

Privacy en Toegankelijkheid
in
Gemeenschappelijk te gebruiken Elektronische Patiënten Dossiers



Afstudeerscriptie van:

Ludwig Oberendorff
Koningstraat 40
2316 CG Leiden
071-5217003
oberend@dds.nl
<http://huizen.dds.nl/~oberend>

Leiden, 19 december 1999

THE ELECTRONICAL MEDICAL RECORD HAS BEEN PURSUED AS AN IDEAL BY
SO MANY, FOR SO LONG, THAT SOME SUGGEST THAT IT HAS BECOME THE
HOLY GRAIL OF MEDICAL INFORMATICS

S. Kay & I.N. Purves 1996

Voorwoord

Eerder tijdens mijn studie aan de Universiteit Leiden verrichtte ik, met subsidie uit het Transparant Stimuleringsprogramma van het Ministerie van VWS, onderzoek naar de juridische privacy aspecten van Elektronische Patiëntendossiers in de Geestelijke Gezondheidszorg. Daaropvolgend werd ik om advies gevraagd bij het ontwikkelen van functionele autorisaties in een commercieel ontwikkeld Elektronisch Patiëntendossier (EPD) en bij het opstellen van een privacyreglement voor een EPD van een aantal fuserende psychiatrische instellingen. Daarnaast heb ik in de praktijk enige ervaring in de somatische gezondheidszorg opgedaan als administratief medewerker van het nachthoofd in een algemeen ziekenhuis. De bij voorgaande bezigheden opgedane kennis en ervaringen zijn de basis voor deze scriptie.

Privacybedreigingen door EPD's zijn in ruime mate gesignaleerd. Het heeft mij altijd bevreemd dat dat nauwelijks geleid heeft tot concrete beschermings-voorstellen. Vooral op het gebied van toegangscontrole heerst opvallende stilte. Terwijl de beperking van toegankelijkheid van persoonsgegevens nu juist de kern vormt van informationele privacybescherming. Die stilte is funest want de bouw en het gebruik van (semi)EPD's gaat al jaren onverkort voort.

Leiden, december 1999

Ludwig Oberendorff

Inhoudsopgave

1.	Inleiding	1
1.1	Opzet van deze scriptie	2
2.	Context	4
2.1	GEPD's zijn de toekomst	4
2.2	Kanttekeningen	5
2.3	Doel dossier	6
2.4	Papieren traject	7
2.5	Bepaalde toegankelijkheid conventioneel dossier	8
2.6	GEPD toegankelijker	9
2.7	Samenvatting	10
3.	Wet- en regelgeving	11
3.1	Overzicht	11
3.2	Geschiedenis	11
3.3	WPR	12
3.4	WBP	13
3.5	WGBO	14
3.6	BOPZ	14
3.7	Kwaliteitswet zorginstellingen en BIG	15
3.8	Medisch Beroepsgeheim	15
3.9	Toespitsing	16
3.10	Overzicht en toelichting specifieke bepalingen	18
3.11	Samenloop	29
3.12	Samenvatting	29
4.	Context revisited	
4.1	Veronderstelde toestemming en poortwachtersfunctie	30
4.2	Aanvaarde balans	31
4.3	Ogenschijnlijke ruimte	31
4.4	Gebruik gegevens in nieuwe behandeling	32
4.5	Samenvatting	33
5.	Functionaliteits eisen	34
5.1	Eisen met betrekking tot toegankelijkheid	34
5.2	Haalbaarheid en automatiseerbaarheid	36
5.3	Samenvatting	36
6.	Mogelijkheden	37
6.1	Toegangscontrole	37
6.2	Nadelen van geautomatiseerde toegangscontrole	40
6.3	Opslag van informatie	41
6.4	Labellen	43
6.5	PET	44
6.6	Samenvatting	45

7.	Architectuur	46
7.1	Centrale GEPD variant	46
7.2	Decentrale GEPD variant	47
7.3	Centraal of decentraal, voor en nadelen	47
7.4	Samenvatting	50
8.	Conclusie	51
	Literatuur	54
	Afkortingen	60
	Bijlage	62

1. Inleiding

Binnen de gezondheidszorg is kwaliteit van zorg de laatste jaren een van de hoofdpunten in de beleidsontwikkeling. Onderdeel van dit kwaliteitsbeleid is het verbeteren van de informatiestromen. Zowel van beleidsinformatie binnen de organisatie ter sturing van de zorgprocessen door het management, als van zorginhoudelijke informatie omtrent patiënten. Onderdeel van de informatie die over een patiënt wordt vastgelegd zijn medische gegevens. Deze worden opgenomen in het medisch dossier, ook wel Patiënten Dossier (PD).

Tegelijkertijd hebben op ICT gebied stormachtige ontwikkelingen plaatsgevonden. Diverse zorginstellingen zijn, ondersteund door het ministerie van VWS en overkoepelende organisaties, gaan werken aan projecten waarin informatietechnologie en het medisch dossier worden gecombineerd: het Elektronische Patiënten Dossier (EPD). Technisch is het zeer wel mogelijk dat dat dossier wordt geïntegreerd in een systeem dat niet alleen gebruikt wordt voor zorginhoudelijke informatie uitwisseling, maar dat ook het logistieke en administratieve proces ondersteunt. Een systeem dat naast medische informatie uitwisseling bijvoorbeeld ook gebruikt wordt voor kwaliteitsbewaking, statistiek, beheersing van patiëntenstromen, analyse van het zorgproces, opnamebeleid enzovoorts. Zo'n systeem zou een aanzienlijke bijdrage kunnen leveren aan efficiëntie- en effectiviteitsverbetering en daarmee aan kostenbesparing. Deze mogelijkheid van kostenbesparing is tevens een drijfveer voor vergaande samenwerking tussen zorginstellingen onderling.

Daarnaast wordt het zorgproces steeds meer opgevat als een keten. Samenwerking vindt plaats tussen instellingen van eenzelfde soort (bijvoorbeeld ziekenhuizen onderling) maar vooral tussen verschillende aanbieders in de zorgketen (huisarts-ziekenhuis). Juist dan bestaat de behoefte om informatie te delen, ook medische informatie over patiënten. Een aantal projecten gaat dan ook een stap verder. Hierbij wordt een dossier aangelegd dat niet alleen binnen een instelling geraadpleegd kan worden, maar ook over instellingsmuren heen: het Gemeenschappelijk te gebruiken Elektronisch Patiënten Dossier (GEPD)¹. Met behulp van die systemen denken samenwerkende instellingen een samenhangend pakket van zorg te kunnen bieden. Een kwalitatief beter en meer op maat gesneden zorgaanbod waarbij de bestaande organisatiescheidingen van ondergeschikt belang zijn. De traditionele scheiding tussen intramuraal, extramuraal en de tussenvariant semi-muraal wordt steeds minder relevant: er is een proces van transmuralisering gaande. De continuïteit van zorg vraagt dan om een dossier dat op alle plekken binnen het behandelingscircuit is op te vragen en bij te werken.

Uitwisseling van patiëntinformatie tussen hulpverleners kan op verschillende manieren worden vormgegeven. Daarbij kunnen grofweg twee typen worden onderscheiden:

¹De termen voor de verschillende soorten elektronische dossiers worden niet eenduidig gebruikt. Vaak wordt het GEPD ook met EPD aangeduid. Het Rathenau Instituut gebruikt de term EZD: Elektronisch Zorg Dossier (Berg e.a., 1998). In het artikel 'EZD-studie goed ontvangen' (*Automatisering Gids* 9 april 1999) stelt schrijver T. Smit: "De term EZD is in de gezondheidszorg tot dusver nauwelijks gangbaar. Men spreekt van Elektronische Medische Dossiers (EMD) voor de individuele arts en over een Elektronisch Patiëntendossier (EPD), een virtueel zorgdossier, waarin de informatie over diverse medische zorgverleners is opgenomen." Van Hee gebruikt ook nog de term EBD: Elektronisch Behandel Dossier, dat duidt op het huidige huisarts- dan wel ziekenhuisinformatiesysteem (De Koster 1999).

- Type I : Waarbij automatiseringssystemen binnen instellingen autonoom blijven en waarbij informatie uitwisseling desgevraagd plaatsvindt via een nieuwe infrastructuur. Deze vorm wordt in deze scriptie kortweg: ‘decentraal’ genoemd.
- Type II : Waarbij instellingen gebruik maken van een centrale databank waarin gegevens over patiënten worden bijgehouden. In deze scriptie wordt dat type voortaan met ‘centraal’ aangeduid.

Naast het belang dat de patiënt heeft bij een kwalitatief goed en op maat toegesneden zorgaanbod heeft de patiënt belang bij bescherming van zijn persoonlijke levenssfeer. Er moet worden gezocht naar een afgewogen combinatie van twee in beginsel tegenstrijdige belangen: het belang van adequate informatievoorziening en het privacybelang. Het laatste is een belang dat vooral de patiënt heeft, terwijl bij het eerste zowel patiënt (kwalitatief hoogstaand zorgaanbod) als hulpverlener zijn gebaat. De omvang van de privacyinbreuken (die bij een behandeling onvermijdelijk zijn) dient te worden beperkt. Het opslaan en verzamelen van persoonsgegevens in geautomatiseerde systemen houdt een specifieke bedreiging in van de persoonlijke levenssfeer. Beperking van de mogelijkheid van persoonsgegevens kennis te nemen is een belangrijk aspect van informationele privacy-bewaking. Wanneer medische gegevens tussen een groot aantal verschillende hulpverleners worden uitgewisseld dient dat dan ook van voldoende beschermingswaarborgen te zijn voorzien. Het beroepsgeheim, de gedragsregels en de wet- en regelgeving grijpen hierop terug. Zij beogen niet alleen de exclusiviteit (inzage) van informatie te bewaren, maar ook de integriteit (muteren). De kwaliteit van de opgeslagen gegevens is van cruciale betekenis voor de kwaliteit van het systeem en de op deze informatie gebaseerde gezondheidszorg.

Deze scriptie onderzoekt wat wet- en regelgeving zegt over wie - op welk moment - welke medische gegevens mag inzien. Deze wet- en regelgeving stelt eisen aan de functionaliteit van een GEPD. Tijdens het ontwerpen van een GEPD wordt men gedwongen deze normen in zekere zin te modelleren in het systeemontwerp. Deze scriptie schetst een oplossingsrichting voor normconforme ontsluiting in een GEPD. Steeds dient de praktijk en het huidige ‘papieren traject’ als illustratie- en vergelijkingsmateriaal.

1.1 Opzet van deze scriptie

Samengevat volgt de opbouw van deze scriptie het patroon van de vragen: “wat zijn de normen”, “welke eisen stellen die normen aan het GEPD” en “is het überhaupt mogelijk in een GEPD aan deze eisen te voldoen”.

Meer specifiek heeft dat tot de volgende hoofdstukindeling geleidt. In het tweede hoofdstuk wordt de context van de scriptie besproken. Het geeft aan dat het GEPD als de toekomst wordt beschouwd. Voordelen en kanttekeningen worden geschetst en de kern van het probleem wordt geëxpliciteerd. Daarna wordt de rol van het patiëntendossier besproken. De beperkte toegankelijkheid van het papieren dossier wordt duidelijk na samenvatting van de huidige werkwijze. Informatie blijkt beter toegankelijk in een GEPD. Er wordt aangegeven dat bruikbaarheid van die informatie niet vanzelfsprekend is.

Het derde hoofdstuk gaat over de wet- en regelgeving die privacy beogen te beschermen. Met name de algemene privacybeschermende wetten WPR en WBP worden besproken, daarnaast krijgt de specifiek voor de gezondheidszorg geldende WGBO aandacht en wordt ingegaan op het medisch beroepsgeheim. De artikelen uit WBP en WGBO die specifiek van belang zijn voor ontsluiting van gegevens in het GEPD worden uitgebreid besproken. Per artikel is aangegeven wat het artikel betekent voor het GEPD. Als laatst wordt de samenhang tussen beroepsgeheim, WGBO en WBP voor wat betreft de toegankelijkheid van informatie samengevat. In het vierde hoofdstuk wordt de context nogmaals besproken, daarbij speelt de vraag hoe de bepalingen in het belangrijkste artikel uit de wet aansluiten op de praktijk. Het vijfde hoofdstuk gaat over de uit de normgeving voortvloeiende functionele eisen die aan het systeem kunnen worden gesteld op het gebied van toegankelijkheid. In het zesde hoofdstuk komen procedures en technieken aan de orde die kunnen bijdragen aan normconforme ontsluiting. Het zevende hoofdstuk behandelt de centrale en decentrale variant van een GEPD. Voor- en nadelen van beide varianten worden aangegeven. De scriptie wordt afgesloten met een conclusie.

2. Context

In dit hoofdstuk wordt de context van de scriptie besproken. Het geeft aan dat het GEPD als de toekomst wordt beschouwd. Voordelen en kanttekeningen worden geschetst en de kern van het probleem wordt geëxpliciteerd. Daarna wordt de rol van het patiëntendossier besproken. De beperkte toegankelijkheid van het papieren dossier wordt duidelijk na samenvatting van de huidige werkwijze. Informatie blijkt beter toegankelijk in een GEPD. Er wordt aangegeven dat bruikbaarheid van die informatie niet vanzelfsprekend is.

2.1 GEPD's zijn de toekomst

Wanneer een patiënt gebruik maakt van diensten van meerdere hulpverleners, dan worden er op verschillende plaatsen gegevens over de patiënt vastgelegd: de klachten die de patiënt heeft, de onderzoeken die zijn verricht, de therapie die is ingesteld enz. Deze gegevens kunnen ook van belang zijn voor andere hulpverleners dan degene die in eerste instantie over deze gegevens beschikt. Door gegevens te delen kan dubbel onderzoek voorkomen worden,² kunnen ongewenste interacties tussen therapieën worden voorkomen, kan sneller inzicht worden verkregen in het ziekteverloop van de patiënt enzovoort.³ Het GEPD wordt gezien als instrument om deze doelstelling te realiseren. De verwachtingen rondom het GEPD zijn hooggespannen.⁴ Het wordt door veel partijen beschouwd als de oplossing van verschillende problemen in de zorgsector. Door optimale inzet van IT zouden zowel het primaire zorgproces als daarmee samenhangende processen efficiënter en beter gaan verlopen.⁵ De Raad voor de Volksgezondheid & Zorg noemt het EDP zelfs een must, het papieren dossier voldoet niet meer in verband met zijn slechte toegankelijkheid.⁶ De minister onderschrijft het belang en de prioriteit van de ontwikkeling van het EPD.⁷

Als gangbare definitie van het EPD wordt overigens gebruikt: “het geïntegreerd en elektronisch toegankelijk maken van (onderdelen van) patiëntendossiers, onafhankelijk van plaats en tijd, met het oog op patiënt gerichte zorg“.⁸ Daarmee blijkt overigens ook dat men hetgeen ik hiervoor als GEPD omschreef ook met de term EPD aanduidt. In het vervolg worden de termen dan ook door elkaar gebruikt. Wanneer bedoeld wordt op een stand alone elektronisch patiënten dossier (dat bijvoorbeeld door één huisarts wordt gebruikt) wordt dat expliciet aangegeven.

²Ter Linden 1999, p. 164.

³RVZ advies Informatietechnologie in de zorg 1996, deel 1, p. 7.

⁴Aldus ook Berg e.a. 1998, p. 16.

⁵Aldus ook Berg e.a. 1998, p. 16.

⁶RVZ advies Informatietechnologie in de zorg 1996, deel 1, p. 8.

⁷Kamerstukken II 1997/98, 25 669, nr.2, p. 4.

⁸Programmacommissie ICZ (Y. de Koster, ‘ICZ in een notendop’, *Zorgtelematica Transparant* (4), 1999-1, p.2).

Men streeft ernaar om gegevens uiteindelijk niet als vrije tekst maar in gecodeerde⁹ vorm vast te leggen. Deze eenheid van taal heeft voordelen voor de gezondheidszorg op micro-, meso- en macro niveau. Het maakt voor de hulpverlener uitwisseling van informatie- en het gebruik van beslissingsondersteunende systemen mogelijk (micro niveau), en biedt op hoger niveau mogelijkheden voor onderzoek, bedrijfsvoering, management en beleid. Het RVZ advies noemt standaardisatie essentieel,¹⁰ het rapport geeft aan dat gebruik gemaakt dient te worden van op open standaarden gebaseerde systemen.¹¹ Hiermee hoopt de Raad belemmeringen voor gegevensuitwisseling weg te nemen.

2.2 Kanttekeningen

Naast vergaand techno-optimisme zijn er ook kritische geluiden. In de literatuur wordt veel aandacht besteed aan specifieke juridische en ethische randvoorwaarden, maar deze sterk juridisch-technische analyses zijn abstract en non-empirisch van aard.¹² De aandacht die in de literatuur wordt besteed aan de haken en ogen heeft nauwelijks geleid tot praktische implementatie van normen in systemen. In het efficiency- en doelmatigheids denken wordt privacy vaak beschouwd als last, hindernis en struikelblok. Het rapport van de RVZ vertoont hiervan symptomen.¹³ Mijns inziens is privacybescherming echter een belangrijk kwaliteitselement.

Men zit duidelijk in zijn maag met het vormgeven van de toegankelijkheid van informatie. De vergrote toegankelijkheid voor bij de behandeling betrokken hulpverleners leidt meestal ook tot een vergrote toegankelijkheid voor anderen. Dat laatste moet worden voorkomen. Dat kan door identificatie en authenticatie van gebruikers, versleuteling van gegevens tijdens transport, scheiden van identificerende- en andere gegevens (PET) en controle van gebruik achteraf. De technische mogelijkheden om dit te bewerkstelligen zijn voorhanden, kostbaar, en relatief onomstreden. Dit zijn dan ook de mogelijkheden die breedvoerig worden

⁹Gecodeerd wordt hier niet gebruikt in de betekenis van versleuteld, maar in de zin van eenheid van taal, het vastleggen van gegevens (bijv. klacht, diagnose, verricht onderzoek) volgens een gestandaardiseerde systematiek.

¹⁰RVZ advies Informatietechnologie in de zorg 1996, deel 1, p. 17.

¹¹RVZ advies Informatietechnologie in de zorg 1996, p. 9. Het Coördinatiepunt Standaardisatie Informatievoorziening Zorgsector (CSIZ) ontplooit coördinerende activiteiten met betrekking tot deze standaardisatie.

¹²Berg e.a. 1998, p. 16. Op diezelfde pagina: “Maar het abstracte en non-empirische karakter van deze analyses brengt ook beperkingen met zich mee. De (...) literatuur bediscussieert een aantal belangrijke aspecten die relatief geïsoleerd zijn van praktische contexten, zonder de onderlinge samenhang van deze problematieken te expliciteren”.

¹³Dit verleidde de minister van VWS tot de opmerking: “Als belangrijke randvoorwaarde beschouw ik privacybescherming: ik zie dit niet als een belemmering zoals de RVZ, maar als een voorwaarde voor toepassing van IT in de zorg.” (*Kamerstukken II 1997/98, 25 669, nr. 2, p.4*).

aangehaald in wat Berg e.a. juich-literatuur noemen.¹⁴ Waar opvallend weinig aandacht aan besteed wordt is de vraag: hoe kun je een GEPD zo vormgeven dat alleen diegenen die gegevens mogen gebruiken dat ook kunnen.¹⁵ Dit is precies waar we de kern raken van informationele privacybescherming. Wie gegevens mogen gebruiken is vastgelegd in wet- en regelgeving, wie gegevens kunnen gebruiken wordt bepaald door het systeem. Het gaat hier om een vitaal belang, want de toedeling van inzagebevoegdheid hangt samen met wijzigingsbevoegdheid. Privacybescherming ziet niet alleen op de exclusiviteit van gegevens, maar ook op de kwaliteit ervan. Foutieve gegevens kunnen dodelijk zijn. Het niet beschikbaar zijn van gegevens ook. Daar ligt de kern van het probleem: toegankelijkheid- tegenover exclusiviteit en integriteit van gegevens.

2.3 Doel dossier

Het primaire doel van het patiëntendossier is de ondersteuning van de hulpverlening aan de individuele patiënt. Zowel ter ondersteuning van de taak van de hulpverlener die de gegevens oorspronkelijk heeft vastgelegd, als van andere betrokken hulpverleners. Het dossier heeft wat dat betreft een communicatiefunctie. Zorgrelevante informatie kan medische, verpleegkundige of andersoortige informatie zijn. Het gaat hierbij om een veelheid aan verschillende soorten gegevens zoals symptomen en klachten, resultaten van onderzoek, diagnoses, behandelingsplannen, het ziekteverloop et cetera. Deze gegevens worden gebruikt voor het stellen van een diagnose, prognose, behandeling en follow-up van de patiënt. Met het vastleggen van zijn bevindingen, conclusies etc. legt de hulpverlener tevens verantwoording af ten aanzien van zijn handelen en geeft het inzicht voor medebehandelaars in de samenhang tussen anamnese, diagnostiek en therapie, bijvoorbeeld doordat vastgelegd wordt wat de relatie tussen een diagnose en een therapie is, wat de reden is van wijziging van een therapie of om welke reden een diagnostisch onderzoek is aangevraagd.¹⁶

Het Rathenau instituut vat in haar rapport de rol van het patiëntendossier samen: “dossiers accumuleren inscripties en coördineren activiteiten”. Accumulatie betekent het vergaren en assimileren van zorginformatie: zorgprofessionals schrijven in dossiers, krijgen overzicht over complexe zorgsituaties met behulp van dossiers, en gebeurtenissen worden in dossiers geregistreerd. Coördinatie betekent het op elkaar afstemmen en reguleren van handelingen en gebeurtenissen.¹⁷ Nieuwe informatieverwerkings- en communicatie-mogelijkheden van informatietechnologie kunnen aan beide rollen een actievere invulling geven.

Hier wordt stilgestaan bij de toegankelijkheid van gegevens voor het primaire zorgproces. Bij mogelijkheden die geaggregeerde gegevens bieden voor andere processen als onderzoek, bedrijfsvoering, management en beleid wordt slechts zijdelings stilgestaan.

¹⁴Berg e.a. 1998, p. 16.

¹⁵Met andere woorden hoe kun je een GEPD zo vormgeven dat autorisaties aansluiten bij daadwerkelijke bevoegdheden. Een goede aansluiting is belangrijk want op dit punt vindt potentiële privacy aantasting plaats. Hier komen identificerende- en niet identificerende gegevens bij elkaar, worden gegevens onversleuteld kenbaar en is de inbreuk al geschied voordat controle achteraf kan ‘herstellen’.

¹⁶RVZ advies Informatietechnologie in de zorg 1996, p. 71.

¹⁷Berg e.a. 1998, p. 63.

2.4 Papieren traject

Tegenwoordig wordt nog voornamelijk¹⁸ gebruik gemaakt van het conventionele ‘papieren traject’.¹⁹ In een algemeen ziekenhuis bestaat er voor patiënten die ooit zijn opgenomen een klinisch dossier.²⁰ In dit dossier het geheel van vastgelegde informatie betreffende één patiënt, dat wil zeggen het geheel van zorgrelevante gegevens betreffende die patiënt. Financiële administratie komt er niet in voor. Naast het klinisch dossier bestaan er vaak ook nog poliklinische dossiers. Per specialisme is er meestal sprake van één poliklinisch dossier per patiënt. Hoewel voor het EPD ook deze poliklinische dossiers van belang zijn, concentreren we ons hier op het klinisch dossier. De informatie in deze dossiers is gegeneerd door zorgverleners, als direct resultaat van de interactie met de patiënt of met individuen die persoonlijke kennis over de patiënt hebben (of beide). In het klinisch dossier zit informatie van verschillende hulpverleners, mogelijk met verschillende specialismen, mogelijk ten aanzien van verschillende behandelingen (bijvoorbeeld een bypass- en een liesbreukoperatie) in de loop der tijd. In het dossier zitten kopieën van brieven aan de huisarts (onder andere de ontslagbrief), E.C.G.’s, uitdraaien van lab-uitslagen, statussen. Bij chronisch zieken groeit deze map vaak tot buiten proportie.²¹ Op het moment dat de patiënt ontslagen wordt bergt men het klinisch dossier op in het medisch archief.²²

Wanneer een specialist die een patiënt behandelt een onderzoek bij een andere hulpverlener aanvraagt, doet hij dat door op de, aan de andere hulpverlener gerichte onderzoeksaanvraag, de voor die andere hulpverlener noodzakelijke gegevens te noteren, tezamen met een vraagstelling. Wanneer de andere hulpverlener onverhoopt meer gegevens nodig heeft wendt deze zich daartoe tot de aanvragend arts. Nadat de andere hulpverlener het onderzoek heeft uitgevoerd stuurt hij de aanvragend arts de uitslag van het onderzoek. De communicatie met de huisarts vindt plaats via de verwijfsbrief en de ontslagbrief. In de verwijfsbrief stelt de huisarts de specialist een gerichte vraag n.a.v. de klachten waarvoor hij de patiënt verwijft. Deze vraag wordt vergezeld van informatie met betrekking tot die klacht (bijvoorbeeld klachtverloop en verricht onderzoek). De ontslagbrief wordt door de specialist geschreven aan de huisarts. De specialist meldt samengevat het onderzoek, de resultaten, de diagnose, de behandeling, het resultaat en hetgeen hij na dit ontslag van de huisarts verwacht.²³

Het is belangrijk te constateren dat verstrekking vaak uitgaat van de hulpverlener die de zorg vraagt. De huisarts die doorverwijft naar de specialist, de specialist die een andere

¹⁸Van Hee zegt zelfs dat er in Nederland nog nergens een ècht EPD bestaat (De Koster 1999, p.20).

¹⁹Het rapport (Berg e.a. 1998, p. 60-62) geeft -goed onderbouwd- aan dat het papieren dossier ‘het zo gek nog niet doet’.

²⁰De hier- en verderop genoemde werkwijzen dienen als illustratie, niet als uitputtende opsomming van werkwijzen en procedures. Het is een vergaande versimpeling van de werkelijkheid.

²¹Dat wil zeggen de fysieke omvang van de map uit.

²²Meestal is dit een beveiligde afdeling in een ziekenhuis waar alle klinische dossiers, die op dat moment niet worden gebruikt, zijn opgeslagen.

²³Berg e.a. 1998, p. 82.

hulpverlener om onderzoek vraagt, de specialist die de huisarts om een vervolgbehandeling van de ontslagen patiënt vraagt. Je zou dit kunnen omschrijven als push-informatie.²⁴

De verstrekking gaat niet altijd uit van een andere hulpverlener. Soms bestaat er behoefte aan eerder verzamelde informatie maar bestaat er geen zorgaanvragend hulpverlener die die informatie tot zijn beschikking heeft. In noodgevallen bijvoorbeeld.. Het kan zijn dat de patiënt zelf informatie kan verschaffen maar ingeval van een aan het noodgeval gerelateerde ziektegeschiedenis willen hulpverleners meestal informatie uit het dossier. Zo gebruikt de arts die EHBO dienst heeft vaak het gehele klinische dossier.²⁵ Hier pakt de hulpverlener als het ware de informatie, je zou dat kunnen omschrijven als pull-informatie.²⁶

Bij de eerste soort informatie ligt het initiatief bij de zorgaanvrager (niet bij de uitvoerende hulpverlener), deze aanvrager verstrekt. Voor de uitvoerende hulpverlener wordt een selectie gemaakt uit de tot de zorg-aanvrager ter beschikking staande informatie. Deze selectie heeft verschillende functies waaronder het wegnemen van werklast bij de uitvoerende hulpverlener. Deze hoeft dan niet het gehele dossier door te spitten op zoek naar de voor hem relevante informatie. Daarnaast zet de aanvragende hulpverlener tijdens het samenvatten alles nog eens op een rijtje en destilleert hetgeen voor de geadresseerde belangrijk is.

Niet in alle gevallen is een aanvragend hulpverlener een schakel. Bij de tweede soort informatie ontbreekt een zorgaanvrager en de verstrekking is dus ook niet aan zijn supervisie onderworpen, het initiatief ligt bij degene die de informatie nodig heeft. Alleen anticiperen op eventuele inzage kan nu nog. De informatie vastleggende hulpverlener kan bijvoorbeeld besluiten een uitdrukkelijk toevertrouwd geheim niet in het dossier op te nemen.

Tussenvorm van deze beide soorten informatie is de situatie waarin de door een hulpverlener aangevraagde behandeling aanleiding tot behoefte aan informatie waarin de aanvrager niet heeft voorzien, de ingeschakelde hulpverlener wendt zich met een verzoek om meer informatie tot de zorg-aanvragend arts. Het initiatief ligt bij deze uitvoerende hulpverlener. Toch bepaalt de aanvragend arts hier, waar mogelijk, welke informatie wordt verstrekt. De aanvrager blijft de verstrekker. Dat laatste heeft verschillende functies, de aanvragende arts kan onder andere het best de waarde van de hem ter beschikking staande informatie bepalen. Informatie is namelijk sterk context-gevoelig.²⁷

2.5 Beperkte toegankelijkheid conventioneel dossier

Het conventionele papieren dossier is goed toegankelijk voor degene die de gegevens erin heeft vastgelegd. Dat geldt in mindere mate voor collega-hulpverleners die er gebruik van maken. Het conventionele dossier heeft beperkte structureringsmogelijkheden. Benodigde gegevens zijn hierdoor niet snel terug te vinden. Naast het probleem van de inhoudelijke toegankelijkheid is ook de technische toegankelijkheid beperkt. Een papieren dossier kan

²⁴De zorgaanvragend specialist 'duwt' de informatie als het ware naar de ander. NB. de term push-informatie slaat dus niet op de aard van de informatie zelf, maar op de manier waarop deze is verkregen.

²⁵Meestal beperkt hij zich uit efficiency overwegingen tot de laatste brief aan de huisarts.

²⁶De behandelend specialist 'trekt' de informatie als het ware naar zich toe. NB. ook de term pull-informatie slaat dus niet op de aard van de informatie zelf, maar op de manier waarop deze is verkregen.

²⁷Berg e.a. 1998.

slechts op één plaats tegelijkertijd zijn. Het komt regelmatig voor dat ontslagbrieven, laboratoriumuitslagen en röntgenfoto's elders zijn als men ze nodig heeft.²⁸

Echter papieren dossiers functioneren voor ervaren zorgprofessionals beter dan wordt verondersteld.²⁹ Deze zorgprofessionals beschikken over “effective strategies for limitation of search space by perception of positional and textural features”. Een computerscherm doet wat dat betreft onder voor papieren dossiers. Deze bevatten informatierijke cues zoals ruiters, gekleurde- pagina's en inkt, hun omvang, de verschillende handschriften, opgeplakte notitieblaadjes, onderstrepingen, pijltjes, markeringen enzovoort. De snelheid waarmee een ervaren zorgverlener kan inzoomen op de relevante onderdelen van het dossier is opmerkelijk, en de hoeveelheid informatie die kan worden “covered by a glance is enormous”.³⁰

Maar vooral wanneer er behoefte is aan ‘extra informatie’ schiet het papieren dossier te kort. Het is slecht geschikt voor pull-informatie.

2.6 GEPD toegankelijker

Een GEPD is beter geschikt voor dit soort vragen. Het potentieel aan toegankelijkheid van informatie is namelijk veel groter.

Binnen het GEPD kunnen gegevens op drie niveaus worden vastgelegd: als beeld (fax/foto), als vrije tekst en als gecodeerde gegevens. Het eerste niveau, dat met de term gescand elektronisch patiëntendossier wordt aangeduid, verdient de term EPD volgens de RVZ niet. Dergelijke systemen belemmeren volgens de Raad de ontwikkeling van ‘echte’ GEPD's (tweede en derde niveau) waarin gegevens binnen een adequate structuur als vrije tekst of in gecodeerde vorm worden vastgelegd.³¹ Gecodeerde GEPD's zouden volgens de Raad zeer goed een rol kunnen vervullen bij hulpverlening, informatie van de patiënt, kwaliteitsbeleid, onderwijs, onderzoek, bedrijfsvoering, management en beleid.

Het Rathenau instituut zegt hierover: “De accumulerende rol van dossiers, zo kunnen we concluderen, krijgt nieuwe dimensies door de komst van informatietechnologie. Met actievere accumulatie ontstaan geheel nieuwe gebruiksmogelijkheden, maar dient er ook meer werk te worden verzet om de informatie ‘accumuleerbaar’ te maken. Indien zorggegevens over ‘universele kwaliteiten’ lijken te beschikken dan is dat het resultaat van veel werk, en geen intrinsieke eigenschap die ‘van nature’ in zorginformatie besloten ligt. Zodra dit werk verricht dient te worden om voor derden de gegevens meer inzichtelijk te maken dienen kritische vragen te worden gesteld. Het belasten van toch al zwaar belaste primaire zorgverleners met

²⁸RVZ advies Informatietechnologie in de zorg 1996, deel 2, p. 74.

²⁹Zo concludeert Harper e.a. (R.H.R Harper e.a., ‘Toward the paperless hospital?’, *British Journal of Anaesthesia* (78), p. 762-767) volgens Berg e.a. 1998, p. 62.

³⁰Volgens van Nygren & Henriksson (E. Nygren & P. Henriksson, ‘Reading the medical record. Analysis of physicians’ ways of reading the medical record’, *Computer Methods and Programs in Biomedicine* (39), p. 1-12) in Berg e.a. 1998, p. 62.

³¹RVZ advies Informatietechnologie in de zorg 1996, deel 2, p. 74.

deze additionele taak kost tijd die aan andere bezigheden zou kunnen worden besteed - zoals de patiëntenzorg.”³²

2.7 Samenvatting

Het GEPD wordt beschouwd als de toekomst. En dat ondanks de aanzienlijke risico's die dergelijke systemen met zich meebrengen, onder andere ten aanzien van de privacy van patiënten. Waar te weinig bij stilgestaan wordt is hoe de toegankelijkheid tot gegevens moet worden vormgegeven. Het primaire doel van het patiëntendossier is de ondersteuning van de hulpverlening aan de individuele patiënt. In het papieren traject verstrekt een hulpverlener vaak op eigen initiatief en gericht. Voor het opvragen van gegevens is het minder geschikt. Het GEPD biedt daartoe veel meer mogelijkheden. Het gereed maken voor het gebruik van gegevens voor een ander doel dan het primaire vergt het nodige extra werk.

³²Berg e.a. 1998, p. 70-71.

3. Wet- en regelgeving

Dit hoofdstuk gaat over de wet- en regelgeving die privacy beogen te beschermen. Met name de algemene privacybeschermende wetten WPR en WBP worden besproken, daarnaast krijgt de specifiek voor de gezondheidszorg geldende WGBO aandacht en wordt ingegaan op het medisch beroepsgeheim. De artikelen uit WBP en WGBO die specifiek van belang zijn voor ontsluiting van gegevens in het GEPD worden uitgebreid besproken. Per artikel is aangegeven wat het artikel betekent voor het GEPD. Als laatste wordt de samenhang tussen beroepsgeheim, WGBO en WBP voor wat betreft de toegankelijkheid van informatie samengevat.

3.1 Overzicht

Diverse wet- en regelgeving beogen privacy te beschermen. Algemene privacy regulering is te vinden in het (Europees) Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM), het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR), het Verdrag van Straatsburg, de Europese Algemene Privacy Richtlijn, de Grondwet (GW) en de Wet Persoonsregistraties (WPR). Voor gevoelige gegevens is onder de WPR nog een afzonderlijk besluit van kracht: het Besluit Gevoelige Gegevens. De WPR wordt binnenkort vervangen door de Wet Bescherming Persoonsgegevens (WBP).³³ Bescherming voor specifiek medische persoonsgegevens is te vinden in de Wet op de Geneeskundige Behandelings Overeenkomst (WGBO), de Wet Bijzondere Opnemings Psychiatrische Ziekenhuizen (BOPZ), de Wet op de Beroepen in de in de Individuele Gezondheidszorg (BIG) en de Kwaliteitswet zorginstellingen (KWZ). Deze wet- en regelgeving dient steeds in samenhang te worden gezien met het medisch beroepsgeheim dat daarnaast onverkort blijft gelden.

3.2 Geschiedenis

Mede naar aanleiding van de maatschappelijke onrust die begin jaren '70 ontstond bij de volkstelling is men begonnen met studies naar specifieke algemene privacy wetgeving.³⁴ Ook het Verdrag van Straatsburg was aanleiding voor het tot stand brengen van dergelijke wetgeving. De verdragsluitende partijen bonden zich hier tot het maken van specifieke wetgeving op basis van in het verdrag genoemde minimum principes. De verdragsluitende partijen probeerden zo de hindernissen die wellicht zouden ontstaan bij grensoverschrijdend persoonsgegevensverkeer te ondervangen. De betrokken staten probeerden een balans te vinden tussen de free flow of information en het recht op (informatie) privacy. De Nederlandse invulling van de in het verdrag aangegane verplichting is de Wet op de

³³Aangezien de parlementaire behandeling van dit wetsvoorstel nog niet is afgerond dient WBP vooralsnog gelezen te worden als “wetsvoorstel bescherming persoonsgegevens”.

³⁴Bepalingen in het EVRM (artikel 8), IVBPR (artikel 17) en GW erkennen al een (grond)recht op persoonlijke levenssfeer.

Persoonsregistraties die per 1 juli 1989 gedeeltelijk en per 1 juli 1990 geheel in werking is getreden.

Het Verdrag van Straatsburg veroorzaakte niet genoeg gelijkwaardige wetgeving in de verschillende Europese landen om het doel van onbelemmerd grensoverschrijdend dataverkeer te bereiken³⁵. Toch werd de behoefte daaraan zeker niet minder. Binnen de Europese Gemeenschap is naast een vrij verkeer van personen en goederen ook vrij verkeer van informatie gewenst. De Europese Commissie is dan ook gekomen met een Europese Richtlijn ter harmonisatie van de privacywetgeving van haar lidstaten. Deze richtlijn heeft voor Nederland geleid tot het ontwerp Wet Bescherming Persoonsgegevens die de WPR gaat vervangen. De privacy beginselen die ten grondslag liggen aan de WPR bepalingen hebben niet aan waarde verloren, zij liggen tevens ten grondslag aan de richtlijn en de WBP.

3.3 WPR

De WPR vindt haar grondwettelijke basis in artikel 10 lid 2 en 3 Grondwet. Deze leden behelzen een instructienorm aan de wetgever: het tot stand brengen van wetgeving op het gebied van persoonsgegevens. Zij vormen tevens een mogelijkheid tot beperking van het (grond)recht op eerbiediging van de persoonlijke levenssfeer dat ieder individu heeft op grond van artikel 10 lid 1, het algemeen recht op de eerbiediging van de persoonlijke levenssfeer. Dit is het enige lid van artikel 10 waarop de burger zich direct kan beroepen. Maar alleen ten opzichte van de overheid. Een dergelijk grondrecht regelt immers de relatie overheid naar burger. Zulke bepalingen zijn slechts indirect van belang voor de relatie tussen burgers onderling, bijvoorbeeld bij het bepalen of sprake is geweest van onrechtmatig gedrag. Directe bescherming ten opzichte van andere burgers ontleent de burger aan uit dit artikel afgeleide wetten als de WPR.

De WPR regelt een beperkt deel van een rechtsverhouding. Meestal zijn tegelijkertijd ook andere wetten van toepassing. Deze kunnen te maken hebben met andere materie maar raken soms ook aan dezelfde normen als de WPR. Ze regelen dan op specifiek afgebakende gebieden, zoals bijvoorbeeld Wet op de Inlichtingen en veiligheidsdiensten, ter uitvoering van dezelfde instructienorm. Ze werken aanvullend, zoals bijvoorbeeld Wet invoering Sociaal-Fiscaal nummer. Maar hebben ook wel eens een tegengesteld doel, bijvoorbeeld de Wet Openbaarheid Bestuur.

Voor bepaalde categorieën van gegevens (waaronder medische) is de minister van justitie krachtens artikel 7 WPR gekomen tot het Besluit Gevoelige Gegevens.³⁶ Voor de gezondheidszorg geldt paragraaf 5 van de wet. Aangezien de WPR binnenkort wordt vervangen door de WBP ligt hier de nadruk op de WBP.

³⁵Het verdrag ging immers uit van minimum principes, verschillende landen met (strengere) privacywetgeving verboden verstrekking van gegevens naar andere landen.

³⁶Besluit van 19 februari 1993, Stb.158, houdende regels inzake het opnemen in een persoonsregistratie van persoonsgegevens als bedoeld in artikel 7, eerste lid van de wet persoonsregistraties.

3.4 WBP

Het wetsvoorstel Wet Bescherming Persoonsgegevens behoort eveneens tot de categorie algemene privacy wetgeving. Het is geen overkoepelende privacywet, want zij gaat slechts over informatieve privacy en bijvoorbeeld niet over de ruimtelijke en lichamelijke privacy van mensen.³⁷

De wet vormt de uitvoering van de Europese richtlijn van 24 oktober 1995. De implementatie had voor 26 oktober 1998 voltooid moeten zijn. Nederland is één van de laatste landen waar implementatie nog moet plaatsvinden³⁸.

Naast de richtlijn bestaat er een tweede aanleiding voor de totstandkoming van de WBP, namelijk de evaluatie van de WPR. Er heeft een juridische³⁹ evaluatie plaatsgevonden en een sociaal-wetenschappelijke⁴⁰. Deze onderzoeken concludeerden dat de WPR als strak en bureaucratisch werd ervaren in verband met de grote nadruk op procedure's, en dat de WPR achterloopt op technische ontwikkelingen. Bij het gebruik van ICT technieken is het vastleggen van persoonsgegevens in registraties namelijk slechts een van de mogelijke aspecten van het totale gegevensverwerkingsproces, waaronder alle bewerkingen met betrekking tot persoonsgegevens vallen. Het accent bij de omgang met persoonsgegevens is verschoven van de registratie naar het gehele verwerkingsproces⁴¹. De wetgeving zal dan ook in plaats van op persoonsregistraties 'grijpen' op de verwerking van persoonsgegevens⁴².

Er sprake van een grote mate van continuïteit tussen de WPR en de WBP. De wetgever heeft de Europese Richtlijn waar dat vereist was overgenomen en de bandbreedte die vrij was⁴³ grotendeels conform de WPR ingevuld.⁴⁴ Speciale bepalingen met betrekking tot gevoelige gegevens worden in tegenstelling tot de WPR (Besluit gevoelige gegevens) in de WBP zelf geregeld.

³⁷Hooghiemstra 1999, p. 19.

³⁸Nederland is hiervoor door de Europese Commissie in gebreke gesteld, uitblijven van duidelijkheid kan leiden tot een procedure bij het Europese Hof van Justitie in Luxemburg en hoge boetes of dwangsommen ('Nederland moet Europese privacyrichtlijn volgen', *NRC Handelsblad* 23 augustus 1999).

³⁹Overkleef-Verburg 1995.

⁴⁰Onder leiding van J.E.J. Prins van de Katholieke Universiteit Brabant.

⁴¹Gardeniers 1995, p.22.

⁴²Het begrip *persoonsregistratie* dat in de WPR een centrale rol speelt past niet meer bij de praktijk en de mogelijkheden van de hedendaagse techniek.

⁴³De richtlijn leidt niet tot een volledige harmonisatie van de privacywetgeving, maar biedt een zekere bandbreedte. Het betreft minimum normen die tot een bepaald maximum door de Lid-staten kunnen worden ingevuld.

⁴⁴Hooghiemstra 1999, p. 19; Gevers 1999, p. 64.

3.5 WGBO

De Wet op de Geneeskundige Behandelings Overeenkomst is een voorbeeld van specifieke wetgeving die op het terrein van de gezondheidszorg een zelfstandige regeling in het leven roept ter bescherming van de informationele privacy. In het algemeen heeft deze wet tot doel om de materiële rechtspositie van de patiënt te versterken door een aantal fundamentele aspecten daarvan uitdrukkelijk vast te leggen, de bescherming van de persoonlijke levenssfeer van de patiënt daaronder begrepen.⁴⁵

De wet is van toepassing op patiëntdossiers die worden aangelegd voor/door hulpverleners, deze bevatten immers medische gegevens. Daaronder wordt verstaan: alle gegevens betreffende iemands lichamelijke of geestelijke gezondheid in het verleden, heden of in de toekomst, alsmede genetische gegevens.⁴⁶

Indien een dossier wordt gevoerd in de vorm van een persoonsregistratie in de zin van de WPR, dient de hulpverlener tevens rekening te houden met de verplichtingen op grond van de WPR. Op een aantal punten vormt de WGBO een *lex specialis* ten opzichte van de WPR.⁴⁷ Dat wil zeggen dat op die punten de bepalingen van de WGBO prevaleren boven die van de WPR omdat zij op die punten een specifiekere speciale regeling bieden. Wanneer de WPR zal zijn vervangen door de WBP zullen voor de elektronische dossiers altijd eveneens de bepalingen van de WBP gelden aangezien de WBP ziet op elke geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens (artikel 2 lid 1 WBP). De verhouding tussen WBP en de WGBO is hetzelfde als tussen WPR en WGBO.⁴⁸ De WBP en WGBO zijn ook geen *lex specialis* ten opzichte van elkaar, maar vullen elkaar aan.⁴⁹

3.6 BOPZ

Voor onvrijwillig opgenomen patiënten geldt de wet Bijzondere Opneming Psychiatrische Ziekenhuizen (BOPZ). De BOPZ zou je, eveneens slechts op een aantal punten kunnen beschouwen als *lex specialis* ten opzichte van de WPR/WBP en de WGBO. De WGBO heeft namelijk ook betekenis voor andere dan reguliere behandelingssituaties. De werkingssfeer strekt zich uit over al het geneeskundig handelen, in en buiten de gezondheidszorg, zelfs

⁴⁵Nouwt 1997, p. 224.

⁴⁶Artikel 1 *Appendix to the Draft Recommendation on the Protection of Medical Data*, Raad van Europa, Straatsburg, 23 maart 1993.

⁴⁷De WGBO dient niet als een *lex specialis* te worden beschouwd ten opzichte van de WPR. De WPR (en daarmee de daarop gebaseerde regelgeving) is in beginsel geheel van toepassing op de gegevensbestanden in de gezondheidszorg, tenzij uit de WGBO voortvloeit dat een bijzondere bepaling van toepassing is (Hustinx 1993, p. 411). Zo ook Sluyters & Biesart 1995, p. 71. Een ander uitgangspunt heeft Leenen: “Als algemeen uitgangspunt geldt dat de WGBO een *lex specialis* is ten opzichte van de WPR, ook al is met die typering de onderlinge verhouding tussen beide wetten niet voldoende aangegeven. Zij grijpen in elkaar. Ten aanzien van de rechten van de patiënt is bij dubbel regime een grondregel dat de regeling die de meeste waarborgen biedt prevaleert.” (Leenen 1994, p. 219).

⁴⁸Gevers 1999, p. 65; *Kamerstukken II 1997/98*, 25 892, nr.3, p. 12, 42, 108.

⁴⁹Ter Linden 1999, p. 165.

ongeacht de vraag of ter zake wel van een overeenkomst tussen arts en patiënt/cliënt/burger kan worden gesproken. De WGBO is in beginsel⁵⁰ van toepassing op sterk uiteenlopende gebieden waaronder dwangverblijf op grond van de wet BOPZ.⁵¹

3.7 Kwaliteitswet zorginstellingen en BIG

De Kwaliteitswet zorginstellingen is specifieke gezondheidszorgwetgeving maar heeft slechts zijdelings (onder de noemer 'verantwoorde zorg') tot doel de informatiele privacy te beschermen. In de wet BIG komen bepalingen voor die de privacy beschermen. Voor alle beroepsbeoefenaren die betrokken zijn bij de uitvoering van de wet BIG, dus ook voor diegenen die niet zijn geregistreerd, is in de wet BIG een algemeen geformuleerde geheimhoudingsplicht opgenomen.⁵²

3.8 Medisch Beroepsgeheim

Het medisch beroepsgeheim bepaalt dat individuele hulpverleners geen informatie over hun patiënten aan derden mogen verstrekken. Het biedt dus een vorm van privacy bescherming.⁵³

Het geheim bestaat enerzijds uit een zwijgplicht en anderzijds uit een verschoningsrecht. Het opzettelijk doorbreken van de zwijgplicht is strafbaar gesteld in artikel 272 Wetboek van Strafrecht. De hulpverlener dient te zwijgen over al hetgeen hem in zijn beroepsuitoefening bekend is geworden, hij is bijvoorbeeld voorts zwijgplichtig over wat een derde hem over de patiënt mededeelt. Het geheim komt toe aan de patiënt, ten opzichte van de patiënt kan de hulpverlener zich dus niet op zijn zwijgplicht beroepen.⁵⁴ Het gaat om een plicht van de hulpverlener en niet om een recht.⁵⁵ De zwijgplicht voor de hulpverlener geldt in beginsel ten opzichte van ieder ander dan de patiënt zelf. Meer specifiek geldt ze tegenover andere patiënten, waarmee een patiënt op een zaal ligt, andere hulpverleners die niet bij de behandeling betrokken zijn⁵⁶, ook al hebben deze een eigen zwijgplicht, en tegenover de

⁵⁰Artikel 7:465 BW.

⁵¹Gevers 1994, p. 742.

⁵²Sluyters & Biesart 1995, p. 109.

⁵³Gevers noemt het: "in zekere zin privacybescherming 'avant la lettre'" (Gevers 1990, p. 33).

⁵⁴Uitzondering hierop is de situatie dat een patiënt informatie wordt onthouden omdat mededeling ervan kennelijk ernstig nadeel voor de patiënt met zich mee zou brengen omdat hij die bijvoorbeeld psychisch helemaal niet 'aankan'. Dit wordt ook wel therapeutische exceptie genoemd.

⁵⁵Ook wel als de functionele opvatting van het beroepsgeheim aangeduid (Nouwt 1997, p.94).

⁵⁶Medisch Tuchtcollege Zwolle, 18 april 1953, NJ 1954/179. De zwijgplicht geldt ook ten opzichte van andere artsen wanneer ze niet bij de behandeling zijn betrokken, Leenen zegt hierover: "Het idee dat men ten aanzien van 'artsen onder elkaar' de zwijgplicht minder nauw zou behoeven te nemen, is wellicht terug te voeren op de onjuiste opvatting dat de arts recht op het geheim zou hebben, en op de gedachte dat de collega ook een beroepsgeheim heeft. Uit deze 'intercollegiale loslippigheid' kan een vervolging ex. 272 WvSr volgen. Hetzelfde (wordt vervolgd...)

partner en familieleden van de patiënt. Het beroepsgeheim geldt voor alle informatie die een hulpverlener ter kennis komt, met name wanneer het gaat om feiten die de persoonlijke levenssfeer van de aan hem toevertrouwde patiënt betreffen. De zwijgplicht kan worden doorbroken op grond van een wettelijk voorschrift of door de toestemming van de patiënt. Zo kan gegevensverstrekking plaatsvinden op grond van artikel 2 Wet bestrijding infectieziekten en opsporing ziekteorzaken. Ook de toestemming van de patiënt kan de hulpverlener ontslaan van diens zwijgplicht. In de literatuur wordt wel gesproken van gerichte toestemming, waarmee wordt bedoeld dat de patiënt vooraf dient te weten waarvoor de toestemming wordt gevraagd en welke consequenties daaraan zijn verbonden.⁵⁷

Het verschoningsrecht van de hulpverlener komt aan de orde wanneer hij als getuige wordt verhoord door de rechter. Dit verschoningsrecht komt toe aan hen die zich daarop op grond van de wet en jurisprudentie kunnen beroepen. Niet iedereen die een zwijgplicht heeft, heeft ook het verschoningsrecht.

Het medisch beroepsgeheim is gecodificeerd in onder meer artikel 88 van de wet BIG⁵⁸, artikel 11 derde lid WPR, artikel 9 lid 3 WBP, artikel 7:457 lid 1 en 2 BW. De reden voor de zwijgplicht is de wens van de wetgever om aan de ene kant een sfeer te creëren waarin de samenleving erop moet kunnen vertrouwen dat men zonder terughoudendheid medische hulp kan inroepen (het collectieve aspect), daarnaast bestaat er het individuele aspect: de patiënt moet zonder terughoudendheid alles aan een arts kunnen vertellen en erop kunnen vertrouwen dat die gegevens niet zonder zijn toestemming aan derden worden verstrekt of voor andere doeleinden zullen worden aangewend. Daarnaast dient het beroepsgeheim het belang van de hulpverlener, aangezien het zijn betrouwbaarheid en dat van zijn beroep ten opzichte van het publiek ten goede komt.⁵⁹

3.9 Toespitsing

In voornoemde wet- en regelgeving zijn voor het GEPD een groot aantal artikelen van belang. Privacybescherming wordt geboden wanneer gegevensverwerkingen voldoen aan verschillende criteria, zoals doelbinding, rechtmatige verwerking, toedeling van verantwoordelijk- en aansprakelijkheid, informatieplicht enz. De bepalingen kunnen als een ‘traject’ dienen bij het opzetten van een normconforme verwerking.

Hoewel deze beginselen van cruciaal belang zijn voor legitieme gegevensverwerking wordt hier gefocust op de toegang tot gegevens in GEPD's, dientengevolge worden maar een

⁵⁶(...vervolg)
geldt uiteraard ten aanzien van anderen die beroepsgeheim hebben.” (Leenen 1994, p. 200).

⁵⁷Nouwt 1994, p. 173.

⁵⁸Eenieder die een beroep het gebied van de individuele gezondheidszorg uitoefent heeft een zwijgplicht. Hieronder vallen artsen, tandartsen, apothekers, klinisch psychologen, psychotherapeuten, fysiotherapeuten, verloskundigen en verpleegkundigen. Voor andere betrokkenen van het behandelingsproces geldt een afgeleide geheimhoudingsplicht: assistenten, co-assistenten, medische studenten, biochemici, fysici, paramedische beroepsbeoefenaren, secretaressen etc.

⁵⁹Nouwt 1997, p.95.

beperkt aantal artikelen uit voornoemde regelingen belicht.⁶⁰ Toch raken we juist met deze toegankelijkheid van informatie de kern van informationele privacybescherming. Om niet af te dwalen van de vraagstelling wordt bijvoorbeeld geen aandacht besteed aan: het soort hulpverleners en instellingen dat medische persoonsgegevens mag verzamelen, de grenzen van de reikwijdte van de WBP, minderjarige of onder curatele gestelde patiënten, patiënten die onvrijwillig zijn opgenomen in een psychiatrische instelling, overleden of ongebooren patiënten, keuringen en maar zijdelings aan het gebruik van gegevens voor statistiek of wetenschappelijk onderzoek.⁶¹ De complexiteit van het gebruik van dezelfde medische gegevens door meerdere hulpverleners in een ‘normale’ behandelrelatie biedt al meer dan voldoende materiaal voor een scriptie. We concentreren ons op de WBP, de WGBO en het medisch beroepsgeheim.⁶²

We gaan er van uit dat zowel de WBP op de gegevensverwerking, als de WGBO op de in de dossiers gedocumenteerde behandelrelaties van toepassing is. Immers het betreft gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 1 onder a WBP) en dus persoonsgegevens. Met betrekking tot deze gegevens worden handelingen verricht (verzameld, vastgelegd, bewaard, opgevraagd enz., artikel 1 onder b WBP) en dus verwerkt. De verwerking vindt geautomatiseerd plaats (artikel 2 lid 1 WBP), en we beperken ons tot in Nederland gevestigde gebruikers van het GEPD (artikel 4 lid 1 WBP). De verwerking is noodzakelijk om een wettelijke verplichting na te komen (artikel 8 onder c WBP) aangezien de WGBO de hulpverlener voorschrijft een dossier bij te houden met gegevens omtrent de gezondheid van de patiënt (artikel 454 WGBO), daarnaast is de geneeskundige behandelingsovereenkomst uit de WGBO een overeenkomst waarbij de betrokkene partij is (artikel 8 onder b WBP) en voor wiens uitvoering de verwerking noodzakelijk is.⁶³ De WGBO is van toepassing omdat er sprake is van een overeenkomst inzake geneeskundige behandeling waarbij een natuurlijke persoon of een rechtspersoon, de hulpverlener, zich in de uitoefening van een geneeskundig beroep of bedrijf tegenover een ander, de opdrachtgever, verbindt tot het verrichten van handelingen op het gebied van de geneeskunst, rechtstreeks betrekking hebbende op de persoon van de opdrachtgever of van een bepaalde derde. In ons geval beperken we ons tot de gevallen dat de opdrachtgever zelf de persoon is waarop de geneeskundige handelingen betrekking hebben, simpel gezegd: zelf de patiënt is. Hoewel het in beginsel verboden is gegevens met betrekking tot iemands gezondheid te verwerken (artikel 16 WBP) geldt voor hulpverleners en instellingen voor de gezondheidszorg een ontheffing voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene (i.e. degene op wie de persoonsgegevens betrekking hebben, i.c. de patiënt), dan wel het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is

⁶⁰Niet verder ingegaan wordt er bijvoorbeeld op de algemene bepalingen uit de wet BIG en de summier (Gevers 1999, p. 65) bepalingen uit Kwaliteitswet zorginstellingen, ook de specifieke regeling in de wet BOPZ wordt niet verder behandeld. Daarnaast wordt zoals eerder aangegeven wel aandacht besteed aan bepaalde aspecten van de manier van opslag van gegevens. Artikelen die daarvoor van belang zijn worden eveneens belicht.

⁶¹Toch zal een systeem dat in de praktijk toegepast gaat worden ook met de consequenties van eerdergenoemde bepalingen omstandigheden ‘om moeten kunnen gaan’.

⁶²Op de BOPZ, BIG en Kwz wordt bijvoorbeeld niet nader ingegaan.

⁶³Ter Linden 1999, p. 165.

(artikel 21 lid 1 onder a WBP). Deze ontheffing geldt ook voor -andere dan medische- gevoelige gegevens wanneer dit noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene (artikel 21 lid 3 WBP).

Voorgaande conclusies werden hier snel getrokken, in de volgende paragraaf blijven we bij een aantal bepalingen uit WBP en WGBO langer stilstaan.

3.10 Overzicht en toelichting specifieke bepalingen

Allereerst worden voor het overzicht de specifieke artikelen per wet opgesomd, daarna worden de bepalingen per wet uitgelegd en de consequenties ervan voor het GEPD duidelijk gemaakt. Daarbij moet in het achterhoofd gehouden worden dat de bepalingen een grotere invloed op het GEPD hebben dan de hier genoemde. De hier genoemde invloed richt zich namelijk op de vraagstelling van de scriptie, waarbij het gaat om de toegankelijkheid van gegevens in het primaire proces. Met name de volgende bepalingen zijn voor ons van belang:

WBP

- Artikel 7. Doelbinding verzameling.
- Artikel 9. Doelbinding verwerken en strijd met geheimhoudingsplicht.
- Artikel 11. Kwaliteitswaarborgen gegevens.
- Artikel 12. Geheimhoudingsverplichting.
- Artikel 13. Beveiligingsplicht verantwoordelijke.
- Artikel 14. Beveiligingsplicht bewerker.
- Artikel 34. Informatieplicht bij verkrijgen informatie anders dan van betrokkene.
- Artikel 35. Inzagerecht.
- Artikel 36. Recht op verbetering, aanvulling en verwijdering.
- Artikel 38. Verbetering aan derde verstrekte gegevens.

WGBO

- Artikel 448. Inlichtingen door de hulpverlener en therapeutisch exceptie
- Artikel 449. Recht om niet te worden geïnformeerd.
- Artikel 452. Inlichtingenplicht patiënt.
- Artikel 453. Goed hulpverlenerschap.
- Artikel 454. Dossierplicht, eigen verklaring patiënt en bewaartermijn.
- Artikel 455. Vernietiging op verzoek patiënt.
- Artikel 456. Recht op inzage en afschrift.
- Artikel 457. Geheimhouding. Persoonlijke levenssfeer derde.
- Artikel 458. Gebruik van gegevens voor statistiek en wetenschappelijk onderzoek.
- Artikel 463. Exoneratieverbod.
- Artikel 468. Dwingend recht.

WBP

- ad. Artikel 7 & 9 WBP:
Doelbinding verzamelen, verwerken en strijd met geheimhoudingsplicht
Artikel 7 en 9 zijn de codificatie van het doelbindingsbeginsel. Dit houdt in dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde

doeleinden mogen worden “verzameld”. Verder bepaalt artikel 9 dat ze niet mogen worden “verwerkt”⁶⁴ op een wijze die onverenigbaar⁶⁵ is met de doeleinden waarvoor de gegevens zijn verkregen. Tenslotte wordt in lid 3 van artikel 9 verwerking verboden die in strijd zou zijn met een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift. De doelbindingsbepalingen zijn voor het GEPD van belang aangezien zij verstrekking⁶⁶ verbieden die onverenigbaar is met de doeleinden waarvoor de gegevens zijn verkregen. Daarnaast mag in een GEPD mag geen verwerking plaatsvinden die in strijd is met het medisch beroepsgeheim.

- ad. Artikel 11 WBP:

Kwaliteitswaarborgen gegevens

Dit artikel beoogt de inhoudelijke kwaliteit van persoonsgegevens te waarborgen. Persoonsgegevens mogen slechts worden verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld en verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn. De verantwoordelijke dient de nodige maatregelen te treffen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens verwerkt, juist en nauwkeurig zijn. Volgens de memorie van toelichting legt dit artikel op degene die de gegevens verwerkt een continue verplichting tot toetsing.⁶⁷ In het GEPD worden gegevens vastgelegd om te worden gebruikt door een brede kring hulpverleners, dat is ook het doel van een GEPD.⁶⁸ Gegevens moeten zodoende voldoende nauwkeurig zijn om door die brede kring hulpverleners gebruikt te worden.⁶⁹ Dat betekent wel extra werk voor de hulpverleners die de informatie vastleggen. Zorginformatie is gebonden aan de context waarin zij tot stand is gekomen. Los van hun context verliezen gegevens aan betekenis. Hulpverleners zijn nu gewend gegevens voor gebruik in eigen kring vast te

⁶⁴NB. Onder verwerken worden handelingen met betrekking tot persoonsgegevens verstaan waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede afschermen, uitwissen of vernietigen van gegevens (artikel 1 onder b. WBP).

⁶⁵Een voorbeeld van onverenigbaarheid is het gebruik van gegevens die zijn verzameld in het kader van een ziekteverzekering (loondervingsverzekering) voor het beoordelen van een aanvraag voor een ziektekosten verzekering (Holleman e.a. (Artikelsgewijs commentaar WBP 1240)).

⁶⁶In hun algemeenheid verbieden de artikelen elke onverenigbare verwerking, niet alleen het verstrekken, en zijn zo veel breder voor het GEPD van belang. De speciale aandacht voor verstrekken is een gevolg van de eerder genoemde ‘focus’ van de scriptie. Er wordt bijvoorbeeld ook niet ingegaan op de vraag of het doel: “kwalitatief hoogstaande gezondheidszorg voor patiënten mensen in Noord-Holland” te breed is. Hoewel een (centraal) GEPD staat of valt met de aanvaardbaarheid van een dergelijke doelomschrijving. Het antwoord op een dergelijke vraag is cruciaal voor de legitimiteit van een GEPD. Wanneer bovenstaande doelomschrijving voldoende begrensd blijkt, waar ligt dan het omslagpunt? Bij de grenzen van Nederland, Europa? Ondanks het belang van deze kwestie wordt er in deze scriptie verder geen aandacht aan besteed.

⁶⁷Holleman e.a. (Artikelsgewijs commentaar WBP 1240) verwijst naar *Kamerstukken II 1997/98*, 25 892, nr.3, p. 96.

⁶⁸RVZ advies Informatietechnologie in de zorg 1996, deel 2, p. 75.

⁶⁹Ook de tuchtrechter wijst herhaaldelijk op het belang van een goede verslaglegging voor overdrachtssituaties en voor waarnemers en opvolgers (Sluyters & Biesart 1995, p. 62).

leggen. De gegevens zitten nog vast in hun locale gebruikscontext. Voor gebruik binnen deze kring volstaat deze manier van vastleggen⁷⁰, maar voor zinvol gebruik van deze gegevens in toekomstige behandelrelaties moet er veel extra werk worden verricht.⁷¹

- ad. Artikel 12:

Geheimhoudingsverplichting

Dit artikel geldt voor personen die niet reeds een ambts- of medisch beroepsgeheim hebben. Voor het GEPD betekent dit dat iedereen die er mee werkt, en die niet reeds uit hoofde van een medisch beroepsgeheim een zwijgplicht heeft, in ieder geval op grond van dit artikel een geheimhoudingsverplichting heeft, los van een eventuele afgeleide geheimhoudingsplicht. De geheimhoudingsplicht op grond van dit artikel is minder absoluut dan het medisch beroepsgeheim en een daarvan afgeleide geheimhoudingsplicht.

- ad. Artikel 13:

Beveiligingsplicht verantwoordelijke

Dit artikel sluit aan bij artikel 8 WPR. De verantwoordelijke dient technische en organisatorische maatregelen te treffen teneinde de gegevens te beveiligen. De verplichting tot beveiliging richt zich tegen “verlies” of “onrechtmatige verwerkingen” van persoonsgegevens, zoals onbevoegde kennisname, aantasting, wijziging of verstrekking van de gegevens. De beveiligingsplicht strekt zich uit tot alle onderdelen van het proces van gegevensverwerking. Er is een passend beveiligingsniveau vereist. In dit begrip ligt besloten dat de beveiliging in overeenstemming dient te zijn met de stand van de techniek, het duidt ook op proportionaliteit tussen de te nemen beveiligingsmaatregelen en de belangen van de betrokkenen. Bij de afweging spelen de aard van de gegevens en de context waarin de gegevens worden gebruikt een rol. Naarmate de gegevens een gevoeliger karakter hebben, dan wel de context waarin de gegevens worden verwerkt een grotere bedreiging voor de persoonlijke levenssfeer inhoudt worden zwaardere eisen gesteld aan de beveiliging van gegevens.⁷² In relatie tot het ‘zusterartikel’ (artikel 8) in de WPR is gezegd dat de Registratiekamer beveiliging beschouwt als een bijzonder aandachtspunt⁷³, en daarom een aantal eisen heeft geformuleerd, die een nadere invulling geven aan de wettelijke norm in dat artikel. De mate van beveiliging staat in relatie tot de persoonsgegevens. De

⁷⁰Sterker nog, deze manier van vastleggen is wellicht waardevoller dan vergaand gecodeerde gegevens. Immers voor het lokale zorgproces zo belangrijke nuances en details verdwijnen achter de ‘generieke’ code en zorprofessionals dreigen het overzicht kwijt te raken wanneer ze worden geconfronteerd met een overdosis aan geïsoleerde ‘items’ (Berg e.a. 1998, p. 70).

⁷¹Dat betekent dat gegevens in de praktijk vaak niet gecodeerd worden, het levert degene die het werk verricht namelijk niet direct iets op (Otten & Wildevuur 1996, p. 771). Berg e.a. zeggen daarover: “Zodra dit werk verricht dient te worden om voor derden de gegevens meer inzichtelijk te maken dienen kritische vragen te worden gesteld. Het belasten van toch al zwaar belaste primaire zorgverleners met deze additionele taak kost tijd die aan andere bezigheden zou kunnen worden besteed - zoals patiëntenzorg” (Berg e.a. 1998, p. 71).

⁷²Holleman e.a. (Artikelsgewijs commentaar WBP 1240).

⁷³Registratiekamer rapport Beveiliging persoonsregistraties 1994, p. 4.

aard van de betrokken gegevens leidt in casu tot het stellen van hoge eisen⁷⁴ aan de bescherming van die gegevens en de beveiliging van de communicatie. Deze aanbevelingen gelden tegelijkertijd als uitgangspunt voor de wijze waarop de Registratiekamer haar toezichthoudende taak uitoefenend. Er is geen aanleiding te veronderstellen dat er met betrekking tot het nieuwe artikel een andere invulling gegeven gaat worden aan het beveiligingsbeginsel. Het bepaalde in het rapport is mijns inziens dan ook onverkort van toepassing op het GEPD. In de WPR bestonden naast de beveiligingsbepaling (artikel 8 WPR) nog specifieke bepalingen over verstrekking. In artikel 6 lid 2 WPR wordt verstrekking binnen de organisatie van de registratiehouder geregeld⁷⁵, in artikel 11 lid 1 WPR werd verstrekking aan derden⁷⁶ geregeld. Deze drie artikelen waren specifiek van belang voor de toegankelijkheid van gegevens. In de WBP is het gehele verwerkingsproces (dus ook verstrekken) gebonden aan verenigbaarheid met het oorspronkelijke doel (artikel 9 lid 1 WBP) en is alleen het overgebleven beveiligingsartikel hier specifiek van belang voor toegankelijkheid: de beveiligingsplicht die zich richt tegen onrechtmatige verwerkingen van persoonsgegevens, zoals onbevoegde kennisname, aantasting, wijziging of verstrekking van de gegevens. De kwaliteit van de beveiliging is ook van belang met betrekking tot de verderop genoemde eigen verantwoordelijkheid⁷⁷ van elke individuele hulpverlener voor wat betreft het toevertrouwen van medische informatie aan een systeem. Het systeem moet voldoende waarborgen bieden.

- ad. Artikel 14:

- Beveiligingsplicht bewerker.

- De verantwoordelijke die gegevens verwerkt wil hebben buiten zijn rechtsreeks gezag, door een bewerker, is op grond van dit artikel verplicht om met deze bewerker een overeenkomst aan te gaan. De strekking van deze bepaling is te voorkomen dat de verantwoordelijke en de bewerker zich wat betreft hun verantwoordelijkheden achter elkaar zouden kunnen verschuilen.

- Voor het GEPD is dit artikel van belang omdat het via lid 3 onder a voor de bewerker dezelfde beveiligingsplicht als voor de verantwoordelijke in het leven roept. Sommige hulpverleners of externe ICT bedrijven kunnen als bewerker worden beschouwd.⁷⁸

⁷⁴Het vereiste niveau is afhankelijk van de exclusiviteitsklasse die aan de persoonsregistratie moet worden toegekend op basis van een risico analyse. De beoogde systemen blijken te vallen in exclusiviteitsklasse 3: *hoog risico*, daaruit volgt een eis tot zware beveiliging (additionele beveiligingseisen ten opzichte van het basisniveau waaraan elke persoonsregistratie moet voldoen).

⁷⁵Artikel 6 lid 2 WPR luidt: “Binnen de organisatie van de houder worden uit een persoonsregistratie slechts gegevens verstrekt aan personen die ingevolge hun taak die gegevens mogen ontvangen”.

⁷⁶Artikel 11 lid 1 WPR luidt: “Uit een persoonsregistratie worden slechts gegevens aan een derde verstrekt voor zover zulks voortvloeit uit het doel van de registratie, wordt vereist ingevolge wettelijk voorschrift of geschiedt met toestemming van de geregistreerde”.

⁷⁷En daaruit volgende risicoansprakelijkheid.

⁷⁸In artikel 1 onder e WBP wordt als bewerker immers gedefinieerd: “degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen”. Aan indeling van de GEPD deelnemers in termen van de WBP en dergelijke wordt, hoe belangrijk ook, in het kader van de focus van deze scriptie echter geen verdere aandacht besteed.

- ad. Artikel 34:
Informatieplicht bij verkrijgen informatie anders dan van betrokkene
Het artikel schept een informatieplicht voor de verantwoordelijke bij verkrijging anders dan van de betrokkene zelf. De hulpverlener informeert de patiënt hierover of legt wanneer dit onmogelijk is de herkomst van gegevens vast (lid 4).
Voor het GEPD waarvan de kern is ‘informatieverstrekking binnen brede kring’ is dit artikel van belang wanneer gegevens niet direct van de patiënt zelf zijn verkregen (in dat geval geldt immers de uitgebreide informatieplicht uit artikel 33 WBP), maar uit het GEPD.
- ad. Artikel 35:
Inzagerecht
De betrokkene kan de verantwoordelijke benaderen met verzoeken om informatie, hetgeen een belangrijk onderdeel is van het aan de wet ten grondslag liggende transparantiebeginsel. Op deze wijze kan de betrokkene nagaan waar en door wie gegevens worden verwerkt. De verantwoordelijke geeft een volledig overzicht⁷⁹, alsmede de beschikbare informatie omtrent de herkomst van gegevens. Wanneer een derde naar verwachting bezwaar heeft tegen deze inzage ‘omdat er gegevens tussen zitten die hem betreffen’⁸⁰ moet de verantwoordelijke een belangenafweging maken, de derde moet in staat gesteld worden zijn zienswijze te geven.
- ad. Artikel 36 & 38:
Recht op verbetering, aanvulling en verwijdering, ook van aan derden verstrekte gegevens
In artikel 36 is het correctierecht vastgelegd. In artikel 38 is vastgelegd dat deze correcties aan derden aan wie de nog ongecorrigeerde informatie is verstrekt moeten worden doorgegeven. Binnen het GEPD moet het mogelijk zijn op verzoek van de patiënt correcties aan te brengen. Wanneer ‘foutieve’ gegevens zijn verstrekt dienen de ontvangers van de correctie op de hoogte te worden gesteld.⁸¹

WGBO

- ad. Artikel 448:
Inlichtingen door de hulpverlener en therapeutisch exceptie
Onder omstandigheden worden inlichtingen⁸² niet aan de patiënt verstrekt wanneer dat kennelijk ernstig nadeel voor de patiënt zou opleveren. Hier is getracht twee belangrijke

⁷⁹Holleman e.a. (Artikelsgewijs commentaar WBP 1240).

⁸⁰In patiëntendossiers in de GGz komt relatief veel informatie met betrekking tot derden voor.

⁸¹Zij zouden de informatie namelijk opgenomen kunnen hebben in hun autonome systeem. Bij een centraal GEPD speelt dit door het ontbreken van ‘informatie duplicatie’ minder.

⁸²Er bestaat een fundamenteel verschil tussen het recht op informatie en het inzagerecht. Het recht op informatie waar dit artikel op doelt (en waarop in het besproken lid 3 een uitzondering wordt gemaakt) hangt zeer nauw samen met het geven van toestemming die nodig is voor het verrichten van medische handelingen. Het inzagerecht staat daarentegen in beginsel los van enige concrete medische handeling en beoogt toezicht te kunnen houden op persoonsgegevens die zijn vastgelegd (Nouwt 1997, p. 228).

rechten van de patiënt zo goed mogelijk met elkaar in evenwicht te brengen, namelijk het recht op goede en volledige informatie en het recht op zo goed mogelijke medische zorg. In het GEPD kan informatie aanwezig zijn waarbij dat gevaar voor ernstig nadeel aanwezig is. Deze informatie zal dus ook niet via het GEPD tóch bij de patiënt terecht mogen komen.

- ad. Artikel 449:

Recht om niet te worden geïnformeerd

Wanneer een patiënt aangeeft bepaalde inlichtingen *niet* te willen ontvangen dan respecteert de hulpverlener dit verzoek (onder voorwaarde dat het nadeel dat daaruit voor de patiënt en anderen voortvloeit niet te groot is).

Ook hier mag deze informatie niet via het GEPD tóch bij de patiënt terecht mogen komen.

- ad. Artikel 452:

Inlichtingenplicht patiënt

Naast de hulpverlener is de patiënt verplicht naar beste weten inlichtingen en medewerking te geven die de hulpverlener redelijkerwijs voor het uitvoeren van de behandelingsovereenkomst behoeft. Dit kan erin bestaan dat de patiënt gegevens over hemzelf aan de hulpverlener verstrekt of instemt met de toegang tot elders reeds eerder opgeslagen persoonsgegevens. Er is niet beoogd een afdwingbare verplichting in het leven te roepen.⁸³

- ad. Artikel 453:

Goed hulpverlenerschap

In dit artikel wordt met de voor hulpverleners geldende professionele standaard bedoeld op de *medisch*-professionele standaard.⁸⁴ 'Goed hulpverlenerschap' zal overigens niet mogen leiden tot inperking van de in de wet toegekende rechten van de patiënt. Inbreuken op deze rechten zijn alleen mogelijk voor zover expliciet geregeld bij of krachtens wet. Goed hulpverlenerschap is voor het GEPD in het kader van deze scriptie van belang omdat het onder andere invulling geeft aan de in artikel 457 genoemde zorgplicht van de hulpverlener.

- ad. Artikel 454:

Dossierplicht, eigen verklaring patiënt en bewaartermijn

Dit artikel verplicht de hulpverlener met het oog op een goede hulpverlening medische dossiers in te richten. Dat brengt onder omstandigheden de aanleg van een gegevensverwerking met zich mee. De verplichting ziet niet op persoonlijke werkaantekeningen van de hulpverlener, omdat deze geacht worden niet voor communicatie bestemd te zijn, doch slechts voor de eigen gedachtevorming (persoonlijke gebruik) van de hulpverlener.⁸⁵ De patiënt kan de hulpverlener niet ontslaan van de dossierplicht. De hulpverlener moet de noodzakelijke gegevens vastleggen, zelfs tegen de

⁸³Nouwt 1997, p. 232. Het artikel is volgens Nouwt in de literatuur nogal omstreven omdat het opleggen van een dergelijke verplichting niet thuis zou horen in de WGBO en bovendien niet afdwingbaar zou zijn.

⁸⁴Leenen 1994, p. 159.

⁸⁵Van Lomwel & Van Veen 1996, p. 92; Nouwt 1997, p. 234, 236; Sluyters & Biesart 1995, p. 65.

uitgesproken wil van de patiënt in.⁸⁶ De hulpverlener is verder verplicht op verzoek van de patiënt een door hem afgegeven verklaring met betrekking tot de reeds in het medische dossier aanwezige stukken toe te voegen aan dat dossier. Zo'n verklaring kan bijvoorbeeld de zienswijze over een aangelegenheid van de patiënt of van een andere hulpverlener bevatten. De bewaartermijn die geldt voor in het dossier opgenomen bescheiden is tien jaar. Wanneer dat redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit mogen ze langer worden bewaard.

Wanneer het GEPD een functie bevat voor persoonlijke werkaantekeningen⁸⁷ dan mogen deze ook alleen maar toegankelijk zijn voor de hulpverlener die ze heeft gemaakt. Wanneer ze op een of andere wijze in de communicatiesfeer terecht komen verliezen zij hun persoonlijke karakter en gaan ze tot het dossier behoren.⁸⁸ Het gevaar van een persoonlijke werkaantekeningen-functionaliteit is dat hulpverleners hierin, uit angst voor gebruik door derden (bijvoorbeeld omdat ze niet 'gecontroleerd' willen worden) gegevens gaan opnemen die in het dossier zelf thuishoren. Daarnaast is het natuurlijk niet zo dat het plichtmatig karakter van deze bepaling (vastlegging vindt plaats zelfs tegen de uitgesproken wil van de patiënt in) strekt tot de legitimatie van vastlegging en gebruik van gegevens binnen een gemeenschappelijk te gebruiken elektronisch patiënten dossier (GEPD) in die zin dat de patiënt er niks over te vertellen heeft. Het GEPD moet in verband met de bewaartermijn in staat zijn gegevens te dateren.

- ad. Artikel 455:

Vernietiging op verzoek patiënt.

De patiënt heeft recht op de vernietiging van gegevens, die in de door de hulpverlener bewaarde stukken (het dossier) voorkomen. Wanneer hij daartoe verzoekt moet de hulpverlener binnen 3 maanden aan dit verzoek voldoen. Er zijn daarop een aantal uitzonderingen waaronder wanneer de bewaring van de gegevens van aanmerkelijk belang is voor een ander dan de patiënt.

Dit is voor het GEPD van belang omdat van gegevens moet duidelijk zijn bij welke hulpverlener ze horen, en of ze informatie met betrekking tot anderen bevatten (dan is er vergrootte kans op aanmerkelijk belang voor die ander).

- ad. Artikel 456:

Recht op inzage en afschrift

Wanneer de patiënt dat wenst dient de hulpverlener hem zonder tussenkomst van derden, inzage en afschrift te verstrekken van het in artikel 454 genoemde dossier. Een uitzondering daarop is wanneer het belang van de bescherming van de persoonlijke levenssfeer van een ander een overwegend karakter heeft.

⁸⁶Dat blijkt uit de memorie van toelichting p. 35 (Sluyters & Biesart 1995, p. 63). De patiënt heeft daarnaast overigens wel recht op vernietiging of aanvulling van de gegevens (artikel 455 en 454 lid 2 WGBO).

⁸⁷Dat is wel zo praktisch, de hulpverlener heeft zo zijn persoonlijke werkaantekeningen en het dossier van de patiënt snel bij de hand.

⁸⁸Sluyters & Biesart 1995, p. 66.

- ad. Artikel 457:

Geheimhouding. Persoonlijke levenssfeer derde

Dit is, voor deze scriptie, het belangrijkste artikel uit de WGBO. Aangezien het hier uitgebreid wordt besproken is de wetstekst van de eerste twee leden van het artikel opgenomen:

Artikel 457. 1. “(...) draagt de hulpverlener zorg, dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage of afschrift van de bescheiden bedoeld in artikel 454 (dossier *m.t.*) worden verstrekt dan met toestemming van de patiënt. (...)”⁸⁹

2.: “Onder anderen dan de patiënt zijn niet begrepen degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de hulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden”.

De bepaling geeft antwoord op de vraag hoever de geheimhoudingsplicht van de hulpverlener reikt inzake verstrekking van patiëntgegevens door middel van het geven van inzage of het geven van afschrift. De in deze bepaling neergelegde hoofdregel houdt kortgezegd in dat voor het verstrekken van informatie aan anderen dan de patiënt vooraf toestemming van de patiënt nodig is, tenzij een wettelijke bepaling tot gegevensverstrekking verplicht. Verder bepaalt het eerste lid van dit artikel dat verstrekking alleen kan plaatsvinden voor zover daardoor de privacy van een ander niet wordt geschaad. Voordat de arts informatie verschaft aan anderen dient hij derhalve na te gaan of de eventueel in het dossier opgenomen gegevens over derden daarvan uitgesloten moeten worden.

Uitzondering op de vereiste toestemming wordt gemaakt door in bepaalde gevallen toestemming te veronderstellen, veronderstelde toestemming geldt voor personen die rechtstreeks bij de behandeling betrokken zijn alsmede de vervanger of waarnemer van de arts. Ingevolge het tweede lid van dit artikel kunnen deze over de voor hen in het kader van de behandeling noodzakelijke gegevens beschikken, zonder dat daarvoor de uitdrukkelijke toestemming van de patiënt nodig is.⁹⁰ Deze uitzondering heeft onder anderen betrekking op medebehandelaars, assistenten, verpleegkundigen en doktersassistenten. De behandelend arts zal moeten bepalen welke gegevens ‘noodzakelijk’⁹¹ zijn en of dat bijvoorbeeld ook geldt voor in het dossier aanwezige gegevens over anderen dan de patiënt. De toestemming wordt verondersteld, dit betekent dat de patiënt desgewenst kan aangeven dat bepaalde gegevens ook niet aan deze bij de behandeling betrokkenen kenbaar

⁸⁹Omwille van de duidelijkheid worden hier slechts de voor ons relevante delen van het lid geciteerd. Met de bescheiden bedoeld in artikel 454 wordt het dossier bedoeld, deze aanwijzing is mijn toevoeging (*m.t.*).

⁹⁰Doppegieter 1993b, p. 512.

⁹¹Dat is dus waarschijnlijk niet alle informatie die met betrekking tot deze behandelingsovereenkomst is verzameld, en helemaal niet alle informatie die met betrekking tot eerdere behandelingen is verzameld, maar slechts die gegevens die op grond van de huidige behandelingsovereenkomst voor de door die andere hulpverleners in dat kader uit te voeren werkzaamheden noodzakelijk zijn.

mogen worden⁹²: hij behoudt de mogelijkheid een geheim uitdrukkelijk aan een bepaalde hulpverlener toe te vertrouwen.⁹³

Men kan constateren dat de hulpverlener met wie de patiënt een behandelingsovereenkomst sluit een speciale verantwoordelijkheid krijgt toebedeelt t.a.v. de aan hem toevertrouwde gegevens.⁹⁴ Dat zijn meer gegevens dan de door hem in het kader van de behandeling ingeschakelde collega-hulpverleners ter beschikking krijgen.⁹⁵ Wanneer de patiënt door een andere hulpverlener, bijvoorbeeld de huisarts, naar die hoofdhulpverlener is doorverwezen heeft ook daar een selectie van gegevens plaatsgevonden, toegesneden op de door die hoofdhulpverlener te starten behandeling. Je zou kunnen zeggen dat in een normale situatie de hoofdbehandelaar een soort poortwachters functie heeft. Deze functie heeft een zorginhoudelijk aspect, maar ook een privacy beschermend aspect. Het is goed te beseffen dat de zorgpraktijk niet altijd naadloos aansluit bij dit systeem der wet, dat bij de contractspartij-hulpverlener een rol legt als coördinator van zorg en daarmee van gegevensverstrekking.⁹⁶

Zoals in het vorige hoofdstuk al werd geschetst heeft bij spoedgevallen de hoofdhulpverlener soms de beschikking over meer gegevens, er is geen aanvragend hulpverlener en tijd om de te verstrekken gegevens toe te snijden op de behandeling. De poortwachtersfunctie wordt dan niet vervuld. Spoedgevallen vormen in bepaalde gevallen een rechtvaardigingsgrond, namelijk wanneer er sprake is van ‘noodtoestand’.

Noodtoestand is een confrontatie met een actuele concrete nood. Het leven van de patiënt heeft prioriteit boven de bescherming van zijn privacy. Juridisch leidt dat bij doorbreken van de zwijgplicht tot overmacht, dat staat in de weg aan strafbaarheid. ‘Noodtoestand’ komt in de gezondheidszorg natuurlijk veelvuldig voor.

Mèt uitdrukkelijke toestemming van de patiënt mogen aan derden inlichtingen worden verstrekt. De toestemming moet in vrijheid gegeven worden en op voldoende informatie berusten. De toestemming moet gericht worden gegeven en concreet zijn; een blanco volmacht is niet toereikend.⁹⁷

De gevolgen van deze bepaling voor het GEPD zijn groot. Men zou kunnen betogen dat informatie ontsluiting buiten de behandelrelatie om, plaats kan vinden wanneer de patiënt maar toestemming geeft (lid 1). Echter toestemming tot gebruik van medische gegevens in

⁹²Doppegieter 1995b, p. 1270.

⁹³Wanneer de behandeling door deze andere hulpverleners niet door kan plaatsvinden zonder deze gegevens, dan moet de patiënt een afweging maken. Vaak is een behandeling door deze andere hulpverleners (anders dan de term “noodzakelijk” doet vermoeden) echter ook zonder deze gegevens mogelijk. In de Geestelijke Gezondheidszorg is zoiets bijvoorbeeld goed voorstelbaar .

⁹⁴Van Lomwel & Van Veen 1996, p. 69.

⁹⁵Bookelman 1996, p. 686.

⁹⁶Zie over deze problematiek in het algemeen, en met name met betrekking tot transmurale ‘zorg op maat’ het artikel van Hulst & Kerff 1998.

⁹⁷Sluyters & Biesart 1995, p. 105; Beljaars 1994, p. 746.

het GEPD komt te dicht in de buurt van een blanco volmacht.⁹⁸ Hoewel de arts die zijn patiëntendossier laat bijhouden in een centraal registratiesysteem daarvoor wel de uitdrukkelijke toestemming van zijn patiënt nodig heeft⁹⁹, legitimeert deze toestemming alleen, de terbeschikkingstelling van gegevens voor ontsluiting in het GEPD niet. Daarnaast is de hulpverlener namelijk verplicht er bij gegevensverstrekking voor te zorgen dat zijn gedrag verenigbaar is met de zorg van een goed hulpverlener.¹⁰⁰ Ondanks toestemming van de patiënt kan de hulpverlener besluiten niet te verstrekken.¹⁰¹ Het artikel impliceert een zorgplicht ten aanzien van de hem toevertrouwde gegevens.¹⁰² Hij blijft uiteindelijk verantwoordelijk voor het zorgvuldig en behoorlijk gebruik van de verstrekte gegevens, getoetst aan de normen die het medisch beroepsgeheim (via 'goed hulpverlenerschap' aan de WGBO gekoppeld) daaraan stelt. Uit de zorgplicht volgt dat het bij verstrekking aan andere *niet* bij de behandeling betrokken hulpverleners met toestemming van de patiënt niet zo mag zijn dat de verstrekte informatie volkomen los staat van de mogelijke nieuwe behandeling waar deze hulpverleners wèl bij zijn betrokken. Direct bij de huidige behandeling betrokkenen zouden op grond van lid 2 alleen voor hen in het kader van de door hen te verrichten werkzaamheden noodzakelijke informatie krijgen, terwijl anderen alle informatie tot hun beschikking krijgen, omdat zij toestemming hebben van de patiënt. De enkele grondslag 'toestemming van de patiënt' rechtvaardigt dat niet.

Hoe abstracter hetgeen waarvoor de patiënt toestemming heeft gegeven, des te minder deze toestemming alléén, verstrekking rechtvaardigt. Bij het GEPD is het probleem dat gegevens niet voor een concrete situatie verstrekt worden, maar 'klaargezet worden' voor eventuele toekomstige verstrekking ten bate van deze- of een nieuwe behandeling. De hulpverlener zal, als dat al mogelijk is, zijn zorgplicht op voorhand moeten vervullen. Hij zal erop vooruit moeten lopen. Deze actieve zorgplicht impliceert dat hij de gegevens niet zal mogen toevertrouwen aan een systeem dat onvoldoende mogelijkheden biedt om daarop vooruit te lopen. Dat geldt ook in het algemeen, de hulpverlener zal de gegevens

⁹⁸ Van Herten: "Hierbij is de vraag in hoeverre de toestemming van de patiënt om gegevens op te slaan perfect kan zijn, als de patiënt niet kan overzien wat bewaard wordt en wie inzage heeft. Met name kan men zich afvragen of een in het kader van een actuele behandeling gegeven toestemming tot vastlegging van gegevens, mede inhoudt dat die gegevens vele jaren na het afsluiten van die behandeling nog door derden mogen worden ingezien." (Van Herten 1995, p. 78).

⁹⁹In de memorie van toelichting, *Kamerstukken II*, 21 561, p. 18 (Hulst & Kerff 1998, p. 496).

¹⁰⁰Nouwt 1997, p. 238.

¹⁰¹In de literatuur wordt er op gewezen dat dit een uitzonderingssituatie is (Sluyters & Biesart 1995, p. 105; Leenen 1994, p. 203). Mijns inziens is het mede een uitzonderingssituatie omdat het daar steeds de wens van de patiënt was gegevens te verstrekken. Hier is het niet de concrete wens van de patiënt, maar wordt als het ware 'op de zaken vooruitgelopen'. In deze situatie kun je dan ook telkens (i.t.t. uitzondering) zeggen dat toestemming van de patiënt onvoldoende is.

¹⁰²Registratiekamer advies Medische zorgpas 1995, p. 8: "De hulpverlener draagt er zorg voor dat aan derden geen inlichtingen of gegevens worden verstrekt zonder voorafgaande toestemming van de patiënt of zonder dat daaraan een wettelijke regeling ten grondslag ligt. Dit vergt een actieve instelling van de hulpverlener om te voorkomen dat persoonsgegevens ten onrechte bij (onbevoegde) derden terechtkomen."

niet mogen toevertrouwen aan een systeem dat onvoldoende waarborgen biedt voor de bescherming van de geheimhouding.¹⁰³

Het GEPD zal redelijkerwijs ook een voorziening moeten bieden die in geval van nood (bijvoorbeeld het eerder genoemde ‘noodtoestand’) direct informatie over een patiënt vrijgeeft. Er dient te worden voorkomen dat een dergelijke achterdeur de achilleshiel van het GEPD wordt. Het leerstuk van de noodtoestand ontslaat hulpverleners natuurlijk niet van hun plicht waar mogelijk de privacy-inbreuk te voorkomen en anders de omvang ervan te beperken.

Het GEPD zal informatie met betrekking tot een ander (in de zin van een ander dan de patiënt) moeten kunnen herkennen, in een medisch dossier kan immers ook informatie voorkomen met betrekking tot anderen dan de patiënt. Informatie door anderen gegeven over de patiënt, zichzelf of andere personen, of door de patiënt gegeven informatie over anderen. Deze anderen zouden bijvoorbeeld kunnen zijn: de ouders, voogd of leerkracht van de patiënt. Ten aanzien van informatie door anderen gegeven geldt dat de hulpverlener ook zwijgplichtig is over wat die derde hem over de patiënt mededeelt. Deze gegevens zullen dus slechts onder dezelfde voorwaarden als de overige gegevens mogen worden verstrekt. Deze anderen kunnen uiteraard evenals de patiënt een geheim uitdrukkelijk toevertrouwen, met andere woorden bepalen dat de gegevens slechts aan bepaalde kring van personen kenbaar mogen worden gemaakt. Ten aanzien van informatie over anderen geldt dat verstrekking slechts mag plaatsvinden voor zover daardoor de persoonlijke levenssfeer van die ander niet wordt geschaad. Wanneer de gegevens door de ander zelf zijn verstrekt zal deze duidelijk moeten worden gemaakt hoe deze informatie zal worden gebruikt. Hij kan dan uiteraard bezwaar maken/beperkingen aangeven.

- ad. Artikel 458:

Gebruik van gegevens voor statistiek en wetenschappelijk onderzoek

Onder voorwaarden kunnen patiëntgegevens uit het dossier ten behoeve van statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid worden gebruikt. Een van de voorwaarden is dat de patiënt daartegen geen uitdrukkelijk bezwaar heeft gemaakt (lid 2 onder c). Hier dit belangrijk voor de manier van opslag van gegevens. Ingevolge lid 3 moeten gedane verstrekkingen voor wetenschappelijk onderzoek in het dossier worden vastgelegd. In het GEPD moet dat dus ook gebeuren.

- ad. Artikel 463:

Exoneratieverbod

De aansprakelijkheid van een hulpverlener kan niet worden beperkt of uitgesloten.

- ad. Artikel 468:

Dwingend recht

Van de bepalingen in de WGBO kan niet per overeenkomst worden afgeweken. Zij behelzen dwingend recht. In het GEPD kan men dus niet door middel van contractuele

¹⁰³Ploem 1999, p. 57; Leenen 1994, p. 216; Registratiekamer advies Medische zorgpas 1995, p. 14: “Zo zal hij ondanks toestemming geen medische gegevens op kunnen nemen in een systeem dat omtrent geheimhouding onvoldoende waarborgen biedt”.

bepalingen een andere verantwoordelijkheidsverdeling ten opzichte van de patiënt¹⁰⁴ scheppen.

3.11 Samenloop

Simpelgezegd geldt: “het GEPD mag medische persoonsinformatie verstrekken wanneer WBP, WGBO en medisch beroepsgeheim geen belemmeringen opwerpen”. Wanneer het medisch beroepsgeheim eraan in de weg staat kunnen gegevens niet worden verwerkt (artikel 9 lid 3 WBP), ook al is verwerking op grond van de rest van de WBP wèl geoorloofd. Voorzover bepalingen in de WGBO (in een bepaalde situatie) al niet een correcte codificatie van het medisch beroepsgeheim zijn, wordt het via artikel 453 (goed hulpverlenerschap) ‘boven’ de WGBO ingeschakeld in die zin dat wanneer het beroepsgeheim een door de WGBO geoorloofde verstrekking verbiedt, het medisch beroepsgeheim prevaleert. Over de verhouding tussen WPR en WGBO kan gezegd worden dat wanneer beide soorten regelingen op een zelfde punt verschillend regelen, in dat geval wordt aangenomen dat die bepaling, die de betrokkene het meest beschermt, voorgaat.¹⁰⁵ Wanneer dat geen uitsluitel biedt dan kan de regel dat de bijzondere wet aan de algemene derogeert uitkomst brengen.¹⁰⁶ Aangezien voor het beoogd gebruik de WGBO de ruimste bescherming biedt gaat hier de WGBO voor.

Daarnaast blijft het natuurlijk zo dat wanneer sprake is van noodtoestand, WBP, WGBO en de zwijgplicht uit het medisch beroepsgeheim opzij kunnen worden gezet. Zo kunnen medische persoonsgegevens bijvoorbeeld tòch worden verstrekt aan een hulpverlener in een land dat in termen van de WBP onvoldoende bescherming biedt, wanneer deze gegevens nodig zijn om het leven van de patiënt te redden.

3.12 Samenvatting

Verschillende wet- en regelgeving bevatten regels die de informationele privacy beogen te beschermen. Bepalend voor de beoogde verstrekkingen blijkt met name het medisch beroepsgeheim, dat gedeeltelijk is gecodificeerd in artikel 457 WGBO. Dat artikel blijkt specifiek van belang voor de beoogde verstrekkingen.

¹⁰⁴Wanneer meerdere partijen in een GEPD participeren is het wel verstandig verantwoordelijkheden en aansprakelijkheden -ten opzichte van elkaar- te expliciteren. Dat zou kunnen door het opstellen van een interchange agreement (R.van Esch, ‘Interchange agreements’, *The EDI Law Review* (1) 1994, p. 3-41).

¹⁰⁵Gevers 1999, p. 65; Hooghiemstra (1999, p. 27) noemt *Kamerstukken II* 1990/91 21 561, nr. 6, p. 6 en 1991/92, 21 561, nr. 11, p. 4 en verder.

¹⁰⁶Gevers 1999, p. 65.

4. Context revisited

In dit hoofdstuk wordt de praktijk en de beoogde praktijk in een GEPD gelegd langs de bepalingen uit artikel 457. Zij sluiten niet altijd op elkaar aan. Allereerst wordt er ingegaan op veronderstelde toestemming, daarna op de poortwachtersfunctie van bepaalde hulpverleners. Daaropvolgend wordt aangegeven dat de papieren werkwijze een aanvaarde invulling van de zorgplicht blijkt en waarom. Enkele voordelen van het papieren traject ten opzichte van het GEPD worden geschetst, maar ook papieren onvolkomenheden komen aan bod. Daarna blijkt de ruimte die de exacte formulering van de wetstekst lijkt te laten voor ruimere verstrekking, te worden afgesloten door de strekking en het systeem der wet. De paragraaf die hierop volgt behandelt de vraag wat er moet gebeuren wanneer gegevens gebruikt gaan worden in het kader van de uitvoering van een andere behandelingsovereenkomst dan die waarin ze zijn verzameld. Uiteindelijk wordt in de laatste paragraaf een aan privacybescherming en het medisch beroepsgeheim ten grondslag liggend beginsel geformuleerd.

4.1 Veronderstelde toestemming en poortwachtersfunctie

Het juridisch systeem past zoals eerder gemeld niet altijd even goed op de ontstane praktijksituatie zoals transmurale zorgarrangementen of toekomstige plannen zoals het GEPD. Eigenlijk heeft het nooit goed op pull-informatie gepast. Wanneer bij een spoedopname medische informatie (vastgelegd met betrekking tot de uitvoering van oude behandelingsovereenkomsten) wordt opgevraagd door de nieuwe behandelaar, kan dit worden ondergebracht in het stelsel der wet¹⁰⁷ door toestemming van de patiënt te veronderstellen. De ‘oude’ hulpverlener heeft dan voldaan aan zijn zorgplicht uit artikel 457 WGBO. Aan anderen dan de patiënt worden immers geen inlichtingen over de patiënt dan wel inzage in of afschrift van bescheiden verstrekt dan met toestemming van de patiënt. Bij een dergelijke constructie begeven we ons natuurlijk op glad ijs. In een noodgeval rechtvaardigt de situatie dat. Bij een dergelijke verstrekking met veronderstelde toestemming kunnen twee varianten worden onderscheiden. In de eerste is de ‘oude’ hulpverlener voor handen om te verstrekken. Bij de tweede wordt er verstrekt doordat de nieuwe hulpverlener de beschikking krijgt over het gehele klinische of poliklinische dossier, of doordat informatie via de fax aan hem wordt verstuurd. Het gehele klinische of poliklinische dossier wordt verstrekt wanneer het gaat om hulpverleners uit hetzelfde ziekenhuis. Wanneer het gaat om hulpverleners uit verschillende instellingen zal men zich van de fax bedienen. Wanneer de ‘oude’ hulpverlener ontbreekt zal de nieuwe hulpverlener dus informatie pakken (pull-informatie).

In de eerste variant is de ‘oude’ hulpverlener nog in staat zijn poortwachtersfunctie te vervullen. In de tweede variant niet. Binnen het GEPD vindt er in toenemende mate raadpleging van gegevens van hulpverleners door andere hulpverleners plaats, zonder dat die eerste hulpverleners in staat zijn hun poortwachtersfunctie uit te oefenen. Het GEPD zal een gedeelte van die functionaliteit moeten overnemen. Men is daartoe, zoals we hierboven zagen, gedwongen door het medisch beroepsgeheim en verschillende bepalingen in de wet. Er zal een

¹⁰⁷Wanneer het gaat om dezelfde of gerelateerde klacht of complicatie zou je de verstrekking in het systeem der wet kunnen scharen onder een verstrekking aan ‘rechtstreeks bij de behandeling betrokkenen’ (artikel 457 lid 2 WGBO).

aanvaardbare balans tussen toegankelijkheid en privacybescherming gevonden moeten worden.

4.2 Aanvaarde balans

Het papieren klinisch dossier is een in de praktijk aanvaarde balans tussen toegankelijkheid en privacybescherming. Blijkbaar heeft de hulpverlener¹⁰⁸ met het toevertrouwen van het dossier aan het medisch archief zijn zorgplicht voldoende vervuld. Het systeem van procedures dat ongeautoriseerde kennisneming daarvan belet wordt schijnbaar voldoende geacht. Dat betekent niet dat de uiteindelijke informatieverstrekking goed aansluit op de wettelijke vereisten. Er wordt immers het gehele klinische dossier verstrekt of niets. En dat terwijl de wet een op de werkzaamheden toegesneden verstrekking beoogd voor bij de behandeling betrokkenen (artikel 457 lid 2 WGBO), of anders toestemming is vereist (op grond van lid 1 WGBO).¹⁰⁹ Het verstrekken van alles of niets is gelet op deze bepalingen dus eigenlijk niet aanvaardbaar. Dat het toch wordt aanvaard komt doordat daarnaast de fysieke toegankelijkheid van het papieren dossier beperkt is. In de regel zullen de medewerkers van het archief, waarin de dossiers achter slot en grendel zijn opgeborgen, geen dossiers meegeven aan mensen die ze niet herkennen uit de kleine kring van hulpverleners en medewerkers binnen de instelling. Verder is het archief voor kwaadwillenden minder interessant omdat het informatie over relatief (in vergelijking tot het GEPD) weinig mensen bevat, namelijk alleen van die mensen die ooit in dat ziekenhuis zijn opgenomen. Inzage is daarnaast opvallender want fysieke aanwezigheid is noodzakelijk en een kopie maken duurt lang. Toch is ook het papieren dossier in dit opzicht niet vlekkeloos. Hulpverleners (artsen en verpleegkundigen) kunnen alle informatie van een patiënt in het dossier zien, ook die met betrekking tot eerdere losstaande behandelingen. Hulpverleners krijgen dossiers mee zonder dat er getoetst wordt op behandelrelatie, dossiers liggen op een afdeling vaak welhaast voor eenieder voor het grijpen¹¹⁰ enzovoorts.

4.3 Ogenschijnlijke ruimte

Je zou kunnen betogen dat de letterlijke formulering in de wetstekst van lid 2 van artikel 457 “voor zover de verstrekking noodzakelijk is” ruimte laat voor verstrekking van meer dan noodzakelijke gegevens aan direct bij de behandeling betrokkenen. Er staat immers niet dat de

¹⁰⁸Om te spreken van *de* hulpverlener is ook in dit verband een juridische fictie. In het papieren klinisch dossier zit vaak informatie van verschillende hulpverleners, soms ook van verschillende hoofdbehandelaars (i.v.m. verschillende behandelingen).

¹⁰⁹Doppegieter (Doppegieter 1995b, p. 1270) noemt een dergelijke toegankelijkheid zonder toestemming van de patiënt niet conform de WGBO.

¹¹⁰Dat laatste werd pijnlijk duidelijk in een aflevering van Radar. Een medewerker van het programma kon zich op afdelingen van het AMC en het VU ziekenhuis ongehinderd toegang verschaffen tot medische dossiers die daar in grote getale aanwezig waren, ter illustratie bladerde hij ze door en nam er een aantal mee naar buiten (*Radar, Tros Nederland 2*, 7 oktober 1996). Deze uitzending was voor het D66 Tweede-Kamerlid Van Boxtel aanleiding tot het stellen van kamervragen (*Aanhangsel Handelingen II* 1996/97, nr. 233).

verstrekke gegevens noodzakelijk moeten zijn voor de werkzaamheden. De verstrekking moet noodzakelijk zijn. Deze redenering doortrekkend zou je kunnen betogen dat de bepaling dus ruimte laat voor verstrekking van het gehele klinische dossier, ook al bevat het meer dan de noodzakelijke gegevens. In deze gedachtegang is het namelijk noodzakelijk dat aan de hulpverlener het gehele klinische dossier wordt verstrekt aangezien hij anders helemaal niets te zien krijgt. Een dergelijke gedachtegang houdt geen stand aangezien de strekking van dit lid 2 het beperken van gegevensverstrekking is. Beperken van verstrekking tot degene die ‘need to know’ en beperken van de omvang van de verstrekking tot ‘voor zover noodzakelijk voor hun werkzaamheden’. Een dergelijke beperking van de gegevensverstrekking beperkt de omvang van de privacyinbreuk.

Verstrekking van het gehele dossier wordt ook verdedigd aan de hand van het betoog dat toegang tot meer gegevens noodzakelijk is, dan die uiteindelijk voor de behandeling noodzakelijk blijken. De hulpverlener zal zelf op medische gronden moeten kunnen bepalen welke informatie hij gebruikt. Toch lijkt daarvoor in het systeem der wet slechts voor de hoofdhulpverlener (in de wet *de* hulpverlener) ruimte te zijn geschapen. De andere bij de behandeling betrokken hulpverleners schijnen het volgens de wet te moeten doen met de door de hoofdverlener gemaakte selectie. Immers de in lid 1 genoemde zorgplicht van de hulpverlener geldt niet met betrekking tot rechtstreeks bij de behandeling betrokkenen voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden. De hulpverlener zal informatie aan hen dus toegesneden verstrekken.

4.4 Gebruik gegevens in nieuwe behandeling

Een ander probleem met de inpassing van de praktijk in de wetgeving is de overgang tussen behandeling en nieuwe behandeling. Het is de vraag wat er moet gebeuren wanneer gegevens gebruikt gaan worden in het kader van de uitvoering van een andere behandelingsovereenkomst dan die waarin ze zijn verzameld. De wetgeving is duidelijk over het vereiste van toestemming van de patiënt. De veronderstelde toestemming waarmee wordt gewerkt wanneer een patiënt in het kader van dezelfde behandeling wordt behandeld door andere hulpverleners is onvoldoende. Er zal uitdrukkelijk gerichte toestemming gevraagd moeten worden voor verstrekking. Aangezien in een GEPD deze verstrekking mogelijkwijs in de toekomst plaats gaat vinden kan de patiënt niet goed overzien waarvoor hij de toestemming geeft.¹¹¹ Toestemming vooraf, voor het beschikbaar houden van gegevens is dus onvoldoende voor het daadwerkelijk gebruik. Op het moment dat zich een nieuwe concrete behandelingssituatie voordoet zal dan ook opnieuw toestemming gevraagd moeten worden. Wanneer er sprake is van een noodsituatie en de patiënt bijvoorbeeld niet meer bij kennis is, kan toestemming worden verondersteld. Deze veronderstelde toestemming moet zodra mogelijk worden geverifieerd.¹¹²

¹¹¹En dat is wel nodig (Sluyters & Biesart 1995, p. 105; Beljaars 1994, p. 746).

¹¹²Het gebruik van de ‘oude’ gegevens is dan natuurlijk niet meer terug te draaien, wèl kan voortzetten van het gebruik worden stopgezet en kunnen aanwezige gegevens worden vernietigd.

4.5 Samenvatting

De bepalingen uit de wet sluiten niet goed aan op alle in de praktijk gewenste verstrekkingen, met name niet op verstrekkingen in noodgevallen, verstrekking van het gehele dossier in het ‘papieren’ traject en verstrekkingen met het oog op gebruik in toekomstige behandelrelaties. Eerder is al opgemerkt dat de in de WGBO aan de contractspartij-hulpverlener impliciet toebedeelde rol van zorg-coördinator en daarmee van bewaker van het dossier in de praktijk niet altijd past. De behoefte aan duidelijkheid voor deze situaties waarop wetgeving niet geweldig aansluit kan worden ingevuld door het ‘need to know’ beginsel. Deze al eerder bij de strekking van lid 2 genoemde dimensie van het vertrouwensbeginsel ligt goed beschouwd aan de basis van elke legitieme verstrekking van gegevens waarvoor het medisch beroepsgeheim geldt. Alleen aan hen die noodzakelijkerwijs moeten weten, behoeven gegevens te worden doorgegeven. Deze noodzaak tot het verkrijgen van gegevens is aanwezig bij hulpverleners die een patiënt behandelen, bij betrokkenen bij die behandeling en bij hulpverleners die een patiënt voor dezelfde, gerelateerde of andere klachten in de toekomst gaan helpen. Voor de eerste twee groepen is de wetgeving duidelijk. Voor de laatste minder. Alleen toestemming van de patiënt voor beoogde verstrekkingen via het GEPD is onvoldoende, dat werd al eerder betoogd in de artikelsgewijze toelichting in hoofdstuk 3. De hulpverlener blijft naast die toestemming een zorgplicht houden. Een aspect daarvan is dat verstrekking slechts plaatsvindt op need to know basis.

De formulering in lid 1 van artikel 457: “draagt (...) zorg, dat (...) geen inlichtingen (...) worden verstrekt” laat ruimte voor indirecte verstrekking aan hulpverleners die niet bij de huidige behandeling betrokken zijn. De hulpverlener hoeft de gegevens niet zelf te verstrekken. Hij moet er voor zorgen dat ze niet *worden verstrekt*. Dat betekent dat de uiteindelijke verstrekking ook gedaan kan worden door iets of iemand anders: bijvoorbeeld medewerkers van het klinisch archief, of via het GEPD.

De procedure die bij deze uiteindelijke verstrekking in acht wordt genomen moet voldoende waarborgen bieden voor het bestaan van de vereiste need to know basis.

5. Functionaliteits eisen

In dit hoofdstuk wordt beschreven welke functionaliteit het GEPD zal moeten bieden met het oog op de toegang tot gegevens, uitgaande van de hiervoor beschreven wet- en regelgeving. Er worden een aantal eisen geformuleerd aan de hand waarvan later technieken en procedures kunnen worden ontworpen en getoetst.

Het is goed te beseffen dat het hier slechts eisen betreft die op grond van de WGBO aan het GEPD gesteld kunnen worden, daarbij gaat het met name om eisen met betrekking tot de toegankelijkheid in het primaire zorgproces. Daarnaast zijn er andere eisen die uit de rest van de WGBO, de WBP of andere wet- en regelgeving voortvloeien. Maar wet- en regelgeving is natuurlijk niet de enige bron van functionaliteits vereisten. Informatietechniek stelt eisen, bijvoorbeeld aan de representatie van informatie. De praktijk stelt de nodige eisen, bijvoorbeeld aan de gebruiksvriendelijkheid en toegankelijkheid enzovoorts.

5.1 Eisen met betrekking tot toegankelijkheid

Toegang tot gegevens zal moeten zijn toegesneden op:

- De behandelrelatie
Slechts wanneer een hulpverlener een behandelrelatie met de patiënt heeft, of op andere wijze direct bij de behandeling betrokken is bestaat recht op kennisname van medische gegevens (lid 1 en 2 van artikel 457 WGBO). Dat betekent dat de persoon van de hulpverlener en de persoon van de patiënt moeten kunnen worden herkend. Immers een patiënt heeft via zijn behandeling een relatie met een bepaalde hulpverlener.
- De te verrichten werkzaamheden
De kennisname moet zoveel mogelijk zijn toegesneden op de te verrichten werkzaamheden. Voor de hoofdhulpverlener (in het systeem der wet de contractspartij-hulpverlener) en voor de hoofdverlener in een toekomstige behandelrelatie betekent dat toegang tot meer gegevens dan voor, door hen ingeschakelde, hulpverleners. Dat betekent dat moet kunnen worden herkend of de hulpverlener hoofdbehandelaar, medebehandelaar (i.d.z.v. lid 2) of andere (in de zin van lid 1 artikel 457 WGBO) is. Bij het beantwoorden van de vraag “wat zijn de te verrichten werkzaamheden” is de zorgvraag van belang, maar ook de functie van de hulpverlener en de rol die hij in de behandeling aanneemt.¹¹³
- Toestemming
Slechts met toestemming van de patiënt zal aan anderen (in de zin van lid 1 artikel 457 WGBO) toegang mogen worden verleend. Dat betekent dat duidelijk moet zijn òf de patiënt toestemming heeft gegeven, en met betrekking tot welke gegevens (heeft hij wellicht voorbehoud gemaakt met betrekking tot bepaalde gegevens).
- Anderen

¹¹³Een psychiater bijvoorbeeld kan bij een behandeling verschillende rollen hebben. In het ene geval is hij hoofdbehandelaar, in het andere geval waarnemer (niet in de zin van voor een ander waarnemend, maar in de zin van toezichthouder). De functie alleen (psychiater) zegt dus niet alles.

Voor wat betreft informatie met betrekking tot anderen gelden speciale zorgvuldigheidsregels.

Dat betekent dat moet worden herkend welke gegevens uit het dossier informatie met betrekking tot anderen bevatten, en welke gedeelten daarvan te privacy-gevoelig zijn voor verstrekking. Daarbij moet duidelijk zijn ten opzichte van welke kring van personen deze gevoeligheid geldt, behandelaars (verstrekking, artikel 457 lid 1 WGBO), patiënt (inzage, artikel 456 WGBO) of derden (artikel 457 lid 1 WGBO). Verder moet duidelijk zijn of deze informatie in de weg staat aan vernietiging van gegevens (artikel 455 lid 2 WGBO).

- Bewaartermijn

Informatie die tien jaar oud is en die ook niet langer behoeft te worden bewaard dient te zijn verwijderd (artikel 454 WGBO) en is dus ook niet meer via het GEPD benaderbaar. Dat betekent dat de leeftijd van gegevens bekend moet zijn.

- Bezwaar onderzoek

Wanneer de patiënt bezwaar gemaakt heeft tegen gebruik van zijn gegevens voor wetenschappelijk onderzoek (artikel 458 WGBO) dan dient de toegang tot die gegevens voor wetenschappelijk onderzoek onmogelijk te worden gemaakt.

- Niet willen weten

Wanneer er informatie aanwezig is waaromtrent de patiënt niet geïnformeerd wil worden dan dient dat voor gebruikers van die gegevens via het GEPD ook duidelijk te zijn, zodat de patiënt ook niet via via wordt geïnformeerd (artikel 449 WGBO).¹¹⁴

- Therapeutische exceptie

Wanneer er informatie aanwezig is waaromtrent is aangenomen dat kennisname door de patiënt te schadelijk is, dan dient dat voor gebruikers van die gegevens duidelijk te zijn, zodat de patiënt deze inlichtingen ook niet via via te horen zal krijgen (artikel 448 WGBO).¹¹⁵

- Persoonlijke werkaantekeningen

Wanneer er informatie in de vorm van werkaantekeningen in het GEPD aanwezig is dan mogen deze gegevens slechts door de hulpverlener zelf worden ingezien (zie artikelsgewijze uitleg artikel 454 WGBO). Dat betekent dat de eigenaar van gegevens bekend moet zijn.

¹¹⁴Dat wil niet zeggen dat de gegevens niet aan anderen verstrekt mogen worden, maar dat die anderen tijdens kennisname op de hoogte worden gebracht van het speciale karakter van die inlichtingen.

¹¹⁵Ibidem.

5.2 Haalbaarheid en automatiseerbaarheid

Het is de vraag of een GEPD als systeem van geautomatiseerde en menselijke processen in staat is deze functionaliteit te bieden. De geautomatiseerde delen van het GEPD alleen zullen zeker niet alle vereisten uit de wet kunnen vervullen. Het filteren van informatie op bijvoorbeeld ‘noodzakelijk in het kader van de gewenste werkzaamheden’ is werk van mensen, en wel van medische professionals. Dat kan maar gedeeltelijk worden overgenomen door automatische processen. Toch zal in het GEPD door combinatie van techniek en procedures uiteindelijk een aanvaardbare balans gevonden moeten worden tussen toegankelijkheid van informatie en privacybescherming.

5.3 Samenvatting

Wet en regelgeving stelt diverse eisen aan de toegankelijkheid van gegevens in een GEPD. Het is de vraag in hoeverre deze functionaliteit kan worden geboden met behulp van geautomatiseerde processen. Het antwoord op deze vraag wordt in het volgende hoofdstuk gezocht.

6. Mogelijkheden

Het vorige hoofdstuk werd afgesloten met de opmerking dat in het GEPD door combinatie van techniek en procedures uiteindelijk een aanvaardbare balans gevonden moet worden. In dit hoofdstuk worden enkele procedures en technieken besproken die daar een bijdrage aan kunnen leveren.

Een voorbeeld van een procedure is de werkwijze waarbij de benodigde toestemming van de patiënt voor het verstrekken aan anderen (uit artikel 457 lid 1 WGBO) wordt ingevuld door deze te delen in toestemming voor het ‘klaarzetten’ van gegevens voor evt. toekomstig gebruik in het GEPD en toestemming voor het daadwerkelijk gebruik van eerder klaargezette gegevens in een concrete situatie. Wanneer die laatste toestemming wordt vormgegeven doordat de patiënt zijn chipcard desgewenst als toegangssleutel laat gebruiken is een ideale combinatie van procedure en techniek gevonden. Deze opzet is ook door de RVZ gesuggereerd. Enkel een dergelijke combinatie biedt onvoldoende bescherming. Maar een veelheid van dergelijke combinaties biedt wellicht wèl een aanvaardbare balans.

Hoewel ICT mogelijkheden biedt tot bescherming blijken geautomatiseerde dossiers in de praktijk zeer slecht beveiligd.¹¹⁶ Dat is in strijd met de wetgeving. In een GEPD waarin veel verschillende mensen, ook buiten instellingsmuren met gegevens gaan werken is dat onaanvaardbaar. Hierna worden een aantal technieken beschreven die zouden kunnen bijdragen aan een betere beveiliging.

Computer beveiliging wordt vaak gedefinieerd als een combinatie van confidentialiteit, integriteit en beschikbaarheid.¹¹⁷ In deze scriptie zijn met name de eerste twee van belang.¹¹⁸

6.1 Toegangscontrole

Toegangs- ofwel access control wordt gedefinieerd als “the prevention of unauthorised use of a resource, including the preventions of use of a resource in an unauthorised manner”.¹¹⁹

Het beveiligen van de toegang tot systemen betreft die maatregelen die voorkomen dat onbevoegden toegang kunnen krijgen tot computersystemen en daarin opgeslagen gegevens.¹²⁰ Het valt uiteen in fysieke beveiliging en logische beveiliging. Hier houden we ons slechts bezig met logische beveiliging. Toegangscontrole dient zowel confidentialiteit als integriteit. Het bepaalt uiteindelijk immers wie wat te zien krijgt, en wie wat kan veranderen. Hier gaan

¹¹⁶Aldus ook F. Goosmann in ‘Beveiliging medische gegevens zo lek als een mandje’, *Zorgtelematica Transparant* (4), 1999-3, p. 8; Van Herten 1995, p. 78; Spreeuwenberg 1996, p. 669: “In de praktijk blijken niet-behandelend artsen en mensen die geen arts zijn gemakkelijke toegang tot de gegevens te hebben. Allerlei mogelijkheden die er in theorie bestaan om gegevens te beschermen worden in de praktijk nauwelijks toegepast.”, en in datzelfde artikel over een andere schrijver: “De wijze waarop nu al elektronisch met patiëntengegevens wordt omgegaan, maakt dat hij weinig fiducia heeft in privacy-beschermende maatregelen”.

¹¹⁷Bleumer 1995, p. 16; Castano e.a. 1994, p. ix.

¹¹⁸Beveiliging tegen availability attacks (i.e. avoiding denial of service) komt niet aan de orde.

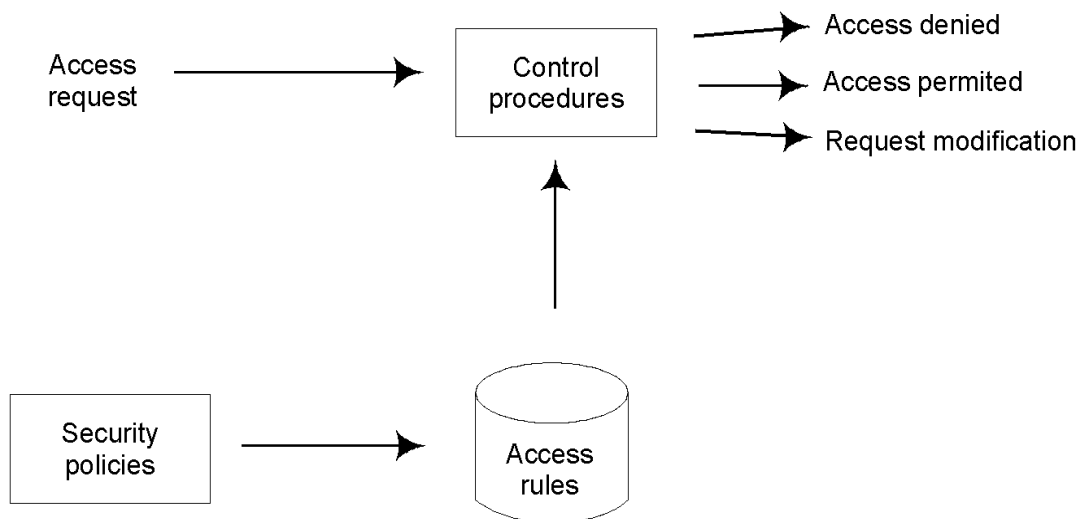
¹¹⁹Volgens Bleumer (1995, p. 15) ISO 7498-2.

¹²⁰RVZ advies Informatietechnologie in de zorg 1996, deel 2, p. 56.

we verder in op authenticatie en access controls. Voor deze beiden wordt ookwel de term autorisatie gebruikt.

Bij authenticatie gaat het erom vast te stellen dat iemand werkelijk degene is die hij of zij beweert te zijn.¹²¹ Dat kan plaatsvinden volgens verschillende methoden. Een methode is gebaseerd op de vaststelling dat iemand iets weet, bijvoorbeeld een password. Een andere methode is gebaseerd op een uniek bezit, zoals een sleutel.¹²² Een derde methode maakt gebruik van een unieke eigenschap, zoals bijvoorbeeld een vingerafdruk. Tenslotte kan men gebruik maken van een methode die verband houdt met een locatie, bijvoorbeeld door gebruik te maken van de terugbelfaciliteit van een inbelmodem.¹²³

Access controls worden als volgt gedefinieerd: “Access controls in information systems are responsible for ensuring that all direct accesses to system objects occur exclusively according to the modes and rules fixed by protection policies. An access control system (figuur 1) includes subjects (users, processes) who access objects (data, programs) through operations (read, write, run). Functionally it consists of two components: 1) a set of access policies and rules: information stored in the system, stating the access modes to be followed by subjects upon access to objects. 2) A set of control procedures (security mechanisms) that check the queries (access requests) against the stated rules (query validation process); queries may then be allowed, denied or modified, filtering out unauthorized data.”¹²⁴



Figuur 2. Access control system.

Toegang tot de opgeslagen gegevens moet voldoen aan de eerder genoemde wettelijke normen en aan de daarna geformuleerde functionaliteits-eisen.. Door het ontwerpen van access rules wordt gepoogd een deel van deze functionaliteit te automatiseren. Access rules sluiten daarom nauw aan op de eerder geformuleerde functionaliteits-eisen. Het zijn vertalingen van eisen naar procedures. Hier wordt het vereiste: ‘behandelrelatie’ toegelicht.

¹²¹RVZ advies Informatietechnologie in de zorg 1996, deel 2, p. 60.

¹²²In de zin van ‘token’ (Registratiekamer rapport Beveiliging persoonsregistraties 1994).

¹²³Committee privacy & security in health care applications 1997, hoofdstuk 4, p. 3.

¹²⁴Castano e.a. 1994, p. 18.

Het is moeilijk automatisch te bepalen of een hulpverlener een behandelrelatie heeft met de patiënt waarvan hij de gegevens opvraagt. Een combinatie van techniek en procedure zou daarvan wel een benadering kunnen geven.

Een systeem waarbij hulpverleners gebruik maken van een zorgprofessionalpas¹²⁵ en waarbij gegevens slechts kunnen worden ingezien wanneer de gebruiker zich met zijn zorgprofessionalpas, in combinatie met bijvoorbeeld een pincode, bij het systeem aanmeldt, biedt bescherming tegen niet-hulpverleners, maar niet tegen nieuwsgierige hulpverleners.¹²⁶

Het voorkomen van dergelijke inzage door deze categorie kan onder andere geschieden door bevoegdheden te splitsen. Een arts kan dan bijvoorbeeld alleen het dossier inzien van patiënten waarmee hij een poliklinische afspraak heeft. Alleen de secretaresse is bevoegd deze afspraken te maken. Deze secretaresse heeft slechts toegang tot de afsprakenmodule van het GEPD en niet tot het dossier. De specialist heeft alleen raadpleeg- en geen wijzigingsbevoegdheid in de afsprakenmodule.

Een ander voorbeeld is het vereiste van dubbele aanvraag tot inzage/verstrekking bij noodgevallen. Slechts wanneer de EHBO verpleegkundige en de arts aanvragen vindt verstrekking plaats. Zo is voorkomen dat de arts toegang heeft tot alle gegevens van alle patiënten in het GEPD.

Daarnaast zou de bevoegdheid van een zaalarts gekoppeld kunnen worden aan de bed bezetting. De arts heeft dienst op een aantal afdelingen, hij heeft slechts inzagebevoegdheid in dossiers van patiënten die op diezelfde afdelingen zijn opgenomen. Een dergelijke koppeling zou ook voor de verpleging gemaakt kunnen worden, zij hebben slechts toegang tot gegevens van patiënten op hun eigen afdeling.

Onerbiedig samengevat zou je kunnen zeggen dat het systeem de feitelijke situatie probeert te benaderen door met behulp van ‘trucjes’ een geautomatiseerd antwoord te verkrijgen op de vraag “is er een behandelrelatie?”. Deze trucjes blijken bij nadere beschouwing steeds aan te sluiten op symptomen van een behandeling. Symptoom van een poliklinische behandeling is een vermelding van die afspraak in het veelal geautomatiseerde afsprakenregister. Symptoom van een spoedeisende behandeling is de gelijktijdige aanwezigheid van patiënt, arts en verpleegkundige op de Eerste Hulp. Symptoom van een behandeling door de zaalarts is bezetting van een bed op de afdeling waar deze arts dienst heeft. Steeds gaat het erom aansluiting te vinden bij gegevens die al wel binnen het systeem bekend zijn, of daaraan eenvoudig kenbaar kunnen worden gemaakt.

Er is een onderscheid te maken tussen werkwijzen die het uitdelen van een bevoegdheden door mensen laten plaatsvinden en werkwijzen waarin deze bevoegdheid door een automatisch proces wordt bepaald. Het geschetste EHBO voorbeeld is een voorbeeld van de eerste werkwijze. De autorisatie van de zaalarts is een illustratie van de tweede werkwijze. Wanneer mensen bevoegdheden kunnen doorgeven of uitdelen wordt dat discretionary access control genoemd.¹²⁷ Voordeel van geautomatiseerde werkwijzen is dat ze minder werk vergen

¹²⁵Doppegieter 1993a, p. 1202.

¹²⁶Wanneer het GEPD een hele regio bestrijkt gaat dat om ontzettend veel gevoelige gegevens van heel veel mensen. Een dergelijke omvangrijke verzameling oefent een grote aantrekkingskracht uit.

¹²⁷Castano e.a. 1994, p. 204.

van hulpverleners en daarom beter aansluiten op de benodigde dynamiek¹²⁸ van autorisaties in GEPD's. De geautomatiseerde werkwijze maakt gebruik van gegevens die toch al in het systeem aanwezig zijn. De hiervoor genoemde poliklinische afspraak uit de geautomatiseerde afsprakenmodule is daar een voorbeeld van.

De hierboven beschreven methoden proberen de vereiste behandelrelatie te onderscheiden. Zoals uit hoofdstuk 5 bleek is een daarop toegesneden verstrekking niet het enige functionaliteitsvereiste. 'Aard van de werkzaamheden' is een ander aspect waarop de verstrekking zich dient te richten. Ik beperk me hier evenwel tot voorbeelden met betrekking tot de behandelrelatie. Het is goed te beseffen dat het GEPD zich niet steeds van dergelijke ietwat kunstmatige symptomen behoeft te bedienen. De aard van de werkzaamheden zou namelijk ook kunnen blijken uit de identiteit van de bij het systeem bekende hulpverlener en de aan deze hulpverlener gekoppelde functie. Of uit de in het systeem genoteerde zorgaanvraag. Daarover later meer in de paragraaf over opslag van informatie.

Hier is het nog belangrijk te constateren dat er, naast het bekend zijn van de functie van de hulpverlener, een mechanisme moet zijn dat de presentatie van gegevens daadwerkelijk op de aard van de werkzaamheden toesnijdt. Dat betekent dat er consensus moet worden bereikt over welke gegevens voor bepaalde werkzaamheden nodig zijn. Het is de vraag of je hier in zijn algemeenheid dingen over kan zeggen. Je loopt immers het risico bepaalde noodzakelijke gegevens niet te laten zien. Dat is een risico van het ontbreken van een menselijke schakel bij pull-informatie. Het effect hiervan probeert men in de praktijk te beperken door terug te grijpen op, in het kader van een eerdere behandeling verzamelde, push-informatie zoals een ontslagbrief van de specialist aan de huisarts. Ondanks de risico's ervan vindt over toegesneden gegevensrepresentatie al het nodige medisch-inhoudelijke overleg plaats. Niet in eerste instantie met de bedoeling om de omvang van privacy inbreuken te beperken, maar om aanwezige informatie behapbaar te maken voor hulpverleners.

6.2 Nadelen van geautomatiseerde toegangscontrole

De eerder beschreven toegangshindernissen zouden een belemmering kunnen vormen voor legitieme inzage. Wanneer een zaalarts wordt geroepen bij een acuut probleem op een andere afdeling omdat zijn collega zaalarts al met een ander spoedgeval bezig is dan moet er toch toegang mogelijk zijn. Dat zou kunnen door bijvoorbeeld de verpleging de bevoegdheid te geven de arts toegang te verlenen¹²⁹, maar dat zou ook kunnen door een noodsituatie voorziening te maken die een hulpverlener toch toegang geeft. De logbestanden van het gebruik van deze faciliteit zouden kritisch bekeken kunnen worden. In sommige systemen moet de hulpverlener deze vorm van toegang verantwoorden door de reden in een speciaal veld in te tikken. Het leeuwendeel van de inzageverzoeken past in de reguliere procedure. Het logbestand van die verzoeken behoeft geen bijzondere aandacht. Het logbestand van de noodsituatie inzagen wèl. Maar doordat het overgrote deel van de inzagen door deze

¹²⁸ Immers behandelingen worden aan de lopende band opgestart, afgebroken en beëindigd, hulpverleners worden constant door andere hulpverleners ingeschakeld voor onderzoeken, poliklinische afspraken veranderen regelmatig enzovoorts.

¹²⁹ Zonder dat ze zelf noodzakelijkerwijs toegang hebben, net zoals bij het voorbeeld met de secretaresse en het poliklinisch spreekuur van de arts.

werkwijze valt te onderscheiden is dat werk (controle logbestand noodsituatie) een stuk uitvoerbaarder geworden.

Hieruit blijkt wederom duidelijk dat privacy bescherming in een GEPD het moet hebben van een combinatie van procedures en technieken. Nadeel van dergelijke combinaties is dat hulpverleners alleen genoeg nemen met een zeer gebruiksvriendelijk systeem. Ze hebben behoefte aan toegankelijkheid en zijn onverdraagzaam ten opzichte van hinderlijke beveiligingsprocedures.¹³⁰ Dat heeft geleid tot systemen waarin alle artsen binnen een instelling toegang hebben tot alle gegevens in alle patiëntendossiers binnen die instelling. Achteraf zou toegang kunnen worden gecontroleerd aan de hand van log files. In het RVZ advies wordt een dergelijke werkwijze gepropageerd.¹³¹ In de praktijk komt echter weinig terecht van controle van de logfiles, laat staan van represailles.

6.3 Opslag van informatie

Wanneer informatie volgens bepaalde normen zal moeten worden ontsloten zal informatie ook op een dusdanige manier moeten worden opgeslagen dat die normen kunnen werken met de informatie. Het systeem zal op de opgeslagen informatie moeten kunnen ‘grijpen’.

Kenmerken van gegevens moeten dus zijn op te maken uit die gegevens zelf, of uit de relaties die die gegevens hebben met andere gegevens of uit meta-informatie. Bepaalde informatie is al in het systeem beschikbaar. Bijvoorbeeld wie de uitvoerder van een bepaald onderzoek is. Soms kan op grond van zulke vastgelegde relaties (inhoud zelf) van het dossier al worden uitgemaakt of er inzage kan plaatsvinden. Soms heeft een geautomatiseerd systeem aan de inhoud van de informatie in het dossier zelf niet voldoende. Wanneer in een anamnese veld voorkomt: “mishandeld door haar nieuwe vriend” dan kan het systeem daar bijvoorbeeld niets mee, er zal meta-informatie moeten worden toegevoegd. Het systeem zal moeten ‘weten’ dat die gegevens informatie met betrekking tot derden bevat. Bij een verstrekings-verzoek door een nieuwe hulpverlener kan die dan automatisch uit de te verstrekken informatie worden gefilterd (request modification, zie figuur 1). Meta informatie kan aan gegevens worden toegevoegd bijvoorbeeld door in een database bepaalde velden te reserveren voor informatie met betrekking tot derden. Andere velden zouden kunnen worden gereserveerd voor uiterst gevoelige informatie enzovoorts. Eigenlijk is dit systeem er op gebaseerd dat gegevens worden onderverdeeld. Zo zou ook informatie kunnen worden toegesneden op de functie van de hulpverlener, of beter nog de rol die hij op dat moment vervult. Informatie die verpleegkundigen mogen inzien bevindt zich in een ander veld dan informatie die artsen mogen inzien.

Er worden echter vraagtekens gezet bij de praktische uitvoerbaarheid van het verdelen van informatie.¹³² Wanneer bij elke rol van een hulpverlener een ander veld zou moeten worden gevuld dan wordt het onderverdelen ondoenlijk, bovendien zou dezelfde informatie op verschillende plekken moeten worden opgeslagen. Dat geeft aanzienlijke kwaliteits risico’s. Er zou gezocht kunnen worden naar een aanvaardbare balans. Verderop in dit hoofdstuk

¹³⁰Barrows Jr. & Clayton 1996, p. 142.

¹³¹RVZ advies Informatietechnologie in de zorg 1996, p. 64.

¹³²Van Herten 1995, p. 78.

wordt een techniek besproken die het mogelijk maakt gegevens los van hun plaats (waarbij het dus niet noodzakelijk is die gegevens in een veld te grouperen) te labelen met meta-informatie.

Op de een of andere manier (inhoud zelf, relaties tussen inhoud of meta informatie) zal van opgeslagen persoonsgegevens in het GEPD duidelijk moeten zijn:

- Tot welke behandelovereenkomst gegevens behoren¹³³
- Voor welke gegevens toestemming tot verstrekken via het GEPD is gegeven
- Welke gegevens uitdrukkelijk alleen een aan bepaalde hulpverlener zijn toevertrouwd (geheim)
- Wat informatie met betrekking tot anderen is
- Wat de leeftijd is van gegevens
- Of er ten opzichte van gegevens bezwaar bestaat tegen gebruik voor wetenschappelijk onderzoek
- Of er ten opzichte van gegevens bezwaar bestaat in verband met het inlichten van de patiënt op initiatief van de patiënt zelf.
- Of er ten opzichte van gegevens bezwaar bestaat in verband met het inlichten van de patiënt op initiatief van de hulpverlener
- Of het persoonlijke werkaantekeningen zijn

Deze kenmerken zijn direct afgeleid van de in hoofdstuk 5 geformuleerde functionaliteitseisen. Daarbij was al opgemerkt dat dat niet de enige eisen zijn die aan een GEPD moeten worden gesteld. In het kader van de opslag van gegevens wil ik nog opmerken dat eveneens van gegevens duidelijk zal moeten zijn:

- Wie of wat de bron¹³⁴ is van gegevens (onderzoek, persoon hulpverlener, patiënt, anderen) en wie ze heeft ingevoerd
- Wat het verloop van de inhoud van gegevens is geweest

Dit vloeit voort uit het vereiste dat men moet kunnen reconstrueren wat er op enig moment aan informatie beschikbaar was. Dat moet kunnen voor zowel voor medisch-inhoudelijke doeleinden als voor aansprakelijkheidsonderzoek. Indirect kunnen deze kenmerken ook van belang zijn voor de eerder geformuleerde eisen. Wanneer de bron van gegevens bijvoorbeeld een hulpverlener is dan heeft deze ten opzichte van die gegevens een speciale verantwoordelijkheid (zorgplicht).

¹³³De bij deze behandelovereenkomst behorende ‘hoofd’ hulpverlener heeft ten aanzien van deze gegevens zoals we hebben gezien namelijk een speciale poortwachters functie.

¹³⁴Dat sluit aan bij het accountability beginsel.

6.4 Labelen

Het toevoegen van meta informatie aan gegevens kan ook met de Extensible Markup Language (XML). Deze metataal is bedoeld om uniforme structuur aan te brengen in de inhoud van een of meerdere documenten.¹³⁵ XML is oorspronkelijk ontwikkeld voor het World Wide Web. De potentie van XML is desalniettemin veel groter. XML wordt toegepast bij EDI, standaardisatie van gegevensuitwisseling¹³⁶, het op afstand aansturen van wetenschappelijke instrumenten¹³⁷, in Elektronische Patiëntendossiers¹³⁸ enzovoorts. XML is voor het web ontwikkeld aangezien HTML (Hypertext Markup Language) te kort schiet. HTML is een layout omgeving geworden, het geeft van informatie voornamelijk aan hoe die er uit moet zien. Dat is nooit de bedoeling geweest.¹³⁹ XML voorziet in de functionaliteit die HTML mist. Het is een oplossing voor het verspreiden van inhoud op het web met als basis “de scheiding van inhoud, definitie en bereiken van flexibiliteit”.¹⁴⁰ XML brengt een scheiding aan tussen inhoud en vorm. De splitsing van definitie (het meta-deel) en de inhoud wordt bereikt door het gebruik van een Document Type Definition (DTD) waarin op meta-niveau de inhoud van een document, de elementen (beter bekend als TAG's) en haar eigenschappen (attributen) beschreven staan. XML onderscheidt zich op dit punt van HTML. In HTML kan een gebruiker geen eigen tags definiëren. In XML is dit een van de krachten en biedt daarmee veel flexibiliteit zodat geheel eigen documentenstructuren gemaakt kunnen worden. Het is tenslotte bedoeld voor tool en leverancier onafhankelijke overdracht van gegevens met behulp van open Internet-standaarden. XML heeft de volgende eigenschappen:

- Strikte scheiding van structuur (DTD), presentatie en inhoud (tekstdocument)
- Gestructureerde toegang tot informatie
- Enkelvoudige bron en meervoudige presentatie mogelijk
- Kwaliteitscontrole (door parser¹⁴¹)

Belangrijke winstpunten zijn dan ook dat hergebruik van gegevens in meerdere presentaties leidt tot minder meervoudige opslag van gegevens in een document. En dat hard- en software onafhankelijke gegevensvastlegging en presentatie plaats kan vinden.

Van de problemen met HTML en zijn implementaties is geleerd om naast XML diverse andere standaarden te definiëren die bijdragen aan goed gebruik: de eXtensible Stylesheet Language (XSL) en Document Object Model (DOM). Een XML document en XSL specificaties leiden tot een document dat door meerdere devices begrepen wordt. Het DOM-

¹³⁵Weegenaar 1999.

¹³⁶Weegenaar 1999.

¹³⁷Bosak & Boray 1999.

¹³⁸T. Smit, ‘Nederlands ziekenhuis begint proef met Duits EPD’ *Automatisering Gids* 22 oktober 1999.

¹³⁹Weegenaar 1999.

¹⁴⁰Weegenaar 1999.

¹⁴¹Een parser is een programma dat (uit het XML-document) een document genereert dat geschikt is voor het apparaat waar de parser op draait, voor opmaakdoeleinden betekend dat aangepast naar schermgrootte, resolutie, kleurdiepte en enzovoort.

model biedt daarnaast mogelijkheden met deze documenten zeer geavanceerde toepassingen te maken. Wanneer verwerking van XML documenten plaatsvindt met de DOM standaard (Document Object Model) dan wordt het voor programma's mogelijk om een XML document te interpreteren en te verwerken. DOM definieert de brug tussen de structuur en de inhoud van het document en het verwerken hiervan naar vele toepassingen. Middels XSL wordt de inhoud (XML document) gescheiden van de presentatie (XSL document).

XML beschikt over een aantal eigenschappen die waardevol kunnen zijn voor het GEPD. Het zou te ver voeren om hier op alle mogelijkheden en technische achtergronden in te gaan. Globaal kan echter worden opgemerkt dat het een open standaard is die voor GEPD doeleinden kan worden aangepast. XML tags zouden gebruikt kunnen worden om informatie te labelen. Voor de ondersteuning van privacybeschermende maatregelen (zie de paragraaf over opslag van gegevens) zou dat kunnen betekenen het merken van informatie als 'extra gevoelig', 'informatie met betrekking tot anderen', 'therapeutische exceptie' enzovoorts. Informatie hoeft dan niet meer persé ingedeeld te worden in database velden. Ook een stuk vrije tekst kan van labels worden voorzien. Informatie kan zo zelfs op gegevensniveau worden gelabeld. Meerdere kenmerken kunnen op dezelfde inhoud worden geplakt.¹⁴² Dezelfde bron kan op verschillende manieren worden gerepresenteerd. Je zou je kunnen voorstellen dat gegevens uit het dossier voor een fysiotherapeut op een andere wijze wordt gepresenteerd dan voor een psychiater. Geautomatiseerde delen in het GEPD zou dan op basis van met behulp van XML toegevoegde meta-informatie kunnen filteren, en zo gericht kunnen verstrekken.

XML is daarnaast flexibel genoeg om gegevensuitwisseling tussen verschillende databases en systemen mogelijk te maken. Over het gemeenschappelijke XML formaat (standaardisatie) dienen dan wel afspraken te worden gemaakt. Of gegevensuitwisseling tussen verschillende systemen noodzakelijk is hangt af van de architectuur van het GEPD. In het volgende hoofdstuk wordt daar bij stilgestaan.

6.5 PET

Privacybescherming in GEPD's wordt vaak in een adem genoemd met PET (Privacy Enhancing Technology). In deze paragraaf leg ik uit dat deze techniek voor ons probleem (hoe sluit verstrekking zoveel mogelijk aan bij 'the need to know') geen specifieke waarde heeft.

De koppeling van gegevens aan de werkelijke identiteit van een persoon is in de meeste gevallen slechts voor een zeer beperkt gedeelte van een informatiesysteem noodzakelijk. Beveiliging die uitgaat van het scheiden van werkelijke identiteit van de rest van gegevens wordt aangeduid met PET. Een belangrijk concept binnen PET is de 'identity protector (IP)'. De IP kan de werkelijke identiteit van een gebruiker omzetten in een pseudo-identiteit. De IP kan ingeschakeld worden tussen dat deel van het systeem waarin de ware identiteit bekend is en de rest van het systeem waarin de gebruiker onder een pseudo-identiteit, te vergelijken met een pseudoniem, bekend is.¹⁴³ Hoewel de werkelijke identiteit van een patiënt niet voor elke bij de behandeling betrokken hulpverlener bekend hoeft te zijn (zo kan een bloedbepaling

¹⁴²Door middel van geneste tags.

¹⁴³RVZ advies Informatietechnologie in de zorg 1996, deel 2, p. 62.

geschieden zonder dat de laborant op de hoogte is van de naam van de patiënt)¹⁴⁴, heeft PET in combinatie met versleuteling vooral voordelen in het systeem zelf. Het biedt bescherming tegen gevaren als bijvoorbeeld het buiten programma's om -op file-niveau- bekluren van data, door kwaadwillende outsiders maar ook bijvoorbeeld door nieuwsgierige systeembeheerders. Voor ons probleem is PET minder waardevol, immers voor bij de behandeling betrokken hulpverleners zullen identificerende en andere gegevens bij elkaar moeten komen.

6.6 Samenvatting

De voor toegangscontrole benodigde toegangs regels moeten aansluiten bij de in het vorige hoofdstuk geformuleerde functionaliteits eisen. Wanneer geautomatiseerde systemen moeten constateren of er aan vereisten voldaan is dan zal dit moeten aansluiten op informatie die ofwel reeds in het systeem aanwezig is, ofwel daar wordt ingestopt. Men kan daarvoor proberen aansluiting te zoeken bij symptomen of sporen van een vereiste. In dit hoofdstuk is dat geschetst aan de hand van de vereiste behandelrelatie. Een ander voorbeeld van een functionaliteits vereiste is het toesnijden van verstrekking op de aard van de werkzaamheden. Dat brengt risico's met zich mee. Dat is namelijk een medisch inhoudelijke aangelegenheid en dus maar beperkt automatiseerbaar. Toch vindt er met dat doel al het nodige overleg plaats tussen medici. Nadeel van geautomatiseerde toegangscontrole is de mogelijke belemmering van legitieme inzage. Deze belemmering kan worden beperkt door het inbouwen van een 'noodingang' maar deze vormt dan wel de achilleshiel van het systeem. Controle van het gebruik van deze voorziening zou een preventief effect kunnen hebben. Hieruit bleek weer dat privacybescherming moet worden bereikt door combinatie van procedures en technieken. Artsen zijn nogal intolerant ten opzichte van dergelijke zichtbare 'hindernissen'. Ik denk echter dat de hierbij voor de hulpverleners opgeworpen beperkingen aanvaardbaar zijn. Zij zijn gezien de risico's die er aan GEPD gebruik -zonder dergelijke maatregelen- zouden kleven in ieder geval onvermijdelijk. Een systeem waarin hulpverleners toegang tot alle gegevens in het GEPD hebben is onaanvaardbaar en in strijd met het medisch beroepsgeheim. Om geautomatiseerde toegangsprocessen met gegevens te kunnen laten werken zullen kenmerken van gegevens moeten kunnen worden afgeleid uit hun inhoud, hun relatie met andere gegevens of uit meta-informatie. Dat bleek in de paragraaf over opslag van gegevens. Meta-informatie kan worden toegevoegd met behulp van XML, dat door zijn flexibiliteit verschillende voordelen biedt, waaronder de mogelijkheid gegevens een keer op te slaan en op verschillende manieren te presenteren. In de laatste paragraaf bleek PET voor ons specifiek probleem geen aanvullende waarde te hebben.

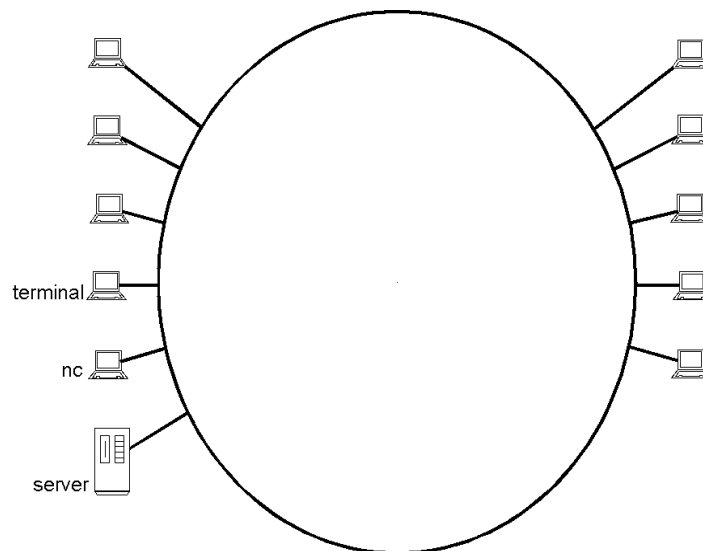
¹⁴⁴Een dergelijke werkwijze sluit wellicht niet goed aan op het menselijk denkpatroon (Van Lomwel & Van Veen 1996, p. 70).

7. Architectuur

In dit hoofdstuk worden de hoofdvarianten in de netwerk architectuur van een GEPD beschreven. Daarnaast is aangegeven wat de voorkeur is van beleidsbepalers. Enkele voor- en nadelen van de onderscheiden varianten met betrekking tot de toegankelijkheid van gegevens worden kort besproken.

7.1 Centrale GEPD variant

In het ontwerp van een EPD zijn zo gezegd twee varianten te onderscheiden. De eerste variant is het centrale type waarbij instellingen gebruik maken gebruik maken van een centrale databank¹⁴⁵ waarin gegevens over patiënten worden bijgehouden. Je zou dit kunnen zien als een groot ziekenhuis informatiesysteem (ZIS) met EPD functie, dat nu niet alleen gebruikt wordt door hulpverleners binnen de instellingmuren, maar ook door hulpverleners daarbuiten zoals: huisartsen, fysiotherapeuten en wijkverpleegkundigen.



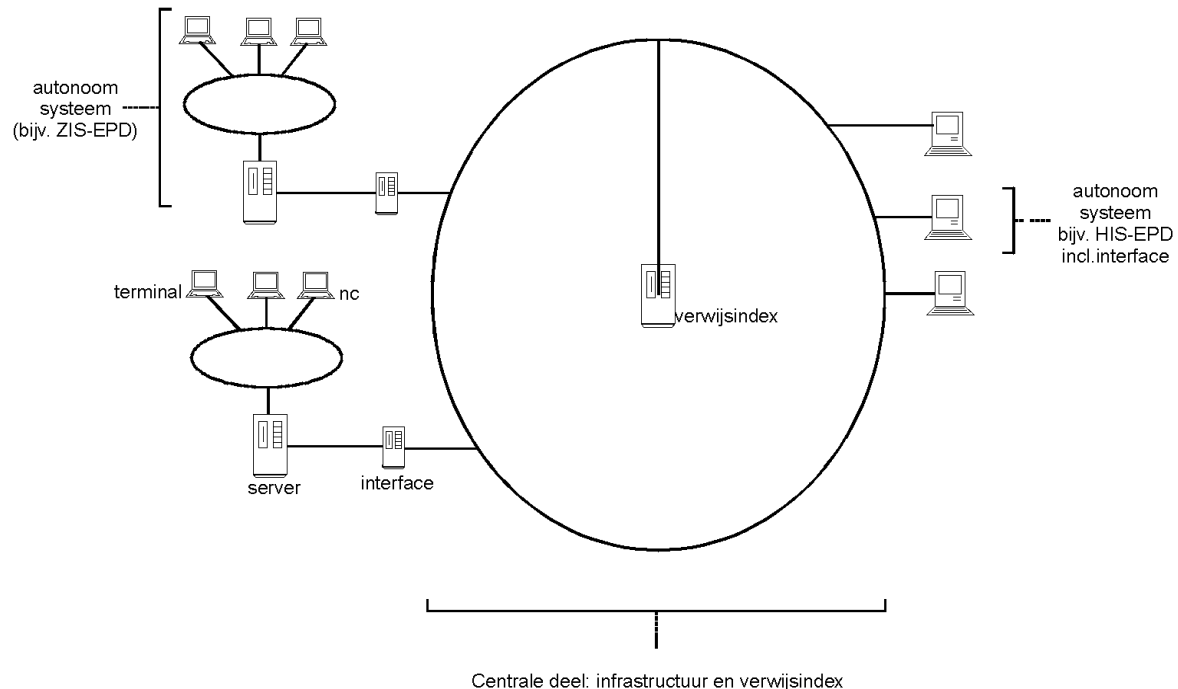
Figuur 3. Centrale variant GEPD

De apparatuur die door de hulpverlener wordt gebruikt is een terminal, een pc of een netwerk computer (nc). De ene terminal staat bij bijvoorbeeld bij een huisarts en de andere in de werkkamer van een cardioloog. De centrale database resideert in dit schema op de server.

¹⁴⁵Gegevens behoeven daarvoor niet fysiek op eenzelfde plaats te worden opgeslagen, met centraal wordt bedoeld: functioneel centraal.

7.2 Decentrale GEPD variant

De tweede variant is het decentrale type waarbij bestaande automatiseringssystemen binnen instellingen autonoom blijven bestaan en waarbij informatie uitwisseling desgevraagd plaatsvindt via een nieuwe infrastructuur.



Figuur 4. Decentrale variant GEPD

Bestaande autonome automatiseringssystemen kunnen in deze variant ziekenhuisbrede EPD's zijn, maar ook EPD-systemen van een maatschap of enkele hulpverlener. Een Huisarts Informatie Systeem (HIS) is een voorbeeld van een EPD van een enkele hulpverlener. Een Ziekenhuis Informatie Systeem (ZIS) is een voorbeeld van een ziekenhuisbreed EPD. Decentrale systemen maken meestal gebruik van een verwijfsindex. In deze index staat aangegeven waar informatie over een patiënt aanwezig is. In deze variant vindt veel uitwisseling plaats van gegevens tussen verschillende systemen. Het formaat van de gegevens zal daarom moeten zijn gestandaardiseerd. De interface verzorgt de vertaalslag van deze standaard naar het autonome systeem en omgekeerd.

7.3 Centraal of decentraal, voor en nadelen

De Raad voor de Volksgezondheid en Zorg staat een decentrale variant van het EPD voor: een verzameling van door verschillende zorgverleners bijgehouden deeldossiers, die via de elektronische snelweg in samenhang geraadpleegd kan worden.¹⁴⁶ De voorkeur van beleidsbepalende professionals op GEPD gebied tendeert naar de decentrale variant.

¹⁴⁶RVZ advies Informatietechnologie in de zorg 1996, deel 1, p. 16.

Opvallend maar voorspelbaar is dat informatici zoals van Hee meer zien in de centrale variant.¹⁴⁷ Pleitbezorgers van privacy kiezen meestal voor de decentrale variant.

Hieronder worden enkele voor- en nadelen van zowel de decentrale als de centrale variant besproken. Achterliggende gedachte bij het formuleren van deze voor- en nadelen is steeds privacybescherming en niet bijvoorbeeld de automatiseringstechnische haalbaarheid. Waar mogelijk vindt terugkoppeling plaats naar de geformuleerde vereisten.

Voordeel van de decentrale variant is in ieder geval dat bestaande systemen blijven bestaan. Aangeschafte hard- en software behoudt zijn functie, en gebruikers blijven de systemen gebruiken waarmee ze bekend zijn. Gegevens over patiënten zijn verspreid opgeslagen. Het is niet zo dat op een plaats alle gegevens van alle patiënten bekend zijn. Dat is wat privacybescherming betreft een voordeel, hoewel inzage in alle andere gegevens wel kan plaatsvinden via het GEPD is wijzigingsbevoegdheid voorbehouden aan de autonome systemen. Dat betekent in ieder geval dat degene die informatie wil wijzigen zich moet voordoen als legitieme gebruiker van het systeem waarin die informatie voorkomt. Hij zal zich niet in een keer wijzigingsbevoegdheid tot alle informatie over een persoon kunnen verschaffen. In een centraal GEPD zou dat wel mogelijk zijn. Kwaadaardige inbreuk zou ontzettend veel medische gegevens over ontzettend veel mensen in gevaar brengen. Het gevaar is dan niet alleen inzage van die gegevens, maar ook wijziging ervan. Toch biedt deze centrale variant meer mogelijkheden om gebruikers in hun diversiteit te herkennen. Alle gebruikers van het GEPD zijn hier overal in het systeem bekend, ook gegevens over bijvoorbeeld functie en rol. Gegevens waarbij aansluiting kan worden gezocht bij het bepalen of er sprake is van een behandelrelatie (symptomen of sporen) zijn ook overal in het systeem voor het systeem voor handen. Dat is niet het geval in het decentrale systeem. Daar moet het autonome systeem er van uit gaan dat de verzoeken om informatie die via het centrale deel van het GEPD bij hem binnenkomen legitiem zijn. Het systeem weet verder niks van de aanvrager. Wanneer het autonome systeem de aangevraagde gegevens via de interface het centrale deel van de infrastructuur opstuurt is het de grip erop kwijt. Verder moet de toegang in de autonome systemen voldoen aan de functionaliteitseisen uit hoofdstuk 5. Dat is in bestaande systemen echter nauwelijks het geval. Het gevaar hiervan is dat iedereen die zich bij in een autonoom systeem kan voordoen als een hulpverlener toegang krijgt tot alle gegevens van alle patiënten bij andere hulpverleners. Wanneer informatie via de infrastructuur wordt verstrekt aan andere systemen dan kan dezelfde informatie op meerdere plekken voorkomen. Een labuitslag staat dan bijvoorbeeld zowel in de ontslagbrief aan de huisarts als in het systeem van het lab. Een centraal GEPD biedt mogelijkheden dat te voorkomen. Een vermelding van een labuitslag in een huisartsenbrief kan daar worden bewerkstelligd door een verwijzing naar de bron. In een decentraal GEPD kan de huisarts slechts een kopie de gegevens worden verstuurd. Dat heeft risico's. Wanneer verzocht wordt om vernietiging en verbetering kunnen dan bijvoorbeeld wel alle kopieën van die informatie worden vernietigd of verbeterd?

Pleitbezorgers van privacy vertonen een welhaast natuurlijke voorkeur voor decentrale systemen, opvallend is dat informatici van nature een voorkeur voor centrale systemen lijken te hebben. Opvallend is ook dat wanneer er met de integriteit van gegevens grote sommen geld op het spel staan, bijvoorbeeld bij banken, er altijd gekozen wordt voor centrale zwaar beveiligde systemen.

¹⁴⁷Y. de Koster 1999, p. 20. Van Hee bedoelt niet dat alle gegevens van alle patiënten op één plaats moeten staan maar dat alle gegevens van één patiënt op dezelfde plaats komen te staan: functioneel centraal.

Zo bezien wordt de keuze voor de decentrale variant uit privacy beschermingsoogpunt steeds minder vanzelfsprekend. Maar het is moeilijk iets in zijn algemeenheid te zeggen over de aanvaardbaarheid van de centrale of decentrale variant. Want het uiteindelijke beschermingsniveau wordt toch bepaald door de combinatie van procedures en technieken. Zo wordt de decentrale variant in de visie van de Raad beveiligd doordat de zorgverlener toegang krijgt tot een verwijsindex op een chipkaart (zorgpas) van de patiënt. Het EPD staat niet op de chipcard¹⁴⁸, maar de chipcard vormt de sleutel tot elders opgeslagen informatie.¹⁴⁹ De minister onderschrijft deze visie. De voorkeur van de minister voor de decentrale variant kan niet los gezien worden van de combinatie met de chipcard. De minister beschouwt ze als complementair en elkaar versterkend.¹⁵⁰ De verwijsindex hoeft niet noodzakelijkerwijs op een chipcard te staan. De index kan ook zijn opgenomen in het 'infrastructuur deel' van het decentrale EPD en fysiek resideren bij bijvoorbeeld de huisarts.¹⁵¹

Nadeel van de chipcard als drager van de verwijsindex is het risico van vergeten, verlies of defect (hoewel een backup van de index bij de huisarts zou kunnen worden gemaakt), verder moet de chipcard aanwezig zijn op het moment dat de hulpverlener wil weten waar informatie aanwezig is (onmogelijk wanneer de patiënt en de chipcard onderweg zijn in een ambulance).

Nadeel van de chipcard als toegangssleutel tot aanwezige informatie is wederom het risico van vergeten, verlies of defect. Hoewel de patiënt met de chipcard voor een bepaalde periode toestemming kan geven¹⁵² lost dit in andere situaties, bijvoorbeeld acute, het gemis van de kaart niet op.

¹⁴⁸Aan het gebruik van de chipcard als drager van het EPD kleven diverse bezwaren. Zowel de RVZ (RVZ advies Informatietechnologie in de zorg 1996, deel 2, p. 82), de minister (*Kamerstukken II 1997/98*, 25 669, nr. 2, p. 8) als de Registratiekamer (Registratiekamer advies Medische zorgpas 1995) wijzen het gebruik van de chipcard als medisch zakdossier af. "De chipcard als medisch zakdossier laten fungeren is een gedachte die inmiddels niet meer als zinvol wordt ervaren. Het medisch beroepsgeheim kan in gedrang komen en medische gegevens zijn teveel muteerbaar, waardoor het dossier niet meer betrouwbaar is." (Ter Linden 1999, p. 163).

¹⁴⁹Dergelijke chipcard toepassingen staan niet op zich, maar maken onderdeel uit van het gehele informatieproces (RVZ advies Informatietechnologie in de zorg 1996, deel 2, p. 33).

¹⁵⁰*Kamerstukken II 1997/98*, 25 669, nr. 2, p. 4.

¹⁵¹Van Herten noemt echter het voorstel om de huisarts de centrale spil te laten zijn bij het verlenen van toestemming aan derden om medische gegevens in te zien onvoldoende doordacht: "Afgezien van de vraag of de huisarts in die positie zou willen verkeren, moeten er waarborgen zijn dat hij inderdaad op de hoogte is van de actuele stand van zaken met betrekking tot datgene zich in de verzameling bevindt. En dat is in de praktijk niet doenlijk. De huisarts wordt in deze visie gezien als de coördinator van de patiëntenzorg, iets dat hij niet altijd, en zo ja, dan ook nog maar vaak ten dele is." (Van Herten 1995, p.78). Uit de opmerking dat de huisarts op de hoogte moet zijn van de actuele stand van zaken kan men concluderen dat er inhoudelijke bemoeienis wordt verondersteld bij het (voorbereiden van) verstrekken van gegevens.

¹⁵²Dit zou tegemoet komen aan het door Nouwt genoemde praktische bezwaar dat een arts bij afwezigheid van de patiënt (en daarmee de chipcard) niet nog eens de gegevens kan bestuderen om te kijken of hij met zijn diagnose in de goede richting zit (M. Schenderling, 'Over nieuwe technologie en privacywetgeving', *Zorgtelematica Transparant* (4), 1999-1, p. 10-11.). Zo behoudt een behandelend arts zijn toegangsmogelijkheid gedurende opname. Het opent echter een nieuwe mogelijkheid - met weer eigen risico's - tot toegang, toegang is immers op enig moment mogelijk zonder chipkaart.

7.4 Samenvatting

De decentrale variant lijkt de voorkeur te hebben van beleidsbepalende professionals en pleitbezorgers van privacybescherming. Bij een nadere beschouwing van de voor en nadelen blijkt dat uit privacybeschermings oogpunt niet vanzelfsprekend. Dat de uiteindelijke bescherming moet worden gezocht in de combinatie van procedures en technieken blijkt ook hier weer. De minister noemt haar voorkeur voor de decentrale variant slechts in een adem met chipcard gebruik.

8. Conclusie

Regelmatig beklagt men zich over het abstracte karakter van privacywetgeving. Ondanks de constatering dat het systeem van de WGBO met name is toegesneden op gerichte verstrekkingen op initiatief van de hoofdhulpverlener blijken de bepalingen in WBP en WGBO een aantal duidelijke eisen te stellen aan de toegang tot medische persoonsgegevens.

Wanneer wetgeving voor het formuleren van de voorwaarden waaronder hulpverleners informatie mogen pakken onvoldoende aanknopingspunten biedt kan worden teruggegrepen op het need to know beginsel. Heeft de hulpverlener de gegevens nodig voor een adequate uitvoering van zijn taak? Het antwoord op die vraag blijkt aan de basis te liggen van alle legitieme verstrekkingen. Verschillende uit wet- en regelgeving voortvloeiende vereisten zijn er dan ook op terug te voeren.

Het blijkt gedeeltelijk mogelijk om op geautomatiseerde wijze te bepalen of er aan de verschillende vereisten voor verstrekking is voldaan. Hierbij wordt gebruik gemaakt van in het systeem bekende symptomen of sporen van vereisten. Privacybescherming kan worden bereikt door van verschillende van deze mogelijkheden gebruik te maken.

Daarnaast kunnen verschillende procedures en juridische constructies bijdragen aan privacybescherming. Het uiteindelijk niveau van privacybescherming dient te worden beoordeeld aan de hand van de combinatie van deze technieken, constructies en procedures.

Pas wanneer een totaaloverzicht van deze combinatie en de werking van het GEPD is verkregen kan een antwoord worden gegeven op de vraag of de hulpverlener aan zijn zorgplicht uit het eerste lid van artikel 457 WGBO heeft voldaan. Slechts wanneer hij aan die zorgplicht heeft voldaan zal hij medische persoonsgegevens in een systeem op mogen nemen.

De hulpverlener en patiënt zullen bij het klaarzetten van gegevens moeten anticiperen op toekomstig gebruik van gegevens door andere hulpverleners, in andere behandelsituaties. De patiënt kan dat doen door aan te geven welke gegevens hij te gevoelig vindt voor gebruik in het GEPD (waar hulpverleners beschikbare informatie zonder tussenkomst van hun huidige hoofdbehandelaar kunnen pakken), waarna de hulpverlener deze als zodanig merkt. De hulpverlener kan anticiperen door aan te geven welke gegevens vallen onder ‘niet geïnformeerd willen worden’, ‘therapeutische exceptie’ enzovoorts. Verder zal de hulpverlener medisch-inhoudelijke voorzorgen moeten nemen zodat de gegevens ook in toekomstige behandelsituaties op hun waarde kunnen worden geschat. Het GEPD zal daartoe mogelijkheden moeten bieden.

De WGBO legt bij de contractspartij-hulpverlener een speciale verantwoordelijkheid. Deze hulpverlener wordt in het systeem der wet gezien als coördinator. Coördinator van zorg, maar ook als coördinator van gegevensverstrekking. Hij vervult een poortwachtersfunctie. Hier kan bij bevoegdheidsverdeling op worden aangesloten. De hoofdhulpverlener zou een selectie kunnen maken van de in het GEPD aanwezige gegevens. Deze ‘werkset’ van gegevens zou de basis kunnen vormen voor verder toegesneden gegevensverstrekking aan direct bij de behandeling betrokkenen.

Om ook in onduidelijke gevallen, zoals transmurale zorg op maat, aansluiting te vinden bij deze speciale verantwoordelijkheid dient voor elke behandelingsovereenkomst een zorgverlener uitdrukkelijk als hoofdhulpverlener bekend te zijn. Van elke behandeling zal duidelijk moeten uit welke behandelingsovereenkomst hij voortvloeit.

Naast het pakken van informatie zal er steeds behoefte blijven bestaan aan gerichte verstrekkingen op initiatief van een hulpverlener in verband met een door deze hulpverlener gestelde zorgvraag. Zoals bleek heeft deze menselijke schakel niet alleen een privacybeschermende- maar ook een zorginhoudelijke functie. Het GEPD zal tot deze gerichte verstrekkingen mogelijkheden moeten bieden.

Een dergelijke functionaliteit kan leiden tot het meerdere malen voorkomen van representaties van dezelfde gegevens. Slechts in een centraal GEPD bleek het mogelijk dergelijke kopieën te voorkomen.

Over de uitwisseling van gegevens tussen verschillende systemen in een decentraal GEPD zullen afspraken gemaakt moeten worden. Bijvoorbeeld over het formaat waarin berichten worden verstuurd. Wanneer systemen gebruik moeten kunnen maken van elkaars gegevens zal er standaardisatie plaats moeten vinden. Binnen die standaardisatie zal er ook plaats moeten worden gemaakt voor privacy-gerelateerde kenmerken van gegevens.

XML biedt verschillende mogelijkheden voor het aanbrengen van deze privacy-gerelateerde kenmerken van gegevens. De functionaliteit van XML is echter veel groter. Haar flexibiliteit past goed bij de gegevensuitwisseling tussen verschillende systemen in een decentraal GEPD. Bovendien biedt het mogelijkheden dezelfde bron op verschillende manieren te presenteren. Er zou begonnen moeten worden met het ontwikkelen van een XML-dialect voor de uitwisseling van medische gegevens. Daarvoor is intensief overleg nodig tussen zorgverleners onderling.

Het Coördinatiepunt Standaardisatie Informatievoorziening Zorgsector houdt zich bezig met standaardisatie van zorginformatie. Bij deze standaardisatie zullen de uit de wet en regelgeving voortvloeiende eerder geformuleerde vereisten moeten worden meegenomen. Wanneer gegevens worden opgeslagen zonder deze privacy-gerelateerde kenmerken dan kan dat in de weg staan aan toekomstige verstrekking van gegevens via een GEPD. Wanneer een hulpverlener informatie wil pakken dan zal het GEPD naast een geautomatiseerde filtermogelijkheid immers toch ook aan gegevens moeten kunnen zien dat het informatie met betrekking tot anderen bevat. Privacy-gerelateerde kenmerken van gegevens dienen dus van meet af aan mee opgeslagen te worden.

Dergelijk overleg vergt investering. Investering in tijd en geld. De implementatie van de in deze scriptie beschreven procedures en technieken vereist eveneens een investering. Tot nog toe bleven deze investeringen uit. De bijzondere privacyrisico's van GEPD's zijn vele malen onderkend. Dat heeft nauwelijks geleid tot concrete resultaten. Concrete resultaten zijn er wel op alle andere gebieden van het GEPD. Daar is wèl het nodige in geïnvesteerd. Verschillende (semi-)GEPD systemen functioneren in de praktijk. Zonder te voldoen aan de geformuleerde vereisten en meestal zelfs zonder er in zekere mate aan tegemoet te komen. In het doelmatigheidsdenken wordt privacy vaak als een last gezien, dat komt omdat het

beperkingen stelt aan het gebruik van informatie en dus aan technische functionaliteit. Niet het feitelijk mogelijke maar de normering door het positieve recht behoort de handelingspraktijk te bepalen. Maar het is natuurlijk vervelend allerlei handige technische mogelijkheden onbenut te moeten laten. In de praktijk gebeurt dat dan ook niet. Wanneer de benodigde beveiligingsmaatregelen aanzienlijke investering vergen, of voor hulpverleners hindernissen opwerpen wordt meestal gewoon besloten het GEPD zonder deze beschermingsmaatregelen in gebruik te nemen. Men zou echter ook eens kunnen besluiten de mogelijkheden van het GEPD te beperken. Misschien moet men eens wat minder hard van stapel lopen en meer aansluiting zoeken bij de huidige werkwijze. Wellicht is dan zo'n gescand EPD zo gek nog niet. Maar men zou natuurlijk ook gewoon eens kunnen gaan investeren in privacy. Deze wordt nu steeds opgeofferd aan toegankelijkheid.

Wanneer investeringen uitblijven wordt het tijd dat er iemand aan de bel trekt, of aan de noodrem.

Barrows Jr. & Clayton 1996

R.C. Barrows Jr. & P.D. Clayton, 'Privacy, confidentiality, and electronic medical records', *JAMIA* (3) 1996-2, p. 139-148.

Beljaars 1994

A.J.J.M. Beljaars, 'Beroepsgeheim: het omgaan met medische gegevens', *Medisch Contact* (49) 1994-22, p.746-748.

Berg e.a. 1998

M. Berg e.a., *De nacht schreef rood*, Den Haag: Rathenau Instituut, 1998. ISBN 90 346 3642 9.

Bleumer 1995

G. Bleumer, *Introduction to the SEISMED Guidelines* (rapport), Hildesheim: Universität Hildesheim 1995.

Bookelman 1996

H. Bookelman, 'De toegankelijkheid van laboratoriumuitslagen. Een complexe zaak', *Medisch Contact* (51) 1996-20, p.685-686.

Bosak & Bray 1999

J. Bosak & T. Bray, 'XML and the second-generation web', *Scientific American* 1999-5 (<http://www.sciam.com/1999/0599issue/0599bosak.html>)(6 december 1999).

Castano e.a. 1994

S. Castano e.a., *Database security*, Amsterdam: Addison-Wesley 1994. ISBN 0 201 59375 0.

Committee privacy & security in health care applications 1997

Committee on maintaining privacy and security in health care applications of the national information infrastructure, *For the record: protecting electronic health information*, (prepublication copy), Washington D.C.: National Academy Press 1997.

Doppegieter 1989

R.M.S. Doppegieter, 'Patiëntendossiers en de Wet persoonsregistraties. Consequenties voor individuele artsen en instellingen van gezondheidszorg', *Medisch Contact* (44) 1989-42, p.1379-1383.

Doppegieter 1990

R.M.S. Doppegieter, 'Persoonsregistratie en de rechten van de patiënt', *Medisch Contact* (45) 1990-39, p.1149-1151.

Doppegieter 1991

R.M.S. Doppegieter, 'De meest gestelde vragen over de Wet Persoonsregistraties. Een inventarisatie', *Medisch Contact* (46) 1991-46, p. 1383-1386.

Doppegieter 1993a

R.M.S. Doppegieter, 'Chipcards in de zorg. Zorgpas en privacy', *Medisch Contact* (48) 1993-39, p.1199-1202.

Doppegieter 1993b

R.M.S. Doppegieter, 'Regelgeving aangaande informationele en ruimtelijke privacy', *Nederlands Tijdschrift voor Geneeskunde* 1993-10, p. 509-514.

Doppegieter 1994

R.M.S. Doppegieter, 'Het geheim van de minderjarige patiënt. Moet de arts de ouders inlichten?', *Medisch Contact* (49) 1994-16, p. 538-541.

Doppegieter 1995a

R.M.S. Doppegieter, 'Vraagstukken rond het dossier en de uitwisseling van gegevens', in: J.Legemaate, *De WGBO: van tekst naar toepassing*, Houten/Diegem: Bohn Stafleu Van Loghum 1995, p. 62-76.

Doppegieter 1995b

R.M.S. Doppegieter, 'WGBO: een aantal vragen over de uitvoeringspraktijk rond het dossier.', *Medisch Contact* (50) 1995-40, p. 1268-1270.

Doppegieter & Rijkssen 1993

R.M.S. Doppegieter & W.P. Rijkssen, 'Het opnemen van gevoelige gegevens in patiëntendossiers', *Medisch Contact* (48) 1993-41, p.1274-1276.

Gardeniers 1995

H. Gardeniers, *Chipcards en privacy. Regels voor een nieuw kaartspel*, Rijswijk: Registratiekamer 1995. ISBN 90 346 3223 7.

Gevers 1990

J.K.M. Gevers 'Het recht op privacy en het beroepsgeheim', in: J.H. Hubben (red.), *De geneeskundige behandelingsovereenkomst. Tekst en analyse van het wetsvoorstel*, Lochem: de Tijdstroom 1990, p. 33-45.

Gevers 1994

J.K.M. Gevers, 'De WGBO. De wetgever en de rechten van de patiënt', *Medisch Contact* (49) 1994-22, p.741-742.

Gevers 1999

J.K.M. Gevers, 'Nieuwe privacywetgeving en de gezondheidszorg', *Sociaal Recht* 1999-3, p. 64-70.

Helmer 1994

F.M.M. Helmer, 'Patiëntenrechten in de praktijk. Het belang van centrale coördinatie bij de effectuering van direct toepasbare patiëntrechten in een ziekenhuis', *Medisch Contact* (49) 1994-18, p. 614-616.

Van Herten 1995

J.H.S. van Herten, *Medisch Beroepsgeheim*, Nijmegen: Van Herten Stichting, 1995.

Holleman e.a. (Artikelgewijs commentaar WBP 1240)

A. Holleman e.a., 'Artikelgewijs commentaar wet bescherming persoonsgegevens', in: A. Holleman (red.), *Handboek bescherming persoonsgegevens* (losbl.), Alphen aan den Rijn: Samsom 1998

Holvast 1998

J. Holvast, 'Wet bescherming persoonsgegevens: overzicht en stappenplan', *Privacy & informatie* (1) 1998-1, p. 4-10.

Hooghiemstra 1998

T.F.M. Hooghiemstra, *Privacy & managed care*, Den Haag: Registratiekamer 1998.

Hooghiemstra 1999

T.F.M. Hooghiemstra, 'De WBP en de gezondheidszorg', *Tijdschrift voor Gezondheidsrecht* 1999-1, p. 17-27.

Hulst & Kerff 1998

E.H. Hulst & R. Kerff, 'Patiëntenrechten en transmurale zorg: wie is verantwoordelijk jegens de patiënt?', *Tijdschrift voor Gezondheidsrecht* 1998-8, p. 485-500.

Hustinx 1993

P.J. Hustinx, *Wet persoonsregistraties*. Nederlandse staatswetten : editie Schuurman & Jordens Zwolle: Tjeenk Willink 1993.

Jansen 1999

B. Jansen, 'Wat is XML?', (<http://www.smallzine.nl/load.html?archief/sz99-33.html>)(12 december 1999).

Kastelein & Legemaate 1994

W.R. Kastelein & J. Legemaate, 'De WGBO in de Tweede Kamer', *Medisch Contact* (49) 1994-9, p.291-292.

De Koster 1999

Y. de Koster, "'Zet alle patiëntgegevens fysiek op één plaats'", *Zorgtelematica Transparant* (4) 1999-2, p. 20.

Leenen 1994

H.J.J. Leenen, *Handboek gezondheidsrecht. Dl. 1: Rechten van mensen in de gezondheidszorg*, Alphen aan den Rijn: Samsom 1994. ISBN 90-6092-771-0

Legemaate 1989

J. Legemaate, 'De onvrijwillige opname. Enige juridische aspecten', *Medisch Contact* (44) 1989-25, p.837-840.

Legemaate 1993

J. Legemaate, 'De BOPZ komt!', *Medisch Contact* (48) 1993, p.361-363.

Legemaate 1994

J. Legemaate, 'De arts en het medisch dossier', *Medisch Contact* (49) 1994-5, p.177-179.

Legemaate 1995

J. Legemaate, 'Eén jaar Wet BOPZ', *Medisch Contact* (50) 1995-5, p.153-154.

Ter Linden 1999

A. ter Linden, 'Checklist voor medische chipcards: een checklist om een chipcardproject een kans van slagen te geven', *Privacy & Informatie* (2) 1999-4, p. 162-169.

Van Lomwel & Van Veen 1996

A.B. van Lomwel & E-B. van Veen, *De WGBO. De betekenis voor hulpverleners in de gezondheidszorg*, Vermande, 1996.

Nouwt 1994

S. Nouwt, 'Privacy en medische informatie', in: J.M.A. Berkvens e.a., *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 1994, p. 171-194.

Nouwt 1997

S. Nouwt, *Zorg voor privacy. Informatietechnologie en informationele privacy in de gezondheidszorg* Den Haag: Sdu 1997. ISBN 90 54 09141 X

Otten & Wildevuur 1996

R. Otten & S.E. Wildevuur, 'De digitale toren van Babel', *Medisch Contact* (51) 1996-23, p. 769-772.

Overkleef-Verburg 1995

G. Overkleef-Verburg, *De wet persoonsregistraties. Norm, toepassing en evaluatie*, Zwolle: Tjeenk-Willink, 1995. ISBN 90-271-4040 5.

Ploem 1999

M.C. Ploem, 'Informationele privacy in de gezondheidszorg: algemene privacywetgeving overbodig?' *Privacy & informatie* (2) 1999-2, p. 52-59.

Van der Put & Berendsen 1994

M.J.M.A. van der Put & R.R.M. Berendsen, 'Houdt de overleden patiënt zijn geheimen? Het recht op en de plicht tot geheimhouding na overlijden', *Medisch Contact* (49) 1994-2, p.61-64.

Registratiekamer onderzoeksrapport Casusregisters GGz 1993

Casusregisters in de geestelijke gezondheidszorg (onderzoeksrapport 9-6-1993), Rijswijk: Registratiekamer 1993.

Registratiekamer advies Patiëntendossier BOPZ 1993

Besluit patiëntendossier BOPZ, (advies aan de regering), Rijswijk: Registratiekamer 1993.

Registratiekamer onderzoeksrapport Rekening arts 1994

De rekening van de arts, (onderzoeksrapport 11-02-1994), Rijswijk: Registratiekamer 1994, p.356-357.

Registratiekamer memorandum Ontwerp EG-richtlijn Bescherming persoonsgegevens 1994

Ontwerp EG-richtlijn bescherming persoonsgegevens (memorandum, advies aan de regering 23-09-1994), Rijswijk: Registratiekamer 1994.

Registratiekamer rapport Beveiliging persoonsregistraties 1994

Beveiliging van persoonsregistraties, (rapport, TA reeks november 1994), Rijswijk: Registratiekamer 1994. ISBN 90 346 31 230.

Registratiekamer advies Medische zorgpas 1995

Advies medische zorgpas (advies aan de regering), Rijswijk: Registratiekamer 1995.

Registratiekamer Medicatiebewaking door centrale patiënten administratie 1998

Medicatiebewaking door centrale patiënten administratie, (rapport) Den Haag: Registratiekamer 1998.

Van Rijen & Van Veen 1991

A.J.G. van Rijen & E-B. van Veen, 'Omgaan met persoonsgegevens. Het ontwerp van Wet op de geneeskundige behandelingsovereenkomst en de Wet Persoonsregistraties: verschillen in kaart gebracht' *Medisch Contact* (45) 1990-39, p.1152-1155.

Van Rossum e.a. 1995

H.van Rossum e.a., *Privacy-enhancing technologies. The path to anonymity*, Rijswijk: Registratiekamer 1995. ISBN 90 346 3202 4.

RVZ advies Informatietechnologie in de zorg 1996

Informatietechnologie in de zorg (advies 10-1996), Zoetermeer: voorlopige Raad voor de Volksgezondheid & Zorggerelateerde dienstverlening 1996. ISBN 90 5732 009 6.

Sluyters & Biesart 1995

B. Sluyters & M.C.I.H. Biesart, *De geneeskundige behandelingsovereenkomst na invoering van de WGBO*, Zwolle: W.E.J. Tjeenk Willink, 1995, p. 62-75, 101-110.

Spreeuwenberg 1996

C. Spreeuwenberg, 'Informereren: mensenwerk of technologie?', *Medisch Contact* (51) 1996-20, p. 669.

Tekstuitgave Privacybescherming persoonsgegevens 1999

Tekstuitgave Privacybescherming persoonsgegevens 1999, Alphen aan den Rijn: Samsom 1999. ISBN 90 422 0210 6.

Walsh 1998

N. Walsh, 'A technical introduction to XML', (<http://www.xml.com/pub/98/10/guide0.html>)(1 december 1999).

Weegenaar 1999

B. Weegenaar, 'XML in a nutshell', (<http://www.informatie.nl/rubrieken/forwebeyesonly/1999/KorteIntroductieXML.html>)(12 december 1999).

Afkortingen

AMvB	Algemene M aatregel van B estuur
APZ	Algemeen P sychiatrisch Z iekenhuis
BGG	B esluit gevoelige gegevens (n.a.v.art.7 ¹ WPR).
BIG	wet op de B eroepsuitoefening in de I ndividuele G ezondheidszorg
BOPZ	Wet b ijzondere o pnemingen in p sychiatrische z iekenhuizen
BPB	B esluit patiëntendossier B opz
CSIZ	C oördinatiepunt S taandaardisatie I nformatievoorziening Z orgsector
DOM	D ocument O bject M odel
DTD	D ocument T ype D efinition
ECG	E lektrocardiogram
EMD	E lektronisch M edisch D ossier
EPD	E lektronisch P atiënten D ossier
EVRM	E uropees verdrag tot bescherming van de rechten van de m ens
EZD	E lektronisch Z org D ossier
GEMD	G emeenschappelijk E lectronisch M edisch D ossier
GEPD	G emeenschappelijk E lektronisch P atiënten D ossier
GGz	G eestelijke G ezondheidszorg
Gz	G ezondheidszorg
Gw	G rondwet
HIS	H uisarts I nformatie S ysteem
HTML	H yper T ext M arkup L anguage
i.c.	in casu
ICT	I nformatie- en C ommunicatietechnologie
ICZ	programma I nformatie- en C ommunicatietechnologie in de Z org
IPZ	I CT P latform in Z org
IVBPR	I nternationaal V erdrag inzake B urgerrechten en P olitieke R echten
KNMG	K oninklijke N ederlandsche M aatschappij tot bevordering der G eneeskunde
KWZ	K waliteitswet Z orginstellingen
LIP	L andelijk I nformatiepunt voor P atiënten
MD	M edisch D ossier.
m.t.	m ijn toevoeging
MvA	M emorie van A ntwoord
MvT	M emorie van T oelichting
NAW	N AW-gegevens, vaste aanduiding voor naam -, adres - en woonplaats gegevens.
NIS	N VAGG I nformatie S ysteem
NP/CF	N ederlandse P atiënten/ C onsumenten F ederatie
NTG	N ederlands T ijschrift voor G eneeskunde
PAAZ	P sychiatrische A fdeling A lgemeen Z iekenhuis
PET	P rivacy-enhancing T echnologies
PG	P arlementaire G eschiedenis
PIG	P atiëntenregister I namurale G ezondheidszorg
REMD	R egionaal E lectronisch M edisch D ossier
REPD	R egionaal E lectronisch P atiënten D ossier

Afkortingen

RIAGG	R egionale I nstelling A mbulante G Gz
RIBW	R egionale I nstelling B eschermende W oonvormen
RIS	R iagg I nformatie S ysteem
SIG	S tichting I nformatievoorziening voor de G ezondheidszorg
SWP	S tichting W aarborging P rivacy
TMI	T ijschrift voor M edische I nformatica
VAGG	V ereniging A utomatisering G eestelijke G ezondheidszorg
VWS	Ministerie voor V olksgezondheid, W elzijn en S port
WBP	W et B escherming P ersoonsgegevens
WGBO	W et op de G eneeskundige B ehandelingsovereenkomst
WPR	W et P ersoonsregistraties
WvSr	W etboek van S trafrecht
WvSv	W etboek van S trafvordering
XML	E xtensible M arkup L anguage
ZIS	Z iekenhuis I nformatie S ystemen

Tijdens mijn onderzoek heb ik diverse gesprekken gevoerd. Daarbij heb ik de welwillende medewerking gehad van de volgende mensen en instellingen, aan wie ik daarvoor dank verschuldigd ben:

prof. dr. A.R. Bakker	(toen Hiscom)
mw. dr. M. Brandsma	(NWO)
drs. D.J. de Bruijn	(Bakkenist ¹⁵³)
mw. mr. R.M.S. Doppegieter	(KNMG)
F.W.M. Fase	(Bakkenist)
mr. P.W.H.M. Francissen	(Ministerie van VWS)
B. Franken	(ZON)
mw. dr. A.M. van Ginneken	(Erasmus Universiteit)
drs. H.B. Haveman	(Ministerie van VWS)
mr. drs. T.F.M. Hooghiemstra	(Registratiekamer)
dr. W. de Jonge	(Vrije Universiteit)
dr. C.P. Louwerse	(Leids Universitair Medisch Centrum)
dr. S. Nouwt	(Katholieke Universiteit Brabant)
mr. M.E.M. Nuyten	(toen Registratiekamer)
mw. prof. mr. dr. H.D.C. Roscam Abbing	(Ministerie van VWS)
ir. H.L. van Rossum	(toen Registratiekamer)
mr. dr. A.H.J. Schmidt	(Universiteit Leiden)
prof. dr. R.J. Wieringa	(toen Vrije Universiteit)
SIAC/ICL ¹⁵⁴	(Maarssen)
Psychiatrisch Ziekenhuis Veldwijk	(Ermelo)
Psychiatrisch Centrum Willibrord	(Heiloo)
Zon & Schild	(Amersfoort)

¹⁵³Bakkenist heet tegenwoordig “Deloitte & Touche Bakkenist”.

¹⁵⁴Siac heet tegenwoordig McKessonHBOC.