen zijn. De overheersende gedachte 'dat elektronische medische dossiers het antwoord zijn op een breed scala aan problemen in de gezondheidszorg, wordt zeker niet gestaafd, nog daargelaten dat de invoering van zulke dossiers op zich weer nieuwe problemen (en fouten) met zich meebrengt', aldus Spaink. Zij waarschuwt dan ook dat uit een eenvoudige aanpak de meeste winst te behalen valt en geeft in overweging het landelijk EPD te beperken tot de belangrijkste informatie van patiënten, bijvoorbeeld de informatie van huisartsen en medisch specialisten.³³

Ter gelegenheid van de publicatie van dit boek laat Karin Spaink in 2005 onderzoek doen naar de beveiliging van de huidige elektronische patiëntendossiers. Met toestemming van twee ziekenhuizen laat zij hun computersystemen hacken, waarbij zij toegang krijgt tot de medische gegevens van meer dan een miljoen mensen.³⁴ Dit onderzoek leidt tot Kamervragen en de toezegging van de Minister van VWS dat er een Wet op het EPD komt, waarin onder meer aandacht wordt besteed aan de beveiliging.³⁵ De ministeriële regeling bij de toekomstige Wet gebruik BSN in de zorg (Wbsn-z)³⁶ zal tot die wet er is regelen welke eisen er aan de beveiliging van elektronische patiëntendossiers worden gesteld.

4. Patiëntenidentificatie en fraudebestrijding

4.1 Wet- en regelgeving

De identificatieplicht is enige jaren terug ingevoerd in zorginstellingen met als doel identiteitsfraude te bestrijden. Fraude met ziekenfondspasjes kwam erg vaak voor en had niet alleen financiële gevolgen, maar ook gevolgen voor de verlening van zorg. De gegevens van alle patiënten die hetzelfde pasje gebruikten werden opgeslagen in hetzelfde dossier, met alle risico's van dien. Daarom werden patiënten die ten laste van de Algemene Wet Bijzondere Ziektekosten of de Ziekenfondswet zorg wilden genieten, verplicht zich te identificeren.³⁷

³³ Karin Spaink, *Medische geheimen. Risico's van het elektronisch patiëntendossier*. Nijgh & Van Ditmar / XS4ALL 2005.

³⁴ Karin Spaink, 'Het medisch geheim gehackt', *de Volkskrant* 3 september 2005.

³⁵ *Kamerstukken II*, 2005/06, 27 529, nr. 18.

³⁶ Wet gebruik burgerservicenummer in de zorg (Wbsn-z). *Kamerstukken II*, 2005/06, 30 380, nr. 2.

³⁷ Fraudebestrijding zorgverzekeringswetten, *Kamerstukken II*, 2003/04, 29 623, nr. 2.

Sinds 1 januari 2006 dient een verzekerde op grond van artikel 118 van de Zvw aan de persoon of instelling die de zorg of dienst zal verlenen, ter inzage een identiteitsbewijs te verstrekken (lid 1). Als het identiteitsbewijs niet onmiddellijk ter inzage kan worden verstrekt, dan kan de persoon of instelling toestaan dat uiterlijk binnen een termijn van 14 dagen aan deze verplichting wordt voldaan (lid 2). Een zorgaanbieder is verplicht om aan de hand van het ter inzage verstrekte document de identiteit vast te stellen van degene aan wie de zorg of dienst wordt verleend (lid 3).

De bestaande identificatieplicht wordt aangescherpt wanneer de Wbsn-z in werking treedt, naar verwachting op 1 januari 2007. Dit wetsvoorstel regelt de invoering en het gebruik van het Burgerservicenummer (BSN) in de zorgsector. Het BSN is een uniek identificerend nummer dat voor de meeste mensen hetzelfde nummer zal zijn als hun huidige sofi-nummer, maar voor veel meer doeleinden zal worden gebruikt. Het BSN wordt ingevoerd met het wetsvoorstel algemene bepalingen burgerservicenummer,³⁸ dat met name het gebruik van dit persoonsnummer binnen de overheidssector zal regelen. Voor het gebruik van het BSN binnen sectoren die in hoge mate bijzondere gegevens verwerken, zoals de zorgsector, is aanvullende wetgeving nodig. De Wbsn-z vervult die functie voor de zorgsector. Zorgaanbieders, zorgverzekeraars en indicatieorganen ('de gebruikers') worden op grond van dit wetsvoorstel verplicht het BSN te verwerken in hun administratie en bij de uitwisseling van persoonsgegevens.³⁹

De invoering van het BSN in de zorg heeft meerdere doeleinden. Het gebruik van één landelijk patiëntnummer wordt als voorwaarde gezien voor de invoering van een landelijk elektronisch patiëntendossier (EPD) en zijn voorlopers, het landelijk elektronisch medicatiedossier (EMD) en het waarneemdossier huisartsen (WDH), omdat een patiënt hiermee uniek kan worden geïdentificeerd wat de onderlinge communicatie aanzienlijk efficiënter en betrouwbaarder maakt. Als voorwaarde voor het EPD, EMD en WDH beoogt het BSN een belangrijke bijdrage te leveren aan het vergroten van de beschikbaarheid van medische gegevens en daardoor het verbeteren van de kwaliteit van de zorg. Daarnaast was de verwachting dat het wetsvoorstel zou bijdragen aan de bestrijding van fraude door het aanscherpen van de identificatieplicht in de zorg.⁴⁰ Tijdens de behandeling van de Wbsn-z in de Tweede Kamer is echter een motie aangenomen op grond waarvan de identificatieplicht in de eerstelijnszorg voor zover het bestaande patiënten betreft zal worden vervangen door een minder strikte vergewisplicht (de verplichting je bij twijfel te vergewissen van iemands identiteit).⁴¹

Om zorgvuldig gebruik te kunnen maken van het BSN in de zorgsector, worden de gebruikers verplicht de patiënt te identificeren en het bijbehorende BSN op te vragen (identificatie- en verificatieplicht). Ook wordt nader ingevuld welke beveiligingseisen gelden voor systemen van zorgaanbieders. Het toezicht op het gebruik van het BSN door zorgaanbieders komt bij de Inspectie voor de Gezondheidszorg te liggen, voor zover het de kwaliteit van de zorg betreft en de Nederlandse Zorgautoriteit (NZa) zal toezicht gaan houden op het gebruik van dit nummer door zorgverzekeraars en indicatieorganen. Uiteraard is het CBP als algemeen toezichthouder op de verwerking van persoonsgegevens ook bevoegd om toezicht te houden op de verwerking van het BSN. De uitbreiding van de bestaande identificatieplicht in de zorg houdt in beginsel in dat alle zorgaanbieders bij het eerste bezoek van een patiënt aan de

³⁸ Wet algemene bepalingen burgerservicenummer (Wabb). *Kamerstukken I*, 2005/06, 30 312, nr. A.

³⁹ V.C. Lucieer, Invoering van het burgerservicenummer in de zorg. *JPG* 2006/91.

⁴⁰ Tweede Kamer 2005/06, 30 380, nr. 3, p.3.

⁴¹ Tweede Kamer 2005/06, 30 380, nr.14.

zorginstelling hun identiteit moeten controleren en ook daarna nog, wanneer er twijfel bestaat over zijn identiteit. Aangezien dit één van de pijlers van het BSN-stelsel is en noodzakelijk om een zorgvuldige invoering van het BSN in de zorg te kunnen garanderen, hecht zelfs het CBP veel waarde aan de strenge identificatieplicht.⁴² Het CBP is dan ook allerm minst gelukkig met het voornemen om, ten gevolge van de Tweede Kamer-behandeling, de identificatieplicht in de eerstelijns ten aanzien van bestaande patiënten te wijzigen in een vergewisplicht.

De Wbsn-z is op 10 oktober 2006 met algemene stemmen aangenomen in de Tweede Kamer. Organisaties zoals de KNMG, NPCF en het CBP hebben in de periode daaraan voorafgaand de aandacht van de kamerleden gevraagd voor zaken als de beveiliging van patiëntendossiers en de toegang tot de zorg voor onverzekerden.⁴³ Dat aandacht voor de beveiliging van elektronische patiëntendossiers nodig is, blijkt wel uit het onderzoek van Karin Spaink (zie § 3.4.2 van deze bijdrage).

Begin 2006 ontving het CBP veel klachten van patiënten van wie de huisarts het sofinummer had opgevraagd. Aangezien dit (op een aantal uitzonderingen na) gelijk is aan het BSN, wilden veel huisartsen hun administratie alvast op orde brengen door de sofinummers van hun patiënten te registreren. Zo lang daar nog geen wettelijke grondslag voor bestaat (de AWBZ is een uitzondering) is het zorgaanbieders echter niet toegestaan het sofinummer te verwerken.⁴⁴

4.2 NVZ Notitie Identificatieplicht

Ook ziekenhuizen mogen ondanks de identificatieplicht het sofinummer nog niet verwerken in hun administraties. Dit is niet toegestaan zolang artikel 118, lid 3, Zvw nog niet in werking is getreden. Dat was medio oktober 2006 nog niet het geval. Deze informatie is onder andere te vinden in een notitie over de identificatieplicht van de NVZ vereniging van ziekenhuizen.⁴⁵

Na een korte beschrijving van de totstandkoming van de identificatieplicht bevat de notitie een overzicht van de verplichtingen voor de verzekerde, het ziekenhuis en voor de zorgverzekeraars. Zo is de verzekerde verplicht om een identiteitsbewijs ter inzage te verstrekken aan de persoon of instelling die de zorg of dienst zal verlenen. Kan een verzekerde geen identiteitsbewijs overleggen, dan kan de persoon of instelling er mee instemmen dat binnen 14 dagen alsnog aan deze verplichting wordt voldaan.

Het ziekenhuis is verplicht om aan de hand van het overgelegde identiteitsbewijs de identiteit vast te stellen van degene aan wie de zorg of dienst wordt verleend. Bovendien moet het ziekenhuis de in dat document opgenomen sofinummer in zijn administratie opnemen. Zoals gezegd is het ziekenhuis daartoe nog niet verplicht omdat artikel 118, derde lid, Zvw nog niet in werking is getreden. De persoon of instelling die de zorg of dienst verleent moet voorts het sofinummer van de verzekerde vermelden op de declaratie van de aan de verzekerde verleende zorg of dienst. Ook deze verplichting, die in artikel 118, vierde lid, Zvw is opgenomen, is nog niet in werking getreden.

De zorgverzekeraar is verplicht om het sofinummer van de verzekerden vast te leggen. Wie een zorgverzekering wenst te sluiten is daarom verplicht de sofinummers van de te verzekeren personen aan de zorgverzekeraar te verstrekken. Voorts moet de zorgverzekeraar de identiteit van de te verzekeren persoon vaststellen aan de hand van de documenten als bedoeld in artikel

⁴² V.C. Lucieer, Invoering van het burgerservicenummer in de zorg. *JPG* 2006/91.

⁴³ Zie http://www.cbweb.nl/documenten/adv_z2005-0807.shtml en <http://www.npcf.nl/?id=804>

⁴⁴ Zie ook College bescherming persoonsgegevens, Verbod op voortijdig opvragen sofinummer door huisartsen. Uitspraak CBP, 4 april 2006, z2006-0238; V.C. Lucieer, Invoering van het burgerservicenummer in de zorg. *JPG* 2006/91.

⁴⁵ NVZ vereniging van ziekenhuizen, *Notitie Identificatieplicht*, 5 december 2005. Beschikbaar op internet: <<http://www.nvz-ziekenhuizen.nl>>.

1 van de (algemene) Wet op de identificatieplicht. De aard en het documentnummer worden, evenals het sofinummer, opgenomen in de administratie.⁴⁶

De notitie bevat voorts een aantal concrete vragen en antwoorden (FAQ's) ter ondersteuning van de toepassing van de identificatieplicht in de praktijk.

5. Analyse en conclusies

De herziening van het zorgstelsel sinds 1 januari 2006 is een omvangrijke wetgevingsoperatie geweest. Bij deze stelselwijziging heeft de privacy van de patiënt c.q. van de verzekerde relatief veel aandacht gekregen. De privacybeschermende maatregelen die zijn getroffen bestaan uit wetgeving voor de gegevensuitwisseling rond zorgdeclaraties en zelfregulering voor onder meer de materiële controle door zorgverzekeraars. Daarnaast moeten technische maatregelen, te weten versleuteling van persoonsgegevens, de privacy garanderen rond het DBC-onderhoud. Een belangrijke ontwikkeling waarbij onvoldoende rekening is gehouden met de privacy van patiënten is de invoering van de DBC's. De verzekerde loopt dan ook nog steeds een privacyrisico als gevolg van de DBC-systematiek.⁴⁷

In de pers verschijnen, zo lijkt het, steeds vaker berichten over familiedrama's. Vaak zijn kinderen daarvan het slachtoffer. We verwijzen in dit verband naar het gezinsdrama in Roermond waar zes kinderen omkomen nadat hun vader het huis in brand stak (12 juli 2002), de driejarige peuter Savanna die in september 2004 dood in de kofferbak van een auto wordt gevonden en waarvoor de moeder en haar vriend worden veroordeeld, en het Maasmeisje Gessica, wiens lichaam in juni en juli 2006 in delen wordt gevonden in de Maas en waarvan de vader de verdachte is. Naar aanleiding van het laatstgenoemde geval pleiten B&W van Rotterdam voor een betere en snellere uitwisseling van persoonsgegevens uit de dossiers van de jeugdhulpverlening. Ter voorkoming van dergelijke misstanden wordt niet alleen voor een betere gegevensuitwisseling gepleit, maar wordt soms ook besloten tot het formaliseren van samenwerkingsverbanden. In bepaalde gevallen, bijvoorbeeld waarin maatschappelijke overlast en behoefte aan zorg bestaan, kunnen samenwerkingsverbanden maatschappelijke problemen verminderen of oplossen. Bij dergelijke samenwerkingsverbanden zijn ook steeds vaker zorgaanbieders betrokken (GGZ, GGD, Jeugdzorg). De huidige wet- en regelgeving met betrekking tot het medisch beroepsgeheim en andere privacybeschermende regelingen geeft onvoldoende duidelijkheid over de wijze waarop kan worden samengewerkt en gegevens kunnen worden uitgewisseld. Daarom worden vanuit de praktijk aanvullende maatregelen getroffen, zoals een Handreiking voor de gegevensuitwisseling bij bemoeizorg en een Modelconvenant voor gemeentelijke samenwerkingsverbanden ter bestrijding van problemen onder jongeren. Wij verwachten dat de behoefte aan gegevensuitwisseling in dit verband verder zal toenemen en dergelijke handreikingen en convenanten ook in de toekomst een belangrijke rol zullen blijven spelen bij het verschaffen van duidelijkheid aan samenwerkende instanties.

Begin 2007 wordt als het goed is eindelijk het Elektronisch Patiënten Dossier (EPD) ingevoerd. Bij zogeheten "koploperregio's" wordt dan gestart met de invoering van twee hoofdstukken uit het EPD-traject: het Elektronisch Medicatie Dossier (EMD) en het Waarneem Dossier Huisartsen (WDH). Na de implementatie in de koploperregio's worden deze hoofdstukken in de rest van Nederland geïmplementeerd. Inmiddels wordt ook al gewerkt aan een volgend hoofdstuk van het EPD: het Elektronisch Kinddossier (EKD).

⁴⁶ Artikelen 4 en 85 Zvw.

⁴⁷ Zie ook: College bescherming persoonsgegevens, *Jaarverslag 2005*. Den Haag: CBP juni 2006, p. 11 en p. 41.

Patiëntgegevens zijn straks landelijk raadpleegbaar voor alle zorgaanbieders. Om de privacy te waarborgen worden daarom eisen gesteld aan de unieke identificatie van de patiënt (door middel van het Burgerservicenummer) en van de zorgaanbieder (door middel van de Unieke Zorgverleners Identificatie-pas), de authenticatie van de zorgaanbieder en de autorisatie voor de zorgaanbieder. Voor een veilige gegevensraadpleging moet een Landelijk Schakel Punt garant staan. Deze centrale dienst moet de slogan van het EPD waarmaken: landelijk, veilig en betrouwbaar. Wij vinden het een goede zaak dat veel aandacht wordt besteed aan een landelijk, betrouwbaar en tegelijk veilig EPD. Er wordt vooralsnog echter onvoldoende aandacht besteed aan onder meer de autorisaties; daardoor is de kring van personen die toegang kunnen krijgen tot de gegevens breder dan noodzakelijk.

De unieke identificatie van patiënten in het kader van het EPD is in onze ogen van even groot belang als de identificatie van patiënten in ziekenhuizen. Op die manier kunnen immers persoonsverwisselingen worden voorkomen, zodat zorgaanbieders over de juiste medische dossiers van de juiste personen kunnen beschikken. Dat is in ons aller gezondheidsbelang. Niettemin leidt de huidige regeling in de praktijk nogal eens tot onduidelijkheden. Zo mogen ziekenhuizen het soft-nummer van patiënten niet vastleggen. Dat mag pas als de Wet gebruik BSN in de zorg is ingevoerd. Problemen met betrekking tot de identificatie van diverse groepen patiënten, zoals illegale patiënten, Alzheimer-patiënten met een verlopen paspoort (omdat die toch niet meer reizen) en kinderen tussen 12 en 14 jaar die zonder medeweten van hun ouders in het ziekenhuis behandeld willen worden maar geen eigen identiteitskaart hebben, leiden in ziekenhuizen tot praktische vragen rond de identificatieplicht. De identificatieplicht mag er niet toe leiden dat mensen de medisch-noodzakelijke zorg wordt onthouden. Overigens zijn wij wel van mening dat de identificatieplicht, immers één van de pijlers van het BSN-stelsel, noodzakelijk is. Met de wijziging van de identificatieplicht voor de eerstelijnszorg in een vergewisplicht, voor zover het bestaande patiënten betreft, wordt deze pijler naar onze mening ondergraven.⁴⁸

⁴⁸ Nieuwsbericht Ministerie van Volksgezondheid, Welzijn en Sport, 11 oktober 2006. Zie ook Tweede Kamer 2005/06, 30 380, nr.14.