

# Spoort de medische praktijk nog met de wettelijke regeling voor het beroepsgeheim?

*Jaap van der Wel*

## *Inleiding*

De gegevensuitwisseling in de zorg breidt zich steeds verder uit en in de nabije toekomst begint zelfs een landelijke verwijsindex. Daardoor dringt de vraag zich op of de wettelijke beschrijving van het medisch beroepsgeheim nog haantbaar is in de praktijk. Dit is een belangrijke vraag omdat uitgebreide gegevensuitwisseling zonder op de hedendaagse praktijk toegespitste wetgeving ten koste gaat van de privacy van patiënten.

## *Snapt de patiënt dit nog?*

Op meerdere plaatsen in de zorg doet zich de vraag voor of de wettelijke regeling van het medisch beroepsgeheim nog wel aansluit op de praktijk.

Zo wisselen in de eerstelijns zorg de vrijgevestigde apothekers<sup>1</sup> steeds meer medicatiegegevens uit. Deze gegevensuitwisseling keurde de toenmalige Registratiekamer goed met onder meer als argument: 'De samenwerking vindt thans plaats op beperkte schaal tussen huisartsen en apothekers zowel geografisch als in aantal deelnemers. Daarbij wordt aangesloten bij de maatschappelijke werkelijkheid en de belevingswereld van de patiënt'<sup>2</sup>. Het is geen letterlijke maar een pragmatische toepassing van art 7:457 lid 1 BW (Wgbo) en de toen geldende Wet Persoonsregistraties (WPR).

Het citaat dateert van 1998. Daarna is de gegevensuitwisseling tussen apothekers toegenomen. Past anno 2005 de uitwisseling van medicatiegegevens tussen de apothekers van de agglomeratie Den Haag wel in de belevingswereld van de patiënt? Waarschijnlijk niet want daarvoor is patiëntenvoorlichting vereist en die ontbreekt op tal van websites of in tal van folderrekken van huisartsen en apothekers.

## *Gegevenstoegang: ja, maar zóveel?*

Ook in de ziekenhuizen doet zich de vraag voor of de wettelijke regeling van het medisch beroepsgeheim toe is aan revisie. Van Veen constateert<sup>3</sup> dat de rechten voor het raadplegen van patiëntgegevens in geautomatiseerde systemen, grofmazig beheerd worden. Hij keurt dat goed met het argument dat er anders niet te werken valt. Alweer geen letterlijke, maar een pragmatische toepassing van de wet. Ik ben het met Van Veen eens dat een zekere grofmazigheid niet te vermijden is, maar hij gaat er aan voorbij dat er vaak nog onbenutte mogelijkheden zijn om ma-zen te verkleinen.

Softwarefabrikanten bijvoorbeeld kunnen de mogelijkheden voor toegangscontrole in hun ziekenhuissoftware verbeteren. Met de huidige software kan een ziekenhuisafdeling gewoonlijk wel de patiëntgegevens afschermen van andere afdelingen. Maar voor bijvoorbeeld de fysiotherapeut die op iedere afdeling enkele patiënten heeft, kan het lastig zijn om de gegevenstoegang te beperken tot de eigen patiëntenkring. Het is alles of niets. In de praktijk wordt het dan alles want het werk moet doorgaan<sup>4</sup>. Een fraai voorbeeld van de 'Law of Code' van Lessig<sup>5</sup>: niet de wet maar de software trekt de grenzen.

Daarnaast kunnen directies meer aandacht besteden aan het rechtenbeheer, een andere mogelijkheid. Dat kan door alert de gegevenstoegang op te heffen en nieuwe te creëren voor medewerkers die van afdeling veranderen.

Ten slotte is concretiseren van de bovengrens van grofmazigheid nog een mogelijkheid, waardoor duidelijker wordt waaraan zorginstellingen zich moeten houden<sup>6</sup>.

---

<sup>1</sup> Korthedshalve ga ik er van uit dat het wetsvoorstel is ingevoerd waarmee de Wgbo ook voor vrijgevestigde apothekers gaat gelden.

<sup>2</sup> CBP, *Medicatiebewaking voor centrale patiëntenregistratie*, 1998, blz. 8. ([http://www.cbpweb.nl/downloads\\_rapporten/rap\\_medicatiebewaking.pdf](http://www.cbpweb.nl/downloads_rapporten/rap_medicatiebewaking.pdf))

<sup>3</sup> mr. E.-B. Van Veen, *Het beroepsgeheim in de individuele gezondheidszorg*, in preadvies voor de jaarvergadering van de Vereniging voor Gezondheidsrecht 2004, p. 64.

<sup>4</sup> Zie voor meer achtergronden: Mr. drs. J.A. van der Wel, ing. N.L. Homma, *Gegevensbeveiliging aan alle kanten lek*, Automatisering Gids 5 september 2003. Zie <http://www.comfort-ia.nl/ag1.pdf>

<sup>5</sup> Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basic Books, 1999

<sup>6</sup> De regeling informatiebeveiliging Politie geeft in de tabel van bijlage 1 hiervan een voorbeeld.

Mogen de artsen van een klein ziekenhuis de gegevens van iedere patiënt van dat ziekenhuis inzien? Geldt dat ook voor een groot academisch ziekenhuis met 3000 medewerkers en zo niet, waar ligt de grens dan wel?

#### *De praktijk volgt de wet niet meer*

Als men grofmazigheid aanvaardt terwijl nog tal van verbeteringen mogelijk zijn, en dat is vaak het geval, dan verwijderd de praktijk zich steeds verder van de oorspronkelijke wettelijke regeling. Inmiddels zijn we bij een punt aangekomen dat de huidige wettelijke regeling van het medisch beroepsgeheim niet goed meer past in dit geautomatiseerde tijdperk.

#### *Met de BSN-invoering komt het weer goed!?*

Interessant is de vraag: komen de instanties die bezig zijn met nieuwe medische informatievoorziening en Burgerservicenummer (BSN) met moderniseringsvoorstellen?

Het 'Samenwerkingsverband Implementatieprogramma Wgbo', bestaande uit KNMG, Arcares, GGZ Nederland, LEVV, NPCF, NVZ en VGN, heeft recentelijk uitvoerig stilgestaan bij het medisch beroepsgeheim en vindt dat de huidige wet volstaat<sup>7</sup>.

De Werkgroep Sectorale Vertrouwensfunctie heeft een notitie geschreven over het gebruik van het Burgerservicenummer in de zorg<sup>8</sup>. Daarin komt ook deze werkgroep niet met voorstellen voor aanpassen van de wettelijke beschrijving van het medisch beroepsgeheim. Wel verwijst de werkgroep naar resultaten van het Nationaal ICT Instituut in de zorg (Nictiz)<sup>9</sup> waarin een belangrijk principe voor informatieuitwisseling is beschreven: *het brengprincipe*. Dit principe past niet in de huidige wetgeving zoals ik hierna zal toelichten.

Bij het brengprincipe plaatst een arts de relevante gegevens die de behandeling van de patiënt heeft opgeleverd, in de landelijke gegevensverzameling. Een andere arts die bij een latere behandeling gegevens nodig heeft over de betreffende patiënt, stelt vast of de patiënt instemt met ophalen van de gegevens dan wel of sprake is van spoed. Tegenover het brengprincipe staat het *haalprincipe*. Dit principe is het uitgangspunt van de Wgbo. De arts die patiëntgegevens nodig heeft, moet weten wie de gegevens beschikbaar heeft én diegene kunnen bereiken om aan de gegevens te komen. Het brengprincipe heft deze twee hindernissen op maar vereist een extra beslissing: die van de 'brenger' van de gegevens.

Dit is een novum en de Wgbo houdt daarmee geen rekening.

Het College Bescherming Persoonsgegevens heeft in de notitie van de werkgroep en het werk van Nictiz geen aanleiding gezien om kanteekeningen te plaatsen bij de Wgbo. Het tegenovergestelde is zelfs het geval: men wil meer duidelijkheid van de werkgroep over de manier waarop de praktijk zich aan de Wgbo gaat houden als de landelijke verwijsindex wordt ingevoerd<sup>10</sup>. Het is duidelijk dat de instanties die bezig zijn met nieuwe medische informatievoorziening, geen moderniseringsvoorstellen overwegen voor de wettelijke beschrijving van het medisch beroepsgeheim.

#### *Lichtpuntjes en vragen*

De eerder genoemde werkgroep doet wel een vernieuwend voorstel door een verwijzing naar de Norm voor Informatiebeveiliging in de Zorg (NEN 7510), die onder meer de directies van zorginstellingen verplicht om aandacht te schenken aan informatiebeveiliging. Ook vernieuwend is het voorgestelde gebruik van de UZI-pas, waarmee de identiteit van artsen met zekerheid geverifieerd kan worden langs elektronische weg.

Er zijn echter meer vernieuwingen nodig om de onduidelijkheden op te heffen die bij de betrokkenen nog resten.

De patiënten om te beginnen. Voor hen is niet altijd duidelijk hoever het gebruik van hun gegevens zich uitstrekt en in hoeverre zij daarop invloed kunnen uitoefenen omdat de voorlichting hierover niet altijd van de grond komt zoals dat zou moeten<sup>11</sup>.

<sup>7</sup> J.M. Witmer, R.P. de Roode (red.), Van wet naar praktijk. *Implementatie van de Wgbo*. Deel 4 Toegang tot patiëntgegevens. Utrecht: KNMG, met name blz. 24.

<sup>8</sup> Werkgroep Sectorale Vertrouwensfunctie in de zorg aan het College Bescherming Persoonsgegevens, *Notitie inzake het gebruik van BSN in de zorg en beoogde waarborgen*, aan het College Bescherming Persoonsgegevens d.d. 20 oktober 2004.

<sup>9</sup> Nictiz, Aorta, *Specificatie van de Basisinfrastructuur in de zorg*, versie 2.1, 17 november 2004, paragraaf 3.7.2.

<sup>10</sup> CBP, *Brief aan Minister Hoogervorst* van 22 november 2004.

<sup>11</sup> Wat voorlichting moet inhouden, is helder uitgewerkt in J.M. Witmer, R.P. de Roode (red.), Van wet naar praktijk. *Implementatie van de Wgbo*. Deel 4 Toegang tot patiëntgegevens. Utrecht: KNMG, bijlage 4. Zie [www.knmg.nl/wgbo](http://www.knmg.nl/wgbo).

Medici blijven met vragen zitten over de verantwoordelijkheden en de overlegprocedures die vooraf moeten gaan aan gegevensoverdracht aan de landelijke verwijsindex.

Voor beheerders van zeer grote gegevensverzamelingen, zoals de landelijke index, zijn meer technische uitgangspunten nodig dan alleen die voor het UZI-gebruik. Een voorbeeld is blokkeren van de toegang die systeembeheerders hebben met gegevensencryptie<sup>12</sup>.

En voor fabrikanten van softwarepakketten zijn ontwerpcriteria nodig, want tot op heden is privacy niet of nauwelijks als ontwerpcriterium meegenomen in ICT-toepassingen (evenzo: Hooghiemstra<sup>13</sup>).

Door deze vragen ondernemen de betrokkenen onvoldoende tot geen actie terwijl de gegevensuitwisseling doorgroeit. Zo komt de privacy van de patiënt onnodig in het gedrang.

#### *Wie kan dit oplossen?*

Beantwoorden van de vragen kan alleen in samspraak met de betrokkenen en vereist combineren van kennis van verschillende gebieden. Het is de vraag of dat lukt zonder een coördinerende rol van het ministerie van VWS. Ook het College Bescherming Persoonsgegevens kan een essentiële bijdrage leveren omdat daar veel kennis over dit onderwerp aanwezig is. Dat blijkt bijvoorbeeld uit het succes van het door het College ontwikkelde concept van de Privacy Enhancing Technology (PET).

#### *En de oplossing:*

De oplossing die hier nodig is, bestaat uit een combinatie van wetgeving, organisatie, procedures en technologie, kortweg een Privacy Enhancing Organisation (PEO). Alleen zo ontstaat de combinatie van openbaarheid, kracht en éénduidigheid van voorschrift die hier nodig is. Ideeën daarvoor zijn al uitgewerkt in de aangehaalde stukken van de werkgroep en het Nictiz, het geheel moet alleen nog uitgewerkt worden in (voorstellen voor) wet- en regelgeving. Samengetvat zijn de kernpunten daarvan (in het beknopte bestek van dit artikel ga ik niet in op de publiek- of privaatrechtelijke kanten van de oplossing en de wetten waarin dit geregeld zou moeten worden):

- 1) De verantwoordelijkheid van de arts die een patiënt behandelt: die noteert als ‘goed hulpverlener’ de kerngegevens (voorlopig alleen nog de medicatiegegevens) in een informatievoorziening met een brede gebruikers-

groep (de landelijke verwijsindex). Een ‘goed hulpverlener’ weet wat professioneel nodig is om te noteren. Een verplichting zoals Van Veen voorstelt<sup>14</sup>, lijkt me dan ook overbodig. Niet de wet maar de professionele voordelen en de noodzaak van de registratie moeten aanzetten tot registratie. Een ‘goed hulpverlener’ houdt óók rekening met de risico’s van gegevenslekken door de grotere gebruikersgroep en overlegt voor bijzonder gevoelige gegevens met de patiënt. De KNMG kan landelijke richtlijnen opstellen voor dit overleg. En artsenkoepels kunnen richtlijnen opstellen die aangeven welke gegevens wel en welke niet (psychiatrische gegevens bijvoorbeeld?) op de landelijke index thuishoren en voor welke medische discipline die gegevens zichtbaar mogen worden. Dit is trouwens ook nodig om de te vaak gehoorde idealisering van het Elektronisch Patiënten Dossier (EPD) als ‘bewaarplaats van alles voor iedere medicus’ terug te brengen tot nuchtere proporties. In dezelfde zin maken Zwetsloot en anderen duidelijk<sup>15</sup> dat het EPD pas betekenis kan krijgen door de mogelijkheden en het nut daarvan te concretiseren en te beperken tot de aantoonbaar nuttige;

- 2) De patiënt moet mogelijkheden krijgen om de toegang tot zijn informatie te beperken, aansluitend op de nieuwe mogelijkheden van informatieuitwisseling. Nederlanders willen dat, zoals blijkt uit een enquête van de Nederlandse Patiënten en Consumenten Federatie (NPCF)<sup>16</sup>. Lokale oplossingen bestaan

<sup>12</sup> Mr.dr. J. Nouwt wijst er in ‘Beveiliging van het EPD’, ICZ, oktober 2004 op dat de toenmalige Registratiekamer gegevensversleuteling van ieder EPD verlangde, een regel die in de zorg niet altijd wordt toegepast.

<sup>13</sup> Mr. drs. Theo Hooghiemstra, *Privacy bij ICT in de Zorg*, ZM Magazine d.d. 11 november 2002 zie [www.cbpweb.nl](http://www.cbpweb.nl)

<sup>14</sup> Van Veen in Het beroepsgeheim in de individuele gezondheidszorg, p. 49 e.v. optie 2.

<sup>15</sup> In die zin ook: Bertie Zwetsloot-Schonk, Kees Louwerse, Theo Hooghiemstra, *Patiënt gegevens te kijk, De verantwoordelijkheid van de behandelaar en toegankelijkheid van het EPD*, *Journal Privacy Gezondheidszorg*, januari 2004 (jaargang 5, nr 1).

<sup>16</sup> NPCF, *Kort eindverslag behorende bij project autorisatie EPD en patiëntenperspectief*, januari 2004, zie [www.nictiz.nl](http://www.nictiz.nl)

hier en daar al maar een uitgebreide, landelijke regeling hiervoor is lastig op korte termijn te realiseren. Een praktische start met een eenvoudig begin moet echter mogelijk zijn en is zelfs noodzakelijk. Hoe langer hiermee gewacht wordt, hoe lastiger het wordt om dat alsnog te doen. De medische informatieuitwisseling groeit namelijk door, zowel in omvang en als diversiteit. Het is nu of nooit;

- 3) De arts die gegevens opvraagt, mag dat doen als de patiënt daarmee heeft ingestemd of in geval van spoed. Deze arts krijgt de gegevens te zien voor zover de voorwaarden die de patiënt en de artsenkoepels stellen, dat toelaten;
- 4) De mogelijkheden van bestraffing van gegevensmisbruik of niet aanleveren van gegevens wordt ondergebracht in het medisch tuchtrecht. Dat geeft betere mogelijkheden dan de geldboetes die de eerder aangehaalde notitie van de werkgroep voorstelt. Geldboetes volstaan niet als een arts vergelijkbaar nonchalant zou zijn als de officier van justitie die zijn PC bij het huisvuil zette.

In uitvoeringsmaatregelen worden de kernpunten van de technische beveiliging van de informatie infrastructuur bindend opgelegd aan de organisatie die een landelijke verwijzindex gaat beheren. Voorbeelden zijn beschikbaar<sup>17</sup>.

#### *Wat recht is, dat bepaalt de software*

Een essentieel onderdeel van de uitvoeringsmaatregelen is de logging van raadplegingen om achteraf de rechtmatigheid daarvan vast te kunnen stellen in combinatie met de *bewijsbaarheid van het bewust raadplegen*. De werkgroep stelt in de eerder aangehaalde notitie *de gebruikersvriendelijkheid van raadplegen* voorop. Als dat er echter toe leidt dat de arts door de patiënten

kan bladeren op zoek naar de goede, dan zou dat iedere poging om gegevensmisbruik juridisch hard te maken zodanig compliceren dat er van de vervolging in de praktijk niets terecht komt. Ook de definiëring van de loggegevens die nodig zijn om tot strafvervolging over te kunnen gaan, is nog een onverkend terrein. Sommige discussies die ik beluister, richten zich op het loggen van elk detail van de raadpleging, waardoor het logbestand zelf weer een monstrum wordt vanuit privacy oogpunt. Een verstandiger aanpak zou zijn de logging van het minimum aan gegevens dat juridisch volstaat om misbruik aan te tonen voor zowel de tucht- als de strafrechter.

#### *Klaar?*

Verder uitwerken van deze PEO is niet eenvoudig. Gegevensuitwisseling en privacy zijn elkaars tegenpolen en dan kunnen in de kleinste details de grootste problemen schuilgaan. In dat krachtenveld hebben partijen wellicht de neiging om de oplossing bij een ander te zoeken waardoor een patstelling ontstaat. Doorbreken van die patstelling is nóg een reden om de wettelijke regeling van het medisch beroepsgeheim te moderniseren.

mr. drs. J.A. van der Wel ([jvdwel@comfort-ia.nl](mailto:jvdwel@comfort-ia.nl)) is directeur van Comfort-IA en lid van de NEN-normcommissie voor informatiebeveiliging in de zorg.

---

<sup>17</sup> AIVD, *Voorschrift Informatiebeveiliging Rijksdienst – bijzondere informatie*(VIR-bi) zie [www.aivd.nl](http://www.aivd.nl) en het overzichtsartikel van Kees Louwerse, Leo Valentijn, Jaap van der Wel: *Vir-bi: interessant voorbeeld voor beveiliging informatie*, Automatisering Gids 22 oktober 2004, te vinden op [www.comfort-ia.nl/virbi.pdf](http://www.comfort-ia.nl/virbi.pdf). Evenzo de wet- en regelgeving voor de elektronische handtekening.