VERENIGING VOOR
GEZONDHEIDSRECHT

Preadvies uitgebracht ten behoeve van de jaarvergadering van de Vereniging voor Gezondheidsrecht op 23 april 1999

Informatietechnologie in de gezondheidszorg

mr P.J. Hustinx

INFORMATIETECHNOLOGIE IN DE GEZONDHEIDSZORG

Mr. P.J. Hustinx

Preadvies voor de Vereniging voor Gezondheidsrecht

Jaarvergadering 23 april 1999

Informatietechnologie in de gezondheidszorg
Mr. P.J. Hustinx

Vereniging voor Gezondheidsrecht
Jaarvergadering 23 april 1999

VOORWOORD

Toen ik ruim een jaar geleden op mij nam het preadvies voor de jaarvergadering van 1999 te verzorgen, stond mij een uitgewerkte beschouwing voor ogen waarin de ontwikkelingen op het terrein van de informatietechnologie binnen de gezondheidszorg en het beleid dat de overheid daarbij volgt, werden geconfronteerd met beginselen van gezondheidsrecht en privacybescherming. Een zinvol mengsel dus van recht en technologie, theorie, praktijk en beleid. In de tijd die er sindsdien is verstreken, heb ik over de vraagstelling rustig kunnen nadenken. Het dagelijkse werk bij de Registratiekamer gaf ook steeds weer aanknopingspunten om mijn gedachten te ordenen en aan te scherpen. Naarmate de tijd vorderde heb ik echter ook moeten ervaren dat de gelegenheden om de beoogde beschouwing op papier te zetten schaars waren en bleven. Het dagelijkse werk stelde eisen, de actuele ontwikkelingen rond de Wet bescherming persoonsgegevens vroegen aandacht, en ook internationale verplichtingen eisten hun tol. Dat alles heeft er toe geleid dat dit preadvies uiteindelijk in betrekkelijk korte tijd en onder hoge tijdsdruk is geschreven, en dat het in elk geval veel later is opgeleverd dan de bedoeling was. Een bijkomend gevolg is dat ik mij de nodige beperkingen heb moeten opleggen.

Bij de uitwerking van mijn gedachten heb ik gebruik kunnen maken van standpunten die in de afgelopen jaren door de Registratiekamer zijn ingenomen en de inzichten die daarbij in overleg met anderen zijn ontwikkeld. Met name wil ik hier degenen noemen die in de loop van die jaren binnen de Registratiekamer in het bijzonder of in belangrijke mate werkzaam zijn geweest op het terrein van de gezondheidszorg: Huib Gardeniers, Jos Dute, Pieter Ippel, Anton Rommelse, Machel Nuyten, Guus de Heij, Theo Hooghiemstra en Annemarie ter Linden. De gedachten die in dit preadvies worden ontvouwd, zijn mede door hen ontwikkeld. Ik ben hun allen dankbaar voor de bijdragen die zij hebben geleverd. Voor de uiteindelijke inhoud en de vorm van dit preadvies, en dus ook voor alle gebreken die er aan kleven, ben ik alleen verantwoordelijk. Ik hoop dat de jaarvergadering er voldoende inspiratie uit zal putten, en zie uit naar de discussie.

Mr. P.J. Hustinx

INHOUDSOPGAVE Blz

1. INLEIDING

1.1. Informatie in de gezondheidszorg

De zorgvuldige omgang met vertrouwelijke informatie van patiënten is altijd een belangrijk aandachtspunt geweest in de gezondheidszorg en het gezondheidsrecht. Het leerstuk van het medisch beroepsgeheim staat daarbij centraal. Dit berust op het uitgangspunt dat iedereen zich om hulp of advies tot een arts of een andere medische hulpverlener moet kunnen wenden zonder de vrees dat informatie die hij of zij in dat kader aan de betrokken hulpverlener toevertrouwt, bij een ander bekend wordt. Duidelijkheid over de reikwijdte, de consequenties en de uitzonderingen op het medisch beroepsgeheim is in het belang van iedere patiënt en van de samenleving als geheel. De kwaliteit van de gezondheidszorg hangt in de praktijk dan ook mede af van de mate waarin die duidelijkheid is verzekerd. De laatste jaren is daarnaast steeds meer aandacht ontstaan voor de wijze waarop de informatie over de patiënt wordt verkregen, vastgelegd en bewaard. Dat heeft geleid tot regels over de inrichting en het beheer van patiëntendossiers en tot specifieke rechten van patiënten met betrekking tot de inhoud van deze dossiers. Het hier zeer in het kort aangeduide complex van rechten en verplichtingen staat in het teken van de zorg van een goed hulpverlener.[1] De zorg voor de patiënt en de zorg voor de informatie over de patiënt zijn in de gezondheidszorg dus nauw verweven.

Hoewel de zorg voor de gezondheid uiteraard nog steeds voorop staat, kan de gezondheidszorg in toenemende mate ook worden beschreven als een informatieverwerkend proces, waarin informatie over patiënten wordt verzameld, vastgelegd, toegankelijk gemaakt en uitgewisseld, en waarin voortdurend ook nieuwe informatie over patiënten wordt gegenereerd en in de verwerkingen wordt betrokken. Dat geldt voor het "primaire proces" – het leveren van de zorg voor de gezondheid – het geldt ook en in nog veel sterkere mate voor de samenhangende processen van intern beheer, financiering, wetenschappelijk onderzoek en beleidsontwikkeling. Vanaf het moment dat een patiënt zich wendt tot een huisarts of medisch specialist, is er sprake van een constante stroom van gegevens over de zorgvraag, de voorgeschiedenis, de aard en de duur van de behandeling, de financiële afwikkeling, de gevolgen

[1] Zie artikel 7:453 e.v. BW.

voor het budget en tal van andere zaken die daarbij relevant kunnen zijn. In feite begint de gegevensstroom al eerder, omdat ook preventie en zorgplanning het nodig maken te weten waar de problemen en de behoeften kunnen liggen. De aard van de betrokken gegevens en de kring waarbinnen deze beschikbaar komen, zijn afhankelijk van het doel waarvoor zij zijn verkregen. De eerder bedoelde regels over het patiëntendossier en de reikwijdte van het beroepsgeheim zijn in dit verband mede bepalend voor de aard van het gegevensverkeer. Binnen de kring van de directe zorg – hoe beperkt of hoe ruim ook bemeten – zullen dus andere gegevens omgaan dan daarbuiten.

Toch zijn er ook duidelijke raakvlakken en zelfs knooppunten in het gegevensverkeer. De zorgsector vormt in de meeste gevallen de bron van de informatie en treedt dus ook op als poortwachter naar andere sectoren die belangstelling hebben. In de praktijk is de feitelijke zorg voor de gegevens echter vaak gedelegeerd of ondergebracht bij een centraal punt. Dit verschijnsel doet zich duidelijker voor naarmate de schaal van het gegevensverkeer toeneemt, met name in ziekenhuizen en andere grotere verbanden. Het is dan zaak de verkeersregels voor en tussen de verschillende sectoren én de ratio daarvan goed in het oog te houden, omdat anders gemakkelijk de neiging ontstaat om het geheel ook in feite als één geheel te behandelen. De schaalvergroting in de gezondheidszorg en de daarmee samenhangende verschuivingen in zeggenschap en zorg voor het gegevensverkeer, leiden zodoende tot de vraag of de uitgangspunten die aan de bestaande verkeersregels ten grondslag liggen nog wel geldig zijn, en zo ja welke voorzieningen nodig zijn om te verzekeren dat deze in een veranderende omgeving tot hun recht komen. Deze vraag staat in dit preadvies centraal en vormt de achtergrond van een globale verkenning van de toepassing van nieuwe informatietechnologie, die in de gezondheidszorg steeds meer wordt ingezet om het gegevensverkeer mogelijk te maken en in goede banen te leiden. Een korte schets van de huidige stand van zaken op dit gebied lijkt nuttig als nadere inleiding en opmaat voor de verdere discussie.

1.2. Informatietechnologie in de gezondheidszorg

Zoals in de meeste sectoren van de samenleving heeft de toepassing van de informatietechnologie in de gezondheidszorg de laatste jaren een sterke ontwikkeling doorgemaakt.[2] De door de minister van VWS in februari 1996 uitgebrachte Beleidsnotitie "Informatietechnologie in de zorg"[3] opende zelfs met de vaststelling dat informatietechnologie (IT) en gezondheidszorg onlosmakelijk aan elkaar zijn verbonden. De medische praktijk, het functioneren van de ziekenhuisorganisatie en de communicatie tussen diverse partijen in de zorgsector zijn volgens de notitie niet goed meer denkbaar zonder toepassing van moderne IT. Het beroep dat in de gezondheidszorg wordt gedaan op een stijgende kwaliteit en grotere doelmatigheid van zorg is daar mede debet aan. In de notitie werd ook gewezen op diverse veranderingen die gevolgen hebben voor de organisatie en werkwijze van de gezondheidszorg en waarbij IT een belangrijk hulpmiddel kan zijn. Zo is de modernisering van de curatieve zorg voor een groot deel gericht op samenwerking tussen de beroepsgroepen binnen en buiten het ziekenhuis en de versterking van de positie van de huisarts in de patiëntenzorg. IT kan een hulpmiddel zijn om de samenwerking en "transmuralisering" van de zorg te ondersteunen. Ook krijgen de verzekeraars een zwaardere rol in de besturing van de curatieve zorg. Informatie over de prestaties en kosten van de zorg en communicatie tussen de verzekeraar en de zorginstellingen kan met moderne IT worden ondersteund.[4]

De Beleidsnotitie signaleerde ook duidelijke tekortkomingen. Zo heeft de IT zich in de zorgsector op diverse manieren ontwikkeld, zodat een onevenwichtige situatie is ontstaan. [5] De automatiseringsgraad binnen de openbare apotheken was destijds al nagenoeg 100 %. Bijna 90 % van de huisartsen was "geautomatiseerd", waarbij ruim 40 % van het totaal ook de medische gegevens in de computer registreerde en 25 % "papierloos" werkte. Elektronische communicatie tussen huisartsen en

---

[2] Zie voor een vrijwel uitputtend overzicht van de ontwikkelingen en de stand van zaken: S. Nouwt, Zorg voor privacy, Informatietechnologie en informationele privacy in de gezondheidszorg, diss. Tilburg, Den Haag 1997, blz. 253-315.

[3] TK, 1995-1996, 24 629, nr. 1

[4] idem, blz. 3

[5] idem, blz. 12 e.v. Zie ook de publikatie "Informatietechnologie in de zorg: feiten en opinies", Rijswijk 1995.

specialisten stuitte evenwel op problemen, omdat de laatste categorie nog nagenoeg niet was "geautomatiseerd" en zijn medische gegevens in elk geval nog niet in een met huisartsen vergelijkbare mate met behulp van computers verwerkte. Binnen ziekenhuizen zou sprake zijn van een sterke eilandencultuur, waarbij afdelingen – ook medische specialismen onderling en versus bedrijfsmanagement – hun eigen weg gaan. Binnen de academische en algemene ziekenhuizen gaat het vaak om een op de instelling afgestemd ziekenhuisinformatiesysteem (ZIS) met als kernen de financiële en personeelsadministratie, diverse andere aspecten van bedrijfsvoering, zoals inkoop en voorraadbeheer, en patiëntenadministratie in verband met facturering, verslaglegging e.d. Met de geautomatiseerde ondersteuning van het primaire proces – het feitelijk leveren van zorg – was het in de ziekenhuizen volgens de notitie nog pover gesteld.

Een belangrijke oorzaak van deze onevenwichtige situatie lag volgens de notitie in het ontbreken van een samenhangende visie bij het veld. In oktober 1996 heeft vervolgens de toenmalige voorlopige Raad voor de Volksgezondheid en Zorggerelateerde dienstverlening (RVZ) een advies uitgebracht, waarin een dergelijke visie voor de langere termijn was neergelegd.[6] In deze visie stonden drie elementen centraal: het gebruik van een *zorgchip*, een chipkaart die de patient bij zich draagt en waarop staat waar welke informatie over de patiënt beschikbaar is; de vervanging van papieren dossiers door *elektronische patiënten dossiers*, waarin zorgverleners de gegevens gestructureerd en gestandaardiseerd in digitale vorm vastleggen; en een *elektronische snelweg* die zorgverleners in staat stelt via de zorgchip, met toestemming van de patiënt, toegang te krijgen tot voor de zorg relevante informatie die elders aanwezig is in elektronische (deel)dossiers. Patiëntengegevens dienden in deze visie in cryptografisch versleutelde vorm verzonden te worden. Om privacyredenen werd hierbij geen gebruik gemaakt van het sofi-nummer voor zorgdoeleinden. Problemen bij het realiseren van deze visie zag de RVZ vooral bij de benodigde standaardisatie rond inhoud en gebruik van elektronische patiëntendossiers, de kennis van IT, de totstandkoming van een infrastructuur die voldoet aan de hoge eisen van de zorgsector, en de privacywetgeving.

---

[6] Informatietechnologie in de zorg, Advies en Achtergronden (Deel I en II), Zoetermeer 1996

De Minister van VWS reageerde een jaar later in de Nota "Informatievoorziening in de zorg".[7] Zij onderschreef hierin de lange-termijnvisie van de RVZ in grote lijnen, maar legde de accenten voor de korte termijn op sommige punten iets anders. Hier wilde zij onder meer aandacht besteden aan het elektronisch patiëntendossier (EPD) en de chipcard in combinatie met de elektronische snelweg. Als belangrijke randvoorwaarden zag de minister privacybescherming, consensus over patiëntenidentificatie, en normalisatie/standaardisatie. Anders dan de RVZ zag zij privacybescherming niet als een belemmering, maar als een voorwaarde voor toepassing van IT in de zorg.

In de begeleidende brief van de minister werd nader ingegaan op de verantwoordelijkheden. Zorgaanbieders zijn volgens de opvatting van de minister primair verantwoordelijk voor een goede inrichting van de informatievoorziening in het primaire proces. De informatie die zij opslaan en uitwisselen met patiënten en andere zorgverleners is vooral bedoeld voor de directe zorgverlening. De doelmatigheid van de zorg dient te worden bewaakt met geaggregeerde informatie die niet tot een een individu herleidbaar is. Deze kan dienen als stuurinformatie bij het afsluiten van zorgcontracten tussen verzekeraars en zorgaanbieders, als spiegelinformatie voor de zorgaanbieder zelf en als algemene informatie voor patiënten. Op macroniveau bestaat bij de rijksoverheid vooral behoefte aan beleidsinformatie die wordt verkregen door aggregatie van gegevens uit het primaire proces of het verkeer tussen zorgaanbieders, verzekeraars en patiënten. Geaggregeerde informatie van verzekeraars of tussenkomende instanties zoals CBS, SIG en NZI is veelal voldoende. De verantwoordelijkheid van de overheid op het macroniveau strekt zich uit tot haar wettelijke taken en de daarvoor benodigde informatie die op wettelijke of vrijwillige basis wordt verkregen. Daarnaast faciliteert de overheid informatievoorziening op micronivèau rechtstreeks (onderzoek en voorbeeldprojecten) of via randvoorwaarden (privacywetgeving en standaardisatie). Elk van deze onderwerpen krijgt in de nota nadere aandacht. Inmiddels lijkt VWS zich overigens weer opnieuw en wat sterker dan tevoren bezig te houden met de strategische vragen op dit gebied.[8]

---

[7] TK 1997-1998, 25 669, nrs. 1 en 2

[8] Zie Financieel Dagblad van 28 december 1998: "VWS trekt zware wissel op verzekeraars" (interview met secretaris-generaal mr. R. Bekker)

1.3. Plan van behandeling

Het hiervoor aangeduide onderwerp is zeer breed. Nadere afbakening en selectie zijn dus geboden. In het licht van het voorgaande heb ik er voor gekozen om eerst in te gaan op de randvoorwaarden in de sfeer van de privacywetgeving, de bestaande en de komende, en daaruit een toetsingskader te destilleren (hoofdstuk 2). Vervolgens zal ik aandacht besteden aan de mogelijkheden om de toepassing daarvan in de sfeer van de IT zelf te faciliteren door het gebruik van *privacy enhancing technologies* (hoofdstuk 3). Tegen deze achtergrond zal wat preciezer worden gekeken naar de vragen die zich voordoen bij het elektronisch patiëntendossier (hoofdstuk 4) en het mogelijke gebruik van chipcards (hoofdstuk 5). In beide gevallen blijkt de identificatie van patiënten een belangrijke kwestie waarover praktijk en beleid zich momenteel het hoofd breken (hoofdstuk 6). Na deze verkenningen richt ik mij op de relatie met de informatiebehoeften buiten de zorg met betrekking tot financiering, onderzoek en beleid, en de toenemende ambities die zich daar aftekenen (hoofdstuk 7). In het afsluitende hoofdstuk trek ik conclusies uit het voorafgaande en tracht ik tot een antwoord te komen op de eerder aangeduide vragen over uitgangspunten en voorzieningen in een veranderende omgeving (hoofdstuk 8).

PRIVACYWETGEVING

1.1. Algemeen

De ontwikkeling van IT is de afgelopen jaren niet alleen in Nederland, maar in de meeste landen van West-Europa gepaard gegaan met de totstandkoming van wetgeving ter bescherming van de persoonlijke levenssfeer in verband met de verwerking van persoonsgegevens. De hoofdlijnen daarvan zijn vervat in het Verdrag van Straatsburg inzake gegevensbescherming (1981) en nader uitgewerkt in een EG-richtlijn van 24 oktober 1995 (Richtlijn 95/46/EG). "Gegevensbescherming" wordt in beide omschreven als het waarborgen van de fundamentele rechten en vrijheden van natuurlijke personen, en met name het recht op persoonlijke levenssfeer, in verband met de verwerking van persoonsgegevens.[9] Het gaat hier dus niet alleen om het recht op privacy, maar ook om andere fundamentele aangelegenheden, zoals gelijke behandeling, vrijheid van meningsuiting en "fair play".

De relatie met het recht op privacy is echter nog steeds sterk. Zo heeft het Europese Hof voor de Rechten van de Mens in zijn arrest van 25 februari 1997 in de zaak Z. tegen Finland[10] gesteld, dat de bescherming van persoonsgegevens van fundamentele betekenis is voor de mogelijkheid om te genieten van het recht op privé- en familieleven als bedoeld in artikel 8 EVRM. In dat kader verwees het Hof uitdrukkelijk naar het Verdrag van Straatsburg. Hoewel het in deze zaak ging om de bescherming van medische gegevens, zoals HIV-status, kan hieruit worden afgeleid hoe het Hof de relatie ziet tussen het Verdrag van Straatsburg en artikel 8 EVRM. Dit artikel omvat kennelijk ook de verplichting om met name gevoelige persoonsgegevens in het nationale recht de bescherming te bieden die het verdrag met zich meebrengt. In artikel 10 Grondwet zijn beide invalshoeken verenigd.

De Wet persoonsregistraties (WPR) is sinds medio 1989 in werking om uitvoering te geven aan de verplichtingen van Nederland op dit gebied. Ingevolge Richtlijn 95/46/EG zal de WPR in de loop van dit jaar worden vervangen door de Wet bescherming persoonsgegevens (WBP). Een desbetreffend wetsvoorstel is aanhangig bij de Tweede

---

[9] Zie artikel 1 Verdrag van Straatsburg en artikel 1 van Richtlijn 95/46/EG.
[10] NJCM Bulletin, 1997, nr. 6, blz. 720-721 (par. 95).

Kamer. [11] De WBP zal evenals de WPR ook van toepassing zijn op de verwerking van patiëntengegevens in de gezondheidszorg. De WGBO blijft daarbij onverminderd van kracht.[12]

Uit het Verdrag van Straatsburg, de EG-richtlijn, de WPR en de WBP zijn de volgende *hoofdbeginselen* af te leiden voor de verwerking van persoonsgegevens in de gezondheidszorg of daarbuiten.

Allereerst dient aandacht te worden besteed aan de *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 betrokkene. Het gaat hier in feite om het principe van "fair play".

Het principe van de *doelbinding* vereist dat persoonsgegevens slechts worden verzameld voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden, dat niet meer gegevens worden verwerkt dan voor die doeleinden noodzakelijk is en dat deze gegevens niet worden gebruikt voor doeleinden die daarmee niet verenigbaar zijn.

Daarnaast moet er volgens de richtlijn steeds sprake zijn van een *rechtmatige grondslag* voor de verwerking van persoonsgegevens. Het kan hierbij gaan om de toestemming van de betrokkene, de uitvoering van een overeenkomst waarbij deze partij is, de nakoming van een wettelijke verplichting of de uitvoering van een publiekrechtelijke taak door een bestuursorgaan. Ook kan een gerechtvaardigd belang de verwerking noodzakelijk maken, terwijl het belang van de betrokkene daardoor niet wordt geschaad. Bij toestemming gaat het steeds om een vrije gerichte toestemming die op toereikende informatie berust.

In verband met de *kwaliteit van de gegevens* moeten deze 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 zo nodig te worden bijgewerkt. In dit verband dienen alle redelijke maatregelen te worden getroffen om tekortkomingen te herstellen.

---

[11] TK 1997-1998, 25 892, nrs. 1-3

[12] Het in februari 1999 ingediende voorstel voor een Aanpassingswet (TK 1998-1999, 26 410, nrs. 1-3) laat de WGBO ongemoeid.

In het kader van de *beveiliging* zal voor passende organisatorische en technische maatregelen gezorgd moeten worden tegen verlies van gegevens of tegen iedere vorm van onrechtmatige verwerking.

Voor bijzondere gegevens of typen van gegevensverwerking kunnen *aanvullende wettelijke voorschriften* gelden. Hierbij valt te denken aan geheimhoudingsverplichtingen, het Besluit gevoelige gegevens (BGG) en de bepalingen in het Burgerlijk Wetboek omtrent de overeenkomst inzake de geneeskundige behandeling (WGBO).

Verder brengen de *rechten van betrokkenen* mee dat deze vrijelijk en zonder onredelijke beperkingen gebruik kunnen maken van rechten op kennisneming, correctie en verzet. Dit laatste recht is in de richtlijn in bepaalde situaties toegevoegd, zodat betrokkenen nu meer invloed kunnen uitoefenen.

Het spreekt voor zich dat steeds moet worden voorzien in passende mogelijkheden voor *controle en handhaving*. In dat kader voorziet de richtlijn tevens in een onafhankelijk toezicht.

1.2. WPR en WGBO

Bij de totstandkoming van de WGBO is de verhouding tussen die wet en de WPR expliciet en uitvoerig aan de orde geweest.[13] Daaruit kan in de eerste plaats worden opgemaakt dat de WGBO geen lex specialis is ten opzichte van de WPR, maar dat beide als onderling aanvullend moeten worden gezien en dat bij eventuele strijdigheid voorrang moet worden gegeven aan de bepaling die de meeste bescherming biedt aan de betrokken patiënt.[14]

De onderlinge verhouding tussen beide wetten is alleen van belang waar zij elkaar overlappen. Dat kan zich voordoen als de dossierplicht van de WGBO wordt nagekomen door het aanhouden van een of meer persoonsregistraties. Het begrip "dossier" is een verzamelbegrip voor het geheel van gegevens over één patiënt, ongeacht of deze onderdeel zijn van een persoonsregistratie. Bij het begrip "persoonsregistratie" is

[13] Zie de memorie van antwoord: TK 1990-1991, 21 561, nr. 6, blz. 6-13 en blz. 38-39.
[14] Idem, blz. 6, 9, 12 en 13.

de structuur juist weer beslissend. Een bijkomend probleem is dat het begrip "hulpverlener" van de WGBO niet behoeft samen te vallen met het begrip "houder" van de WPR. Zo kan een ziekenhuis houder zijn van een persoonsregistratie, terwijl de zeggenschap over opgenomen gegevens deels bij het ziekenhuis en deels bij specialisten binnen het ziekenhuis berust.[15]

Volgens artikel 18 WPR mag een persoonsregistratie slechts worden aangelegd indien dat noodzakelijk is voor een goede vervulling van de taak van de houder en mag deze slechts persoonsgegevens bevatten die voor het doel van de registratie noodzakelijk zijn. Artikel 7:454 lid 1 BW hanteert in feite dezelfde maatstaf voor de dossierplicht, door te verwijzen naar wat noodzakelijk is voor een goede hulpverlening. De in artikel 7:454 lid 2 BW vervatte verplichting voor de hulpverlener om desgevraagd een verklaring van de patiënt aan het dossier toe te voegen gaat verder dan de WPR, omdat de patiënt in principe vrij is om zelf de inhoud van de verklaring te bepalen. De in artikel 7:454 lid 3 BW neergelegde bewaarplicht van tien jaar, of zoveel langer als uit de zorg van een goed hulpverlener voortvloeit, is weer te zien als een concretisering van de algemene norm uit de WPR. De in artikel 7:455 BW vervatte (voorwaardelijke) verplichting om gegevens op verzoek van de patiënt te vernietigen, gaat echter weer verder dan de WPR die alleen voorziet in een verwijdering van gegevens die ten onrechte zijn opgenomen. Het BGG bevat voor de gezondheidszorg geen relevante nadere beperkingen.

Artikel 7:456 BW regelt het recht op inzage en afschrift van gegevens, ook voor patiëntendossiers die niet geheel of ten dele door de WPR worden bestreken. Voor registraties onder het bereik van de WPR gaat de preciezere regeling van die laatste wet echter doorgaans voor, met name op het punt van de termijn en de in rekening te brengen kosten.[16] Op het punt van de uitzonderingen is de WGBO echter weer strikter, zodat inzage en afschrift in principe alleen achterwege kunnen blijven

[15] Idem, blz. 9 e.v. Hier wordt ook ingegaan op mogelijkheden om dergelijke problemen in de praktijk te ondervangen.

[16] Zie het Besluit van 5 juli 1989, Stb. 281 op grond van artikel 36 WPR (Tientjesbesluit), zoals gewijzigd bij Besluit van 8 oktober 1998, Stb. 594, dat voorziet in een hoger tarief voor afschriften van 50 bladzijden of meer, andere gegevensdragers dan papier, of moeilijk toegankelijke registraties. Een kostenvergoeding voor inzage is op grond van de WGBO niet mogelijk.

voor zover dit noodzakelijk is ter bescherming van de persoonlijke levenssfeer van een ander.

De artikelen 7:457 en 458 BW regelen in hoeverre de hulpverlener tot geheimhouding verplicht is. Deze regeling sluit aan op artikel 11 lid 3 WPR, volgens welke een verstrekking achterwege blijft voor zover uit hoofde van ambt, beroep of wettelijk voorschrift geheimhouding – in concreto – geboden is. Voor het overige blijft de regeling van de WPR onverminderd van kracht. De geheimhoudingsplicht in de WGBO is zodanig omschreven, dat de hulpverlener er voor zorg moet dragen dat gegevens ook intern niet ter kennis komen van onbevoegden. Dit is met name van belang binnen grotere organisaties. In feite betekent dit dat ook sprake is van een beveiligingsplicht. Voor persoonsregistraties vloeit deze al voort uit artikel 8 WPR.

De geheimhoudingsplicht geldt ingevolge artikel 7:457 lid 2 BW niet tegenover degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst of optreden als vervanger van de hulpverlener, voor zover de verstrekking van informatie noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden. Het betreft hier in de praktijk veel voorkomende gevallen, die vroeger werden benaderd aan de hand van veronderstelde of stilzwijgende toestemming en waarvoor een duidelijker afbakening wenselijk geacht werd.[17] Bij de mondelinge behandeling is de vraag aan de orde gesteld of het principe van de veronderstelde toestemming niet in de wettekst tot uitdrukking moest worden gebracht. Volgens de regering zou de patiënt ook onder de nieuwe regeling te kennen kunnen geven dat hij bepaalde gegevens niet bekend wil hebben aan mede-behandelaars. Die gegevens mogen dan niet worden verstrekt. Een nadere regeling achtte zij niet zinvol.[18] In het midden is gebleven of het hier ging om een impliciete beperking van artikel 7:457 lid 2 BW of om toepassing van het algemene beginsel van redelijkheid en billijkheid of de zorg van een goed hulpverlener. Gelet op de uitkomst van de discussie in de Tweede Kamer houd ik het op het laatste. Dat neemt niet weg dat de vraag wie nu "rechtstreeks betrokken" zijn bij de uitvoering van een behandelingsovereenkomst, in de praktijk ruimte laat voor nadere invulling. De Registratiekamer heeft zich op het standpunt gesteld, dat

[17] Zie MvA TK (noot 13), blz. 39.
[18] Handelingen TK 1993-1994, blz. 4004.

in dit criterium ook een normatief element besloten ligt. In het kader daarvan overwoog zij het volgende:[19]

'Niet elke persoon of instantie die door de hulpverlener feitelijk bij de uitvoering van een behandelingsovereenkomst wordt betrokken kan als rechtstreeks betrokkene in de zin van de wet worden beschouwd. Het staat de hulpverlener niet vrij naar goeddunken derden bij de uitvoering van de behandelingsovereenkomst te betrekken, althans niet om gegevens over de patiënt aan hen te verstrekken. Bij de beoordeling van hetgeen hier toelaatbaar is, spelen verschillende factoren een rol, zoals de mate waarin inschakeling van de betreffende persoon of instelling binnen de kring van beroepsgenoten wordt aanvaard, de vraag of redelijke alternatieven voorhanden zijn, de zeggenschap van de arts over de werkzaamheden van de betrokkene (met name wanneer het niet-medici betreft) en de maatregelen die zijn getroffen ter bescherming van de persoonlijke levenssfeer van de patiënt. Ook de kenbaarheid voor de patiënt is van betekenis, terwijl voorts meeweegt of het belang van de patiënt erdoor wordt gediend. Indien inschakeling van de betreffende persoon of instantie buiten het verwachtingspatroon van de patiënt ligt of tegen diens belang indruist, ligt de veronderstelling van toestemming niet voor de hand.'

Door mede rekening te houden met de kenbaarheid, het belang en het verwachtingspatroon van de patiënt zijn elementen ingebouwd die een aanvaardbare uitkomst kunnen verzekeren. In het Advies medische zorgpas is overwogen dat de patiënt de mogelijkheid houdt bezwaar te maken tegen gegevensverstrekking.[20] De hiervoor genoemde criteria zijn sindsdien goed bruikbaar gebleken bij het beoordelen van nieuwe ontwikkelingen, met name op het terrein van de IT. Daarbij wordt ook rekening gehouden met de omvang van het verschijnsel.[21] Dit raakt de kenbaarheid en de beheersbaarheid van het gegevensverkeer.

Artikel 7:465 BW over de positie van minderjarigen derogeert onder meer op het punt van de leeftijdsgrenzen aan de overeenkomstige artikelen 11 lid 4 en 29 lid 5 WPR.

---

[19] Registratiekamer, De rekening van de arts, februari 1994, blz. 13. In dit rapport ging het om de rol van administratiekantoren, incassobureaus en factoringbedrijven in de financiële afwikkeling van de geneeskundige behandelingsovereenkomst.

[20] Registratiekamer, Advies medische zorgpas, oktober 1995, blz. 9

[21] Zie bijv: Registratiekamer, Medicatiebewaking door centrale patiëntenregistratie, oktober 1998, blz. 7

2.3 WGBO en WBP

In de toelichting op de WBP wordt op verschillende plaatsen duidelijk gemaakt dat de verhouding tussen WGBO en WBP niet anders zal zijn dan die tussen WGBO en WPR.[22] Dit is later nog eens uitdrukkelijk als volgt bevestigd:[23]

'Er wordt ten opzichte van de huidige situatie geen wijziging beoogd. De Wet bescherming persoonsgegevens enerzijds en een aantal gezondheidswetten – met name de WGBO – anderzijds vullen elkaar wederzijds aan. De WGBO bevat een aantal specifieke regels voor de bescherming van persoonsgegevens in het kader van de geneeskundige behandelingsovereenkomst en moet worden beschouwd als een sectorale precisering van de algemene normen van de Wbp. Waar de WGBO geen bijzondere regels geeft, is gewoon de Wbp van toepassing.'

Omdat de WBP uitwerking geeft aan dezelfde basisbeginselen als de WPR, is er ook overigens sprake van een grote mate van continuïteit. De verschillen hangen voor een deel samen met het feit dat de WBP en de EG-richtlijn een andere invalshoek kiezen.[24]

Zo zal de WBP van toepassing zijn op elke verwerking van persoonsgegevens die geautomatiseerd plaatsvindt of persoonsgegevens betreft die in een gestructureerd bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen.[25] Het begrip "verwerking" omvat het hele proces dat een gegeven kan doormaken vanaf het verzamelen tot het vernietigen. De nieuwe regeling bestrijkt dus een langer traject en volgt de verschillende stadia van het verwerkingsproces ook preciezer. Dit past bij de werkelijkheid van het IT-gebruik. Bij het beheer van een patiëntendossier zal dan ook sprake kunnen zijn van verschillende soorten van verwerkingen.

---

[22] TK 1997-1998, 25 892, nr. 3, blz. 12, 42 en 108.
[23] Zie MvA: TK 1998-1999, 25 892, nr. 6, blz. 9. Zie ook noot 12
[24] Zie ook: R.M.S. Doppegieter, De nieuwe privacywet, Medisch Contact 1998, blz. 1102-1104; T. Hooghiemstra, De WBP en de gezondheidszorg, NTMA, september 1998, blz. 22-25, en J.K.M. Gevers, Nieuwe privacywetgeving en de gezondheidszorg, Sociaal Recht 1999, blz. 64-70.
[25] Het begrip "bestand" komt overeen met het begrip "persoonsregistratie" in de WPR.

Het begrip "verantwoordelijke" komt in de plaats van het begrip "houder". Het gaat hierbij om degene die – al dan niet tezamen met anderen – het doel van en de middelen voor de verwerking vaststelt. In ziekenhuizen en andere grotere verbanden zal dus vaker sprake kunnen zijn van gedeelde verantwoordelijkheid, afhankelijk van de vraag wie "hulpverlener" is in de zin van de WGBO. Dit kan zich ook voordoen bij gegevensverkeer dat meer dan één instelling omvat.

Artikel 6 WBP geeft uitdrukking aan het grondbeginsel van de rechtmatigheid. Persoonsgegevens mogen volgens deze bepaling alleen in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Dit vormt tevens een schakelbepaling naar andere toepasselijke wetgeving, zoals de WGBO, en laat ruimte voor verdere rechtsontwikkeling afhankelijk van de omstandigheden die zich in de praktijk kunnen voordoen.

Artikel 7 WBP schrijft voor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. Dit vereist een nauwkeurige specificatie van die doeleinden voordat de gegevens worden verzameld. Op grond van artikel 8 WBP moet elke verwerking voorts ten minste kunnen steunen op één van de hier omschreven verwerkingsgronden. Bij een patiëntendossier zal het vaak gaan om een verwerking die noodzakelijk is voor de uitvoering van een behandelingsovereenkomst, of een verwerking met toestemming van de betrokkene of ter nakoming van een wettelijke verplichting waaraan de verantwoordelijke gebonden is (onderdelen a, b en c). Volgens artikel 9 WBP gelden daarnaast twee algemene beperkingen. Een verwerking mag niet onverenigbaar zijn met de doeleinden waarvoor de persoonsgegevens zijn verkregen. Zij moet ook achterwege blijven voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift aan de verwerking in de weg staat. Op grond van deze bepaling zal het beroepsgeheim of de zorg van een goed hulpverlener verdergaande consequenties kunnen hebben dan onder de WPR, en bijvoorbeeld ook in de weg kunnen staan aan de opslag van gegevens onder onveilige of onvoldoende geregelde omstandigheden.

Volgens artikel 10 WBP mogen persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor zij worden

verwerkt. Op grond van artikel 11 WBP moeten maatregelen worden getroffen om de kwaliteit van de gegevens te verzekeren en op grond van artikel 13 WBP tegen verlies van de gegevens of enige vorm van onrechtmatige verwerking.

De WBP stelt hogere eisen aan de transparantie van de verwerkingen. Indien persoonsgegevens bij de betrokkene worden verkregen, moet deze volgens artikel 33 WBP vooraf worden ingelicht over de identiteit van de verantwoordelijke en de doeleinden van de verwerking, tenzij hij daarvan al op de hoogte is. Als dat nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen, moet dan óók informatie worden verstrekt over andere onderwerpen. Indien persoonsgegevens op een andere wijze worden verkregen, moet dergelijke informatie op grond van artikel 34 WBP aan de betrokkene worden verstrekt uiterlijk bij de vastlegging. Niet-nakoming van deze verplichtingen leidt tot verkrijging in strijd met artikel 6 WBP.

Voor bepaalde categorieën van bijzondere gegevens gelden op grond van artikel 16 WBP nog nadere beperkingen. Volgens artikel 21 WBP mogen persoonsgegevens over iemands gezondheid echter onder meer worden verwerkt binnen de gezondheidszorg, voor zover dat met het oog op een goede behandeling van de betrokkene, dan wel voor het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is. Volgens artikel 23 WBP is een dergelijke verwerking ook mogelijk met uitdrukkelijke toestemming van de betrokkene.

De rest van de WBP – waaronder de bepalingen over gedragscodes, aanmelding, rechten van de betrokkene, toezicht en handhaving – laat ik buiten beschouwing. Voor de goede orde alleen nog iets over het overgangsrecht. Volgens artikel 79 WBP geldt voor verwerkingen die op het tijdstip van inwerkingtreding van de WBP al plaatsvonden, in principe een overgangsperiode van één jaar. Dat geldt ook voor de verwerking van gezondheidsgegevens. Alleen voor de aanpassing aan *nieuwe* beperkingen in de regeling voor bijzondere gegevens is drie jaar beschikbaar. Voor de gezondheidszorg zou het hier kunnen gaan om de nieuwe regeling voor genetische gegevens in artikel 21 lid 4 WBP en het vereiste van uitdrukkelijke toestemming voor zover een andere specifieke grondslag niet voorhanden blijkt.

2.4. Aandachtspunten

Het voorgaande zou op zichzelf als toetsingskader kunnen dienen voor een beschouwing over het gebruik van IT in de gezondheidszorg. Om de aandacht beter te kunnen richten heb ik er echter voor gekozen om vooral in te gaan op de volgende aspecten:

a. de verantwoordelijkheid: wie is waarvoor verantwoordelijk en hoe ver gaat de verantwoordelijkheid van de "hulpverlener"?
b. de zorg voor de inhoud: welke eisen stelt de zorg voor de inhoud van het "patiëntendossier"?
c. de zorg voor het gebruik: welke consequenties heeft het medisch beroepsgeheim?
d. de rechten van de betrokkene: hoe kunnen deze in de praktijk worden verzekerd?
e. de transparantie: welke bijzondere eisen moeten hieraan worden gesteld?

3. PRIVACY ENHANCING TECHNOLOGIES (PET)

De toepassing van IT binnen de gezondheidszorg is in dit preadvies niet alleen een voorwerp van aandacht bij een confrontatie met regels en beginselen van gezondheidsrechtelijke privacybescherming. Het is inmiddels gebleken dat de mogelijkheden en middelen van de IT ook een belangrijke rol kunnen spelen als het er om gaat de toepassing van die regels en beginselen in de praktijk zo goed mogelijk te verzekeren. Het beste resultaat wordt verkregen als de randvoorwaarden die in het vorige hoofdstuk zijn aangeduid en de inrichting van de verschillende systemen nauw op elkaar aansluiten. Daarvoor is het essentieel dat die randvoorwaarden in het vroegst mogelijke stadium worden doordacht op hun consequenties en dat deze vervolgens worden meegenomen in het ontwerp en de ontwikkeling van de systemen. De "zachte" normen van de privacybescherming kunnen op die manier worden omgezet in "harde" systeemspecificaties. De privacybescherming kan dan als het ware in de systemen worden "ingebouwd".

De eerste en meest belangrijke vraag in deze benadering is steeds of het wel echt noodzakelijk is om over persoonsgegevens te beschikken, en zo ja over welke persoonsgegevens voor welke doeleinden en voor welke gebruikers. Uit een studie die de Registratiekamer in 1995 samen met TNO-FEL en de Information and Privacy Commissioner in Ontario/Canada heeft uitgevoerd, is gebleken dat met reeds bestaande technische middelen informatiesystemen kunnen worden gebouwd die dezelfde functionaliteiten bezitten als conventionele systemen, maar geen of veel minder persoonsgegevens verwerken.[26] Het kernelement is hierbij het gebruik van een *identity protector* die het mogelijk maakt om binnen één systeem onderscheid te maken tussen domeinen waarin de betrokken persoon onder zijn ware identiteit bekend is en domeinen waarin hij alleen bekend is onder een pseudo-identiteit of zelfs geheel anoniem is. Afhankelijk van de positionering van de identity protector kan er voor worden gezorgd dat de ware identiteit van de betrokkene binnen het gehele systeem onbekend is of alleen voor een deel van de toepassingen of een deel van de gebruikers. Bij de nadere uitwerking hiervan spelen cryptografische technieken, digitale handtekeningen en

[26] Privacy-enhancing Technologies: The path to anonymity, Den Haag 1995, Achtergrondstudies en Verkenningen 5A en 5B, en Den Haag 1998 (herziene versie), Achtergrondstudies en Verkenningen 11.

trusted third parties (TTP) een belangrijke rol. In het gegevensverkeer langs de elektronische snelweg zijn dit echter bekende verschijnselen om de veiligheid en de betrouwbaarheid van verzonden boodschappen te verzekeren. Het gaat er dus meer om deze middelen ook in te zetten bij het verankeren van de privacybescherming in IT-systemen. In de zojuist bedoelde studie worden praktische voorbeelden genoemd van situaties waarin deze aanpak zou kunnen worden toegepast. In dat kader is ook aandacht besteed aan de gezondheidszorg. Aanvankelijk ging het daarbij om de toegang tot gegevens voor wetenschappelijk onderzoek. Inmiddels is echter al in de praktijk ervaring opgedaan met deze aanpak binnen ziekenhuizen in breder verband.[27]

Tegen de achtergrond van het voorgaande verdient het de aandacht dat artikel 13 WBP – in aansluiting op artikel 17 van de EG-richtlijn – zal verplichten tot het treffen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen enige vorm van onrechtmatige verwerking. Onder dit laatste valt zonder enige twijfel ook het verwerken van persoonsgegevens zonder dat is voldaan aan de materiële eisen voor de rechtmatigheid van die verwerking, zoals deze in het vorige hoofdstuk op hoofdlijnen zijn aangeduid. Het antwoord op de vraag welke maatregelen "passend" zijn, hangt volgens artikel 13 WBP enerzijds af van de stand van de techniek en de kosten van uitvoering en anderzijds van de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. Het ligt echter voor de hand aan te nemen dat de toepassing van PET in gevallen als bedoeld in dit preadvies, in de praktijk steeds vaker "passend" zal worden geacht. Het verdient dan ook aanbeveling die mogelijkheid in voorkomende gevallen in een zo vroeg mogelijk stadium onder ogen te zien.

---

[27] Idem, Appendix B: Provision of medical data. Zie voorts: G. van Blarkom, Guaranteeing requirements of data protection in a hospital information system with privacy-enhancing technology, British Journal of Healthcare Computing & Information Management, May 1998, blz. 30 e.v.

4. ELEKTRONISCH PATIENTENDOSSIER

4.1. Stand van zaken

Het enkele feit dat patiëntengegevens elektronisch worden vastgelegd en beheerd is al lang geen bijzonderheid meer. Zoals in paragraaf 1.2 naar voren kwam, werden de medische gegevens van hun patiënten al enkele jaren geleden door ruim 40 % van de huisartsen in de computer bijgehouden en werkte 25 % "papierloos". Sindsdien is het overgrote deel van de huisartsen omgeschakeld van de traditionele groene kaart naar de elektronische kaart.[28] De term "elektronisch patiëntendossier" heeft echter in de regel betrekking op iets anders. In de eerste plaats gaat het dan om een gestructureerde vorm van gegevensvastlegging volgens daartoe ontwikkelde normen en standaarden. Een gecodeerd EPD, waarin naast vrije tekst een beperkt aantal gegevens met behulp van standaardclassificaties wordt vastgelegd, lijkt hierbij voorshands het meest waarschijnlijk. In de tweede plaats gaat het om een stelsel van elektronische deeldossiers over één patiënt die door zorgverleners zo nodig op afstand kunnen worden geraadpleegd. Bij voorkeur is dan nog een combinatie mogelijk met kennissystemen die uitsluitsel geven over behandelmethoden. Een dergelijk stelsel zou betrekking moeten hebben op de gehele zorgketen en in theorie alle deeldossiers over één patiënt moeten omvatten. Alleen dan zouden immers zowel kwaliteit als doelmatigheid van zorg gewaarborgd zijn.[29]

Dergelijke visies zijn in de praktijk nog nergens gerealiseerd. In het kader van het programma Informatie- en Communicatietechnologie in de Zorgsector (ICZ) van ZorgOnderzoek Nederland (ZON) wordt wel gewerkt aan de ontwikkeling van bouwstenen die uiteindelijk moeten resulteren in een EPD als eerder bedoeld. Ook is sprake van lokale of regionale proefprojecten. In Zorg 2000, een voorbeeldproject in het kader van het Nationaal Actieprogramma elektronische snelwegen in de proefregio Delft, wordt gestreefd naar permanente voorzieningen op het gebied van elektronische communicatie gericht op het primaire

---

[28] J. van der Lei, Van huisartsendossier naar elektronisch patiëntendossier, NTMA, september 1998, blz. 14-17.

[29] Zie ook: P.E. Postmus, Het zorgketendossier, NTMA, september 1998, blz. 7- 9; A. Hasman e.a., Ontwikkeling van ziekenhuisdossier tot EPD, NTMA, september 1998, blz. 11-13.

proces. Een onderdeel van het project is gericht op de uitwisseling van medicatiegegevens om apothekers en artsen inzicht te bieden in een zo volledig mogelijk medicatiedossier van de patiënt.[30] De ontwikkeling van normen en standaarden wordt begeleid vanuit het Coördinatiepunt Standaardisatie Informatievoorziening Zorg (CSIZ). Daarnaast is er op het technische vlak nog zeer veel werk te verzetten. Steeds meer groeit dan ook het inzicht, dat er mogelijk nooit een alomvattend EPD komt. Veeleer zou gedacht moeten worden aan een verwijsindex die de weg wijst naar relevante deeldossiers. In elk geval lijkt een stap-voor-stap benadering aangewezen.[31]

4.2. Aandachtspunten

Tegen de achtergrond van het voorgaande rijst allereerst de vraag hoe het staat met de verantwoordelijkheid voor de aanleg en werking van elektronische patiëntendossiers. Het verdient daarbij aanbeveling om de analyse te beginnen bij bestaande situaties en van daaruit verder te gaan naar nieuwe en meer complexe verhoudingen in de toekomst. Zo ligt het voor de hand om een huisarts als hulpverlener in de zin van de WGBO ook integraal verantwoordelijk te houden voor de werking van zijn elektronisch patiëntendossier. In het geval van een groepspraktijk waar de hulpverleners regelmatig voor elkaar waarnemen zal onder de WPR in de regel sprake zijn van medehouderschap en onder de WBP van een gezamenlijke verantwoordelijkheid voor de verwerkingen in het kader van de gemeenschappelijke patiëntenadministratie. Indien er binnen de groepspraktijk sprake is van een vaste taakverdeling zou het hulpverlenerschap met die taakverdeling sporen. In zoverre zou er ook sprake kunnen zijn van een afzonderlijke verantwoordelijkheid voor bepaalde deelverwerkingen al naargelang de gegevens waarop deze betrekking hebben. In het geval van een ziekenhuis is dit onder de WPR meestal houder van de centrale patiëntenadministratie en zal dit onder de WBP ook wel de hoofdverantwoordelijkheid dragen voor de verwerkingen die in dat kader plaatsvinden. Dat neemt niet weg dat de hulpverleners die hun patiëntengegevens aan die centrale administratie

[30] Informatievoorziening in de zorg, TK 1997-1998, 25 669, nr. 2, blz. 5 e.v.
[31] J.H. van Bemmel in zijn bijdrage aan het Medidata Congres, Nationaal Aktieplan Informatisering Zorgsector, Den Haag, 25 november 1998.

toevertrouwen, ten minste voor een deel verantwoordelijk blijven voor wat er met die gegevens gebeurt.[32]

Bij de uitwisseling van patiëntengegevens tussen huisartsen onderling – hetzij rechtstreeks, hetzij via een daartoe aangelegd netwerk – blijft het houderschap over de afzonderlijke patiëntenadministraties onder de WPR onverlet. Dat geldt eveneens als huisartsen en specialisten onderling gegevens uitwisselen. Onder de WBP zullen zij dan ook elk voor zich verantwoordelijk blijven voor de verwerkingen die zij in het kader van de onderlinge communicatie laten plaatsvinden. Ik zie geen reden waarom een dergelijke afzonderlijke verantwoordelijkheid niet in gelijke mate richtinggevend zou kunnen zijn voor het transmurale gegevensverkeer in groter verband. De dienstverlenende bedrijven en instellingen die in dit kader in toenemende mate actief zijn, mogen dus wel een grote bedrijvigheid ontwikkelen met alle initiatieven van dien, zij zijn in principe slechts uitvoerders van de opdrachten die hun door de betrokken zorgverleners worden verleend en derhalve zowel onder de WPR als de WBP in de regel slechts bewerkers.[33]

Naarmate de schaal van het gegevensverkeer toeneemt, kunnen zich hierbij nog twee varianten gaan voordoen. In de eerste plaats lijkt het mogelijk dat zich bij een voortgaande integratie tussen zorgverlenende instellingen, een soortgelijke situatie gaat ontwikkelen als nu bestaat binnen één ziekenhuis: een gemeenschappelijke verantwoordelijkheid voor het geheel. Binnen dergelijke samenwerkingsverbanden zal dan vermoedelijk ook weer sprake zijn van gedeelde verantwoordelijkheid voor bepaalde verwerkingen binnen dat geheel, bijvoorbeeld voor die binnen één ziekenhuis, of daarbinnen weer bij de hulpverleners die van de gemeenschappelijke voorzieningen gebruik maken, voor zover het hun patiënten betreft. Hierbij tekent zich dus steeds meer het beeld af van een gestapelde of geschaalde verantwoordelijkheid, zoals zich bij gecompliceerde rechtsbetrekkingen vaker kan voordoen. Zo nodig zou de wetgever hierbij knopen moeten doorhakken en de rollen nader moeten verdelen. Voorlopig lijkt dat echter niet mogelijk en evenmin

[32] Zie TK 1997-1998, 25 892, nr. 3, blz. 58. De centrale aansprakelijkheid van het ziekenhuis ingevolge artikel 7:462 BW staat daar in principe geheel los van.

[33] In geval van dienstverlening die geen verwerking omvat, is onder WPR en WBP geen sprake van bewerkerschap.

zinvol, omdat de komende verhoudingen nog onvoldoende duidelijk zijn uitgekristalliseerd.

Daarnaast kan er behoefte gaan ontstaan aan hulpconstructies die het gegevensverkeer tussen de betrokken patientenadministraties mogelijk maken en op bepaalde punten ondersteunen. Zo is in diverse regio's al sprake van gemeenschappelijke basisregistraties waarin een beperkte set gegevens over patiënten in die regio wordt bijgehouden, al dan niet met de noodzakelijke verwijzingen naar eerdere behandelingen. Zeker indien dergelijke verwijzingen zijn opgenomen, is het gewenst dat de verantwoordelijkheid hiervoor – direct of indirect – blijft berusten bij de deelnemende instellingen. Als het beheer over zulke voorzieningen is verzelfstandigd, behoeft de zeggenschap van de deelnemers dan ook extra aandacht. In de praktijk zal dit minst genomen moeten leiden tot duidelijke contractuele afspraken, omdat de deelnemende instellingen anders hun eigen verantwoordelijkheid niet meer kunnen waarmaken. Bij de in paragraaf 4.1 bedoelde verwijsindex zou ik in principe in dezelfde richting willen denken.

Zoals in hoofdstuk 2 tot uitdrukking kwam, is een verantwoordelijke ook belast met de zorg over de kwaliteit van de verwerkte gegevens en de beveiliging daarvan, althans in die zin dat de nodige maatregelen moeten zijn getroffen om beide te verzekeren. Uit hoofde van de WGBO blijft een hulpverlener verantwoordelijk voor het bijhouden van het medisch dossier. Een hulpverlener die de directe zorg voor het medisch dossier uit handen geeft, zal zich dus moeten vergewissen van de maatregelen die zijn getroffen om de kwaliteit en de veiligheid van de opgenomen patiëntengegevens te verzekeren. Ook de algemene zorg van een goed hulpverlener vergt dit. Om soortgelijke redenen zal een hulpverlener niet kunnen instemmen met de opslag en verwerking van patiëntengegevens onder omstandigheden waarbij de kwaliteit en de veiligheid van deze gegevens onvoldoende is verzekerd. Hiervoor zullen dus afdoende procedures moeten zijn vastgesteld.

Met betrekking tot de toegang tot de gegevens in een elektronisch patiëntendossier kan in principe hetzelfde worden gesteld. Hierbij doet zich echter nog de bijzondere vraag voor naar de reikwijdte van het medisch beroepsgeheim. Het antwoord op die vraag is in meer dan één opzicht van belang. In de eerste plaats moet vaststaan dat de gegevens die een hulpverlener zijn toevertrouwd, mogen worden opgeslagen in

een omgeving waarin derden tot die gegevens toegang zouden kunnen krijgen. In de tweede plaats moet per geval vaststaan dat de betrokken derde bevoegd is tot een dergelijke toegang. Hierbij gaat het telkens om de kwestie of de beheerder van het dossier en degenen die toegang zouden willen hebben, "rechtstreeks betrokken" zijn bij de uitvoering van de behandelingsovereenkomst in het kader waarvan die gegevens zijn verkregen, dan wel of de betrokken patiënt – hetzij stilzwijgend, hetzij uitdrukkelijk – toestemming heeft gegeven voor de bedoelde werkwijze.

Ik meen dat deze kwestie genuanceerd moet worden benaderd. Van de beheerder van het patiëntendossier zal op basis van de in paragraaf 2.2 bedoelde criteria in de regel de "rechtstreekse betrokkenheid" kunnen worden aangenomen, indien sprake is van een veilige en betrouwbare omgeving waarop vanuit de "behandelsector" voldoende invloed kan worden uitgeoefend.[34] Dit vormt een reden te meer om het beheer van elektronische patiëntendossiers zoveel mogelijk binnen de betrokken instellingen te organiseren. Bij de toegang door derden moet van geval tot geval worden getoetst of van rechtstreekse betrokkenheid sprake is. Is deze aanwezig, dan mag de betrokken derde toegang hebben tot alle gegevens die voor zijn werkzaamheden in dat kader noodzakelijk zijn. In alle andere gevallen is – uitzonderlijke situaties zoals wettelijke plichten of noodtoestand daargelaten – de toestemming van de patiënt nodig. Met stilzwijgende toestemming kan dan worden volstaan, als de toegang noodzakelijk is voor een andere behandeling, de betrokken patiënt daarvan op de hoogte is en hij de draagwijdte van een en ander kan overzien. In andere gevallen zullen aan de toestemming zwaardere eisen moeten worden gesteld. Op grond van artikel 23 WBP zou een uitdrukkelijke toestemming nodig kunnen zijn, indien de toegang tot het dossier niet met het oog op de behandeling van de betrokkene of voor het beheer van de desbetreffende instelling of beroepspraktijk noodzakelijk is. Dit laat de toegang in transmurale situaties open, mits deze voor behandelingsdoeleinden noodzakelijk is. Aan de organisatie van de toetsing zullen in de praktijk dus hoge eisen moeten worden gesteld.[35]

---

[34] Zie ook: Registratiekamer, De rekening van de arts, februari 1994, blz. 15, over de verzorging van medische facturen binnen een ziekenhuis.

[35] In geval van spoed kan de toetsing desgewenst ook achteraf plaatsvinden.

In het geval van een beperkte registratie met medicatiegegevens voor artsen en apothekers heeft de Registratiekamer in 1998 "rechtstreekse betrokkenheid" aangenomen. Daaraan zijn echter strikte voorwaarden verbonden.[36] Zo is het oordeel beperkt tot een samenwerking tussen huisartsen en apothers op beperkte schaal, in de directe omgeving van de patiënt en voor deze kenbaar. Ook worden hoge eisen gesteld aan de beveiliging. Zo is de toegang tot de registratie voorbehouden aan de betrokken beroepsbeoefenaars, waarvan de bevoegdheidsprofielen persoonlijk zijn toegekend voor een van tevoren vastgestelde periode. Voor een verificatie van de bevoegdheidsprofielen is het noodzakelijk dat de handelingen van de gebruikers worden vastgelegd. Ook dienen de gegevens in versleutelde vorm te worden verzonden.

De rechten van de patiënt op kennisneming, verbetering, vernietiging, verzet enz. ingevolge WGBO en WBP vergen niet alleen dat voor de uitoefening daarvan procedures zijn vastgesteld die duidelijk bepalen wie waarover beslist, maar ook dat die beslissingen zonder problemen in de praktijk kunnen worden uitgevoerd. Bij de aanleg en het beheer van elektronische patiëntendossiers zal derhalve ook hieraan tijdig aandacht moeten worden besteed.

Transparantie rond de werking van elektronische patiëntendossiers is tenslotte op alle voorgaande punten van belang. Niet alleen bepaalt dit mede de rechtmatigheid van de beoogde verwerkingen tegenover de patiënten, maar zonder voldoende duidelijkheid over de verdeling van verantwoordelijkheden rond de werking van elektronische dossiers, de zorg voor de inhoud en het gebruik van de opgenomen gegevens, en de wijze waarop de betrokkenen hun rechten kunnen uitoefenen is een aanvaardbare werking van elektronische patiëntendossiers eenvoudig niet mogelijk.

4.3. Vooruitzichten

De visie dat elektronische patiëntendossiers om verschillende redenen gewenst zijn, wordt door het voorgaande zeker niet weersproken. Wel kan de opvatting dat een stap-voor-stap benadering is aangewezen, op grond daarvan alleen maar worden onderschreven. Op alle belangrijke

[36] Registratiekamer, Medicatiebewaking door centrale patiëntenregistratie, oktober 1998, blz. 7 en 14.

onderdelen doen zich immers nog complexe vragen voor die in ernst toenemen naarmate het onderwerp meer in de sfeer van grootschalige voorzieningen wordt getrokken. Dat betekent dat aan de ene kant moet worden verder gewerkt aan concrete proefprojecten en dat tegelijk en in samenhang daarmee moet worden gezorgd voor meer duidelijkheid over de in acht te nemen randvoorwaarden. De verscheidenheid die op die manier in de praktijk tot ontwikkeling komt, heeft als voordeel dat de kans op meer inzicht in de beste oplossingen toeneemt.

5. CHIPKAARTEN

5.1. Stand van zaken

Een chipkaart is een plastic kaart ter grootte van een creditcard waarin een chip is aangebracht met bijzondere eigenschappen. Gaat het om een eenvoudige geheugenchip, dan zijn de capaciteiten van de kaart nog bescheiden. Gaat het echter om een microchip, dan heeft deze de eigenschappen van een kleine microcomputer die gegevens kan lezen bewerken, opslaan en verstrekken, maar desgewenst ook gevoelige gegevens kan afschermen en zo nodig meerdere toepassingen los van elkaar kan ondersteunen. De in- en uitvoer van gegevens kan verlopen via elektrisch geleidende contacten op de kaart wanneer deze in een kaartleesapparaat wordt gestoken, of contactloos waarbij de gegevens radiografisch kunnen worden verzonden of ontvangen. Dergelijke intelligente chipkaarten of "smartcards" kunnen gebruikt worden voor meerdere doeleinden, zoals beveiliging, gegevensopslag, identificatie en elektronische beurs.

In eerste instantie werd de aantrekkelijkheid van de chipkaart voor de gezondheidszorg vooral gezien in de mogelijkheid om de patiënt de beschikking te geven over een eigen medisch zakdossier. In het advies van de Registratiekamer over het medische zorgpas werd deze optie van kritische kanttekeningen voorzien.[37] Sindsdien zijn de opvattingen steeds meer in de richting gegaan, dat een chipkaart vooral nuttig zou zijn als sleutel die toegang kan bieden tot een elektronisch dossier. De mogelijkheid tot gegevensopslag komt momenteel vooral aan de orde in het ZorgPas-project van de gezamenlijke zorgverzekeraars, dat zich in de eerste fase alleen richt op administratieve functies, zoals controle op verzekeringsgerechtigdheid en vereenvoudiging van de financiële afwikkeling. Ook zijn er enkele chipkaartprojecten van afzonderlijke zorgverzekeraars. Het meest verstrekkende project op dit gebied is de Zorgpas voor Parkinsonpatiënten van Zorg en Zekerheid, waaraan 400 patiënten bij wijze van experiment zullen deelnemen. Op deze pas zal de medicatiegeschiedenis worden bijgehouden. De legitimatie zal hier langs biometrische weg plaatsvinden met de afdruk van een vinger of handpalm. Dit moet gaan leiden tot een betere communicatie tussen medisch specialisten, apothekers en zorgverzekeraar. Over de verdere

[37] Registratiekamer, Advies medische zorgpas, oktober 1995, blz. 12 e.v.

toekomst van de chipkaart in de gezondheidszorg zijn de opvattingen nog verdeeld. Met name blijft de vraag omstreden in hoeverre ook medische gegevens op de kaart dienen te worden aangebracht, anders dan een beperkte set SOS-gegevens of bepaalde gegevens voor een specifieke doelgroep. Daarbij gaat de discussie over het opnemen van medicatiegegevens of de hoofdlijn van de patiëntengeschiedenis. Ook is nog sprake van indexfuncties die verwijzen naar hulpverleners of plaatsen waar informatie over de patiënt ligt opgeslagen. De gedachte van een medisch dossier op een chipkaart wordt inmiddels algemeen afgewezen.[38]

5.2. Aandachtspunten

Ook hier rijst allereerst de vraag naar de verantwoordelijkheid voor de verwerking van persoonsgegevens op een chipkaart. Anders dan in het geval van het elektronisch patiëntendossier ligt een vergelijking met al bestaande situaties niet aanstonds voor de hand. Chipkaarten ontlenen hun belang immers vooral aan het feit dat zij in samenhang met andere vormen van gegevensverwerking aan een grotere flexibiliteit van het gegevensverkeer kunnen bijdragen. Dat betekent dat zij in het licht van dat bredere gegevensverkeer moeten worden bezien en dat een aparte beschouwing van één chipkaart niet zinvol is. De vraag of er in dat geval al dan niet sprake is van een of meer persoonsregistraties kan in het midden blijven, omdat de functie van een chipkaart met zich meebrengt dat deze in elk geval onderdeel vormt van een proces van gegevensverwerking. De verantwoordelijkheid daarvoor ligt dan ook primair bij degene die voor de desbetreffende toepassing op de kaart verantwoordelijk is.[39] Als het daarbij geheel of in hoofdzaak gaat om een administratieve toepassing ten dienste van de zorgverzekering, ligt de verantwoordelijkheid voor de desbetreffende verwerkingen bij de zorgverzekeraar. Dat neemt niet weg dat daarnaast sprake kan zijn van verantwoordelijkheid voor deelverwerkingen bij anderen, zoals de zorgverleners die bij de afwikkeling van de administratieve processen zijn betrokken. Het gebruik van een chipkaart kan bij deze instanties

[38] A. ter Linden, Een chipcard voor de patiënt? Een beleidsonderzoek naar functies en aspecten van de chipcard in de gezondheidszorg, EUR Rotterdam, september 1998.

[39] Zie: H.J.M. Gardeniers, Chipcards en Privacy, Regels voor een nieuw kaartspel, Achtergrondstudies en Verkenningen 6, Den Haag 1995.

leiden tot verkrijging of verstrekking van bepaalde gegevens over hun patiënten. Met name in het laatste geval zal de verantwoordelijkheid van de hulpverlener voor de nakoming van zijn verplichtingen in het kader van de WGBO mede in het geding kunnen komen. Dit zal des te meer het geval zijn naarmate ook medische gegevens op de chipkaart terecht komen of het gebruik van de kaart een onderdeel gaat vormen van het zorgproces.

De zorg voor de kwaliteit en de beveiliging van de persoonsgegevens op de chipkaart sluit in principe aan bij de zojuist bedoelde verdeling van de verantwoordelijkheid. Bijzondere aandacht verdient hierbij het aandeel van de zorgverlener. Naarmate de chipkaart immers van meer gevoelige gegevens wordt voorzien, zal de zorg van de hulpverlener voor de kwaliteit en de veiligheid van die gegevens toenemen. Daarbij komt dat ook de doorwerking van het medisch beroepsgeheim zich zal laten voelen. Voor zover de gegevensverwerking door de zorgverlener niet een rechtstreeks uitvloeisel is van de financiële afwikkeling van de behandelovereenkomst, zal voor de vastlegging van gegevens op de chipkaart de uitdrukkelijke toestemming van de patiënt nodig zijn. Dat neemt niet weg dat het in strijd zou zijn met de algemene zorg van een goed hulpverlener om een patiënt in een positie te brengen, waarin deze in het bezit komt van een grote hoeveelheid gevoelige gegevens waartoe anderen gemakkelijk toegang zouden kunnen krijgen. Dit was voor de Registratiekamer een belangrijke reden om de gedachte van een medisch zakdossier af te wijzen. Een andere reden was dat in een dergelijke situatie ook de zorg voor de kwaliteit van de gegevens op de kaart in onvoldoende mate kon worden verzekerd. Een en ander kan opnieuw aan de orde komen, indien medische gegevens op grotere schaal dan thans voorzien, op chipkaarten zouden worden opgenomen. Ook de volgende fasen van het ZorgPas-project verdient in dit kader de aandacht. Dit niet alleen met betrekking tot de mogelijke opslag van medische gegevens, maar vanwege de noodzaak de verschillende functies op de kaart zo duidelijk mogelijk van elkaar te scheiden. Ook een mogelijke indexfunctie van de kaart is in dit verband niet zonder problemen. De verwijzing naar hulpverleners of plaatsen waar nadere informatie over de patiënt is te verkrijgen, kan in bepaalde gevallen immers gevoelige medische informatie over hem onthullen.

Met betrekking tot de rechten van de betrokkene en de transparantie doet zich bij chipkaarten tenslotte de moeilijkheid voor dat – zonder

gerichte aandacht hiervoor – beide in de praktijk gemakkelijk in het gedrang kunnen komen. De vluchtigheid die het gegevensverkeer met behulp van chipkaarten nu eenmaal heeft, leidt ertoe dat de voordelen én de nadelen van chipkaartgebruik in de gezondheidszorg hier zonder uitdrukkelijke maatregelen op dit punt zeer dicht bij elkaar komen te liggen.

5.3. Vooruitzichten

Anders dan met betrekking tot het elektronisch patiëntendossier, lijkt de grootschalige invoering van chipkaarten in de gezondheidszorg min of meer voor de deur te staan. Voorshands gaat het daarbij slechts om administratieve toepassingen die het werkproces van zorgverzekeraars én zorgverleners kunnen verlichten. In het verlengde daarvan tekenen zich echter problemen af die de rechtspositie van patienten wezenlijk kunnen beïnvloeden. Het blijft dan ook zaak om de ontwikkelingen op dit gebied nauwlettend in het oog te houden.

6. IDENTIFICATIE VAN PATIENTEN

Zowel in de discussie over het elektronisch patiëntendossier als in die over het gebruik van de chipkaart in de gezondheidszorg duikt steeds vaker de behoefte op aan een unieke patiëntenidentificatie. Het belang daarvan laat zich moeilijk ontkennen. In het eerste geval is het immers van het grootste belang dat de gegevens over één patiënt met elkaar in verband kunnen worden gebracht en daarbij geen verwarring optreedt met de gegevens van een ander. In het tweede geval is de behoefte aan een unieke identificatie minder klemmend. Toch zou de doelmatigheid van administratieve processen in de zorg gediend zijn met een middel om de identiteit van patiënten vast te stellen en in het verkeer tussen zorgverlener en zorgverzekeraar tot uitdrukking te brengen. Dat neemt niet weg dat in beide samenhangen ook enige relativering past. Zolang het elektronische gegevensverkeer in de zorg nog vooral een lokale of hooguit regionale aangelegenheid is, behoeft aan het ontbreken van één landelijke oplossing wellicht wat minder zwaar te worden getild. Daarnaast valt niet in te zien waarom zowel voor de inhoudelijke zorg als voor de administratieve afwikkeling daarvan één en dezelfde wijze van identificatie noodzakelijk zou zijn. Uit beveiligingsoogpunt zou in tegendeel een uitdrukkelijk onderscheid tussen de inhoudelijke zorg en de administratieve afwikkeling daarvan aantrekkelijk kunnen zijn.

Bij de aanpak van het geschetste probleem tekenen zich verschillende richtingen af. De eerste gaat uit van een uniform persoonsnummer. Nu de ziekenfondsen hiertoe gebruik mogen maken van het sofi-nummer en dit nummer voor de uitvoering van de AWBZ ook in gebruik is bij de overige zorgverzekeraars, ligt de gedachte aan verdere uitbreiding van de werkingssfeer van het sofi-nummer voor de hand. Daar staat tegenover dat met betrekking tot het gebruik van dit nummer buiten de directe sfeer van sociale verzekeringen en belastingen een restrictief beleid wordt gevoerd en een dringende noodzaak om het verkeer van gegevens tussen zorgverleners en zorgverzekeraars op deze wijze te faciliteren niet aanwezig lijkt. Zou die stap na zorgvuldige afweging toch worden genomen, dan ligt een verdere uitbreiding tot de sfeer van de zorg niet voor de hand. Veeleer zou gedacht moeten worden aan de ontwikkeling van een sectorspecifieke identificatiemethodiek voor de zorg. In elk geval zou daarvan niet zonder grondig onderzoek naar de haalbaarheid van een dergelijke methodiek kunnen worden afgezien. Zoals in paragraaf 1.2 bleek, kwam ook de RVZ in haar advies over

IT in de zorg tot de conclusie dat gebruik van het sofi-nummer geen aanbeveling verdiende.

Een geheel andere oplossing is het gebruik van biometrie. In paragraaf 5.1 kwam deze al even aan de orde bij het chipkaartproject van Zorg en Zekerheid voor Parkinsonpatiënten. Een grootschalig gebruik van deze methode lijkt voorshands niet erg aannemelijk. Voor specifieke toepassingen en bijzondere belangen behoeft zij echter niet te worden uitgesloten. De mogelijkheden voor biometrische identificatie en de consequenties daarvan uit een oogpunt van privacybescherming zijn op dit moment in onderzoek bij de Registratiekamer. Daarbij wordt mede aandacht besteed aan verschillende methoden van opslag en het gebruik van *privacy enhancing technologies* om de nadelen van deze identificatiemethode te ondervangen.

Als voorlopige oplossing kan ook worden gedacht aan de indexfunctie van chipkaarten. Als het gebruik daarvan beperkt blijft tot uitwendige feiten omtrent de wijze van registratie bij zorgverleners, behoeft deze oplossing niet op al te grote bezwaren te stuiten. Het voordeel daarvan is bovendien dat zij eventuele verscheidenheid van registratie binnen één regio evenals interregionale mobiliteit van patienten zou kunnen compenseren.

7. INFORMATIEBEHOEFTE BUITEN DE ZORG

7.1. Zorgverzekeraars

Omdat de financiële afwikkeling van de verleende zorg nu eenmaal onderdeel vormt van de uitvoering van de behandelingsovereenkomst, kan ook de verstrekking van declaratiegegevens aan verzekeraars in principe gerekend worden tot het gegevensverkeer dat noodzakelijk is voor die afwikkeling. Daarbij is het wel van belang ervoor te zorgen dat niet meer gegevens worden verstrekt dan voor die afwikkeling noodzakelijk is. De Registratiekamer heeft in 1993 bezwaar gemaakt tegen de verstrekking van de ontslagdiagnose-code, waarover tussen de partijen in de zorg uitdrukkelijke afspraken waren gemaakt.[40] Nu het hierbij niet ging om de financiële afwikkeling van verleende zorg, maar om controle door verzekeraars op de doelmatigheid van de zorg waarvoor een toereikende wettelijke basis ontbrak, moest de gemaakte afspraak wijken voor het medisch beroepsgeheim. Van een wettelijke regeling is het sindsdien niet gekomen.

Het voorgaande neemt niet weg dat zorgverzekeraars in de praktijk, ook binnen de aldus gestelde grenzen, de beschikking krijgen over een aanzienlijke hoeveelheid gevoelige gegevens. Indien de verzekeraar vooraf betrokken is bij beslissingen over het verlenen van zorg, kan deze informatie nog uitvoeriger zijn. Volgens artikel 21 WBP mogen verzekeraars niet meer gegevens over iemands gezondheid verwerken dan noodzakelijk is voor de uitvoering van de verzekeringsovereenkomst. De waarborgen die op dit terrein gelden zijn nader uitgewerkt in de Gedragscode verwerking persoonsgegevens verzekeringsbedrijf, die door de Registratiekamer in 1998 is goedgekeurd.[41] In overleg met Zorgverzekeraars Nederland wordt momenteel gewerkt aan een annex bij deze gedragcode die in het bijzonder betrekking zal hebben op de verwerking van declaratiegegevens en het verdere gebruik dat daarvan mag worden gemaakt.

---

[40] Registratiekamer, De verstrekking van de ontslagdiagnose-code, augustus 1993.

[41] Zie Stcrt. 1998, nr. 44

7.2. Wetenschap en statistiek

Op grond van artikel 7:458 BW zijn voor wetenschappelijk onderzoek en statistiek op het gebied van de gezondheidszorg uitzonderingen in het leven geroepen op de geheimhoudingsplicht die hulpverleners op grond van van 7:457 BW in acht moeten nemen. Deze regeling is op onderdelen uitgewerkt in de Gedragscode Gezondheidsonderzoek, die door de Registratiekamer in 1995 is goedgekeurd.[42] Uitgangspunt van deze code is dat onderzoek op dit gebied zoveel mogelijk dient te geschieden met behulp van anonieme of gecodeerde gegevens en pas in laatste instantie met identificerende gegevens. Voor elk van deze drie categorieën zijn in de code toepasselijke waarborgen vastgelegd, die moeten verzekeren dat de betreffende gegevens slechts voor de beoogde doeleinden worden gebruikt. Het gebruik van elektronische patiëntendossiers met gestructureerde en gestandaardiseerde inhoud leidt in beginsel tot het beschikbaar komen van meer en beter toegankelijke informatie voor onderzoek en statistiek. Omdat de eerder bedoelde waarborgen daarbij onverminderd van kracht blijven, heeft dit geen ongewenste gevolgen.

7.3. Beleidsontwikkeling

Voor de ontwikkeling van overheidsbeleid bestaat in principe geen behoefte aan gegevens over individuele patiënten. Waar mogelijk zal voor dit doel gebruik kunnen worden gemaakt van de faciliteiten die artikel 7:458 BW voor onderzoek en statistiek op het gebied van de gezondheidszorg biedt. De toepassing van IT aan de basis van de zorg biedt ook nieuwe kansen aan de informatievoorziening ten behoeve van de beleidsontwikkeling bij de overheid. Zoals in paragraaf 1.2 al tot uitdrukking kwam, dient hier zoveel mogelijk met geaggregeerde informatie te worden volstaan.

7.4. Toenemende ambities

Door het introduceren van marktwerking in de sociale zekerheid en de zorg worden de bestaande regels over een zorgvuldige en behoorlijke omgang met persoonsgegevens op de proef gesteld. Dit zal te meer het geval zijn, indien zorgverzekeraars de mogelijkheid wordt geboden

[42] Zie Stcrt. 1995, nr. 140.

om zorginstellingen te gaan beheren, zoals in het regeerakkoord voor het zittende kabinet is vastgelegd.

In een recente studie naar managed care heeft de Registratiekamer de grenzen op dit gebied verkend. In deze studie wordt geconcludeerd dat managed care en privacy elkaar niet behoeven te bijten als gebruik wordt gemaakt van niet-identificerende gegevens of de uitkomsten van wetenschappelijk onderzoek of statistiek. Daarbuiten is echter sprake van buitengewoon strikte grenzen, waarop het gegevensverkeer in het kader van managed care niet zelden zal kunnen afstuiten.[43]

[43] T.F.M. Hooghiemstra, Privacy & managed care, Achtergrondstudies en Verkenningen 12, Den Haag 1998.

8. SLOTBESCHOUWING

Zoals uit het voorgaande blijkt, zijn bij de toepassing van IT in de gezondheidszorg uiteenlopende waarden en belangen in het geding. In het beleid dat de overheid op dit terrein volgt, staat een verbetering van de kwaliteit en de doelmatigheid van de zorg in een veranderende omgeving voorop. In deze veranderende omgeving en de spanning die in de praktijk tussen de twee hoofddoelstellingen kan bestaan, ligt het gevaar besloten dat het noodzakelijke evenwicht tussen de betrokken waarden en belangen verloren gaat.

De overheid bevindt zich op dit terrein in een lastig parket. Naast het behoud van een precair evenwicht tussen uiteenlopende waarden en belangen, staat zij immers voor de opgave een ambitieuze visie stap voor stap te realiseren vanuit een taakopvatting die tegelijk blijk geeft van terughoudendheid en inzicht in beperkte mogelijkheden. De keuze om in dit spanningsveld de nadruk te leggen op een combinatie van stimulering en randvoorwaardelijke sturing via privacywetgeving en standaardisatie is begrijpelijk. Een hernieuwde overweging van deze beleidsmix zou niet tot wezenlijke veranderingen behoeven te leiden.

Hoewel het toenemend gebruik van IT binnen de gezondheidszorg er toe zou kunnen leiden dat de uitgangspunten van het gezondheidsrecht ten aanzien van de betekenis van het medisch beroepsgeheim en de zorg van een goed hulpverlener in het gedrang komen, biedt de inhoud van de bestaande en komende privacywetgeving op belangrijke punten tegenwicht. Een stelselmatige toepassing daarvan in combinatie met de inzet van privacy-vriendelijke IT zal voorshands kunnen bijdragen aan het noodzakelijke evenwicht.