Extra’s

overwegingen, invallen, inzichten en uitwerkingen

op persoonlijke titel

januari ‘97

L.Oberendorff

Inhoudsopgave

De volgende overwegingen, invallen, inzichten en uitwerkingen vormen een aanvulling op het eindrapport: "Juridische privacy aspecten REMD's".

Terminologie
In diverse recente stukken wordt gesproken van het Gemeenschappelijk te gebruiken Elektronisch Patiënten Dossier (voortaan afgekort als GEPD), in plaats van Regionaal Elektronisch Medisch Dossier. Om verwarring te voorkomen sluit ik me bij deze terminologie aan.

1. Exclusiviteitswaarborgen

Door middel van autorisatie poogt men de exclusiviteit van informatie te waarborgen.
Met exclusiviteit wordt bedoeld het voorbehouden van gegevens aan een beperkte groep mensen.
Niet alleen inzage in gegevens wordt voorbehouden, maar ook mutatie van gegevens.
Autorisatie kan worden onderverdeeld in:

I. het omschrijven van bevoegdheden met betrekking tot bepaalde informatie (ook wel functionele autorisatie)
II. het voorkomen van ontsluiting buiten die bevoegdheden om (hier voortaan 'beveiliging')

1.1 Aandacht

Veel van de aandacht voor privacy gaat uit naar punt II: het beveiligen van systemen tegen ontsluiting buiten de omschreven bevoegdheden om. Versleuteling (encryptie) en toegangsbeveiliging zijn daarbij hoofdzaak. Met toegangsbeveiliging probeert men vast te stellen of degene die zich identificeert als een bepaalde gebruiker ook daadwerkelijk die gebruiker is (authenticatie). Met geavanceerde middelen als biometrische toegangsbeveiliging en chipcards kan deze identiteit met grote zekerheid worden vastgesteld. Het is het systeem dan duidelijk door wie het wordt gebruikt. Dan wordt bekeken welke bevoegdheden (punt I.) deze gebruiker heeft met betrekking tot aanwezige gegevens. En hier knelt de schoen. De daadwerkelijke exclusiviteitswaarborging is voor een belangrijk deel gebaseerd op de omschrijving van die bevoegdheden. Het is de vraag ‘hoe’, en ‘hoe nauwkeurig’ deze kunnen worden omschreven. Daarbij is ook van belang welke norm de wet stelt, welke norm medisch verantwoord is en wat praktisch haalbaar is. Verder moeten de bevoegdheidsomschrijvingen kunnen 'grijpen op' de aanwezige data. Dergelijke vragen behoeven intensief onderzoek.

Dat de aandacht zich toespitst op het beveiligingsdeel (II) doet vermoeden dat hulpverleners impliciet genoegen nemen met een relatief grofmazige uitwerking van bevoegdheden ten aanzien van informatie. Het lijkt erop dat men al in ruime mate tevreden is wanneer de beveiliging ervoor zorg draagt dat alleen hulpverleners toegang tot aanwezige informatie hebben.
In weze komt dat neer op een bevoegdheidsprofiel met daarin slechts de vraag: "Is degene die zich aanmeldt hulpverlener?".

Een dergelijke houding kan voortvloeien uit de door Leenen aangehaalde[1] wijdverbreide misvatting dat artsen het beroepsgeheim onderling minder nauw hoeven te nemen.
Verder zou men ook van mening kunnen zijn dat beroepsgeheim binnen de informatiesamenleving gaandeweg een andere betekenis en inhoud krijgt. Dit kan echter niet zonder heldere, fundamentele discussie[2].
Wanneer het slechts blijft bij ontwikkeling van het beveiligingsaspect vindt deze overgang mede onder

---

[1] Leenen, H.J.J., *Handboek gezondheidsrecht. Dl. 1: Rechten van mensen in de gezondheidszorg.* 3e druk. Alphen aan den Rijn, Samsom, 1994. blz.200: "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 geldt uiteraard ten aanzien van anderen die beroepsgeheim hebben."

[2] Ippel, P en Nuyten, M, *De maatschappelijke rol van de Registratiekamer. Privacy als proces.* Medisch Contact, jaargang 51, nummer 12, 29 maart 1996.

technologische druk geruisloos plaats. Het is echter goed te beseffen dat hierin keuzes kunnen worden gemaakt. De techniek maakt het mogelijk veel gegevens relatief goedkoop vast te leggen voor toekomstige ontsluiting (bijvoorbeeld in andere instellingen), diezelfde techniek maakt het niettemin ook mogelijk gegevens gedetailleerd af te schermen. Dat de nadruk slechts op het eerste komt te liggen is een *duidelijke* beleidsbeslissing, of *zou dat* moeten zijn. Immers dan zijn niet alleen de mensen die deze beslissing nemen, maar ook de buitenwereld van de strekking en de gevolgen doordrongen. De kans dat daarbij de eerder genoemde fundamentele maatschappelijke discussie ontstaat is niet ondenkbeeldig[3].

Voorlopig echter schrijft de wettelijke norm een veel specifieker bevoegdheidsprofiel voor.

Daarbij denk ik dat een uithollende heroriëntatie op de invulling van het beroepsgeheim voor een belangrijk deel kan worden voorkomen door gebruik te maken van mogelijkheden die ICT biedt voor het specificeren van bevoegdheden t.o.v. medische data.

"De normen veranderen niet door de komst van ICT, wel de wijze van invullen ervan."[4]
Wanneer men van mening is dat beroepsgeheim binnen de informatiesamenleving een andere betekenis en inhoud heeft doet men m.i. het tegenovergestelde. Men sleutelt aan de norm terwijl de aandacht gericht zou moeten zijn op de wijze waarop de norm met behulp van ICT kan worden ingevuld. Dat komt ondermeer doordat ICT aanlokkelijke mogelijkheden heeft die men onder druk van privacyoverwegingen moet laten vallen (zie verderop onder "Inleveren op functionaliteit").

1.2 Schema's

Als hulp voor de gedachtevorming zijn verschillende schema's opgenomen (figuur 1 tm. 4 op pagina 4 en 5). Zij schetsen de invloed van een autorisatiestructuur op pogingen tot inzage.

In figuur 1 wordt de huidige papieren situatie geschetst.
Figuur 2 stelt de ideale situatie voor.
Figuur 3 stelt een praktisch haalbare situatie voor. Een GEPD afgeschermd m.b.v. ICT.
Figuur 4 schetst het gevaar wanneer een autorisatiestructuur te veel afschermt.

In elk figuur:

S Stellen A tm. H verschillende medische dossiers voor. Elk dossier is tot aan de bovenkant van het schema gevuld met gegevens. Elke zwarte staaf stelt een poging tot inzage in dat dossier voor. Hoe hoger de staaf, des te meer gegevens uit dat dossier iemand poogt in te zien. De *rangschikking* van de gebeurtenissen A tm. H is willekeurig.

S Geeft de normlijn (rode stippellijn) aan tot hoever inzage wettelijk geoorloofd is[5].

De rode lijn en de zwarte staven lopen in elk figuur hetzelfde.
Wat veranderd is de loop van de gele autorisatielijn.

Daardoor verandert ook de omvang en de betekenis van verschillende velden. De betekenis van een veld wordt aangegeven met een omschrijving en een pijl. Wanneer de betekenis van een veld in een figuur ten opzichte van het figuur daarvoor veranderd is, dan wordt dat in het blauw aangegeven.

---

[3]In het artikel *Zorgdossier staat centraal in nieuw programma ZON* uit Zorgtelematica Transparant (jaargang 1, nummer 5, december 1996) heeft men het over een landelijke discussiecampagne. Deze zou overeenkomstige elementen kunnen bevatten.

[4]Roscam Abbing, H.D.C. *Patiënt en informatie-communicatietechnologie.* Medisch Contact, jaargang 51, 17 mei 1996, blz.679-681.

[5]Daarbij zijn verschillende aspecten van belang (zie verderop onder het kopje "Bevoegdheidsprofielen" en blz.20 eindrapport + artikel 457 lid 2 WGBO).

Figuur 1.
In figuur 1 wordt de werkwijze geschetst bij een papieren klinisch dossier binnen een algemeen ziekenhuis.

De autorisatielijn geeft aan in hoeverre inzage wordt geweigerd.

Kenmerkend voor de papieren situatie is dat de autorisatielijn slechts twee extremen kent. Verstrekking van het gehele klinische dossier -of- totaal géén verstrekking.

Dat resulteert òf in inzagemogelijkheid tot alle gegevens (A tm. F), òf in totaal geen inzage (G+H).
In de tekening: -bij verstrekking van het gehele dossier loopt de gele lijn hoog: er wordt geen inzage geweigerd.
- bij totaal géén verstrekking loopt de lijn laag: de inzageweigering is maximaal.

De loop van de normlijn geeft aan in hoeverre inzage wettelijk geoorloofd is.

De combinatie van normlijn, autorisatielijn en inzagepoging resulteert voor de onderscheiden gevallen[6]:

-D en E. In deze situatie bestaat toegang tot het gehele dossier. De inzage die plaats vindt is legitiem (veld ”Gerealiseerde normconforme inzage”). Inzage in de rest van het dossier was eveneens legitiem geweest[7] (veld “Potentiële normconforme inzage”).

-A en B. In deze situatie bestaat eveneens toegang tot het gehele dossier. De inzage die plaats vindt is gedeeltelijk legitiem (veld ”Gerealiseerde normconforme inzage”), gedeeltelijk ook niet (veld “Gerealiseerde normovertreding”). Het gedeelte boven de normlijn wordt eigenlijk teveel verstrekt: een te voorkomen[8] privacyinbreuk. Er bestond de mogelijkheid nòg meer gegevens zonder noodzaak in te zien[9] (veld “Potentiële normovertreding”).

-C. Ook hier bestaat weer toegang tot het gehele dossier. De inzage die plaats vind is legitiem (”veld Gerealiseerde normconforme inzage”). Verdere inzage was gedeeltelijk legitiem geweest (veld “Potentiële normconforme inzage”) . Daarnaast bestond eveneens de mogelijkheid gegevens zonder noodzaak[10] in te zien (veld “Potentiële normovertreding”).

-F. Er bestaat toegang tot het gehele dossier. Van de wet had er echter in het geheel geen inzage mogen worden verleend. De autorisatiestructuur verhinderd deze inzagepoging echter totaal niet[11]. Inzage vindt tot het maximale plaats (veld “Gerealiseerde normovertreding).

---

[6]NB. Verdere uitleg en praktijkvoorbeelden zijn te vinden in de bijlage.

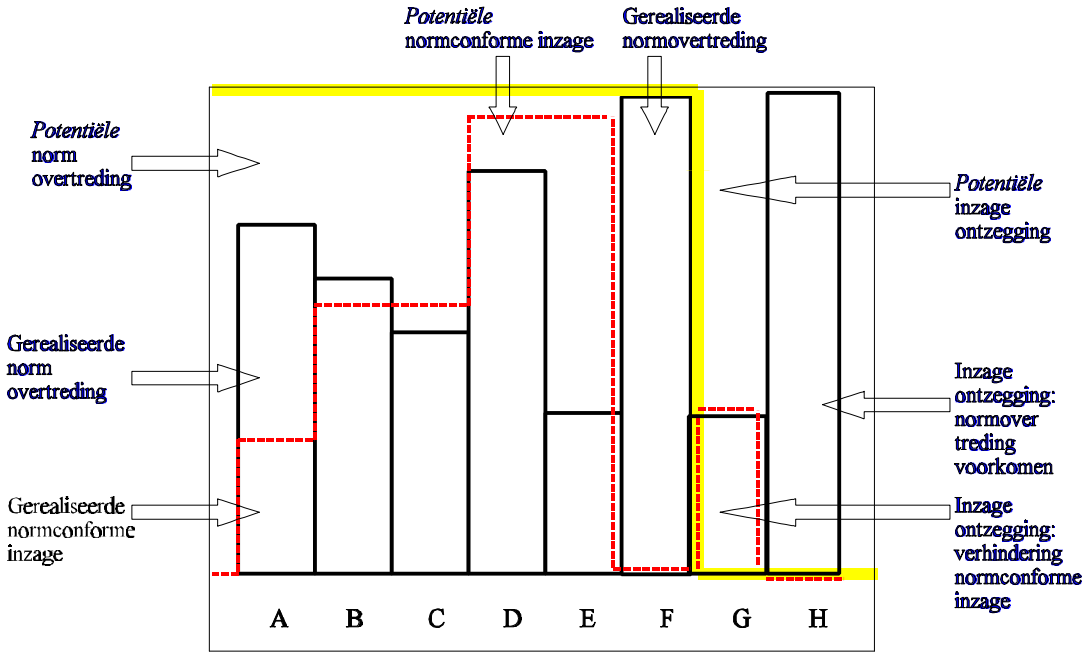
[7]Dat deze niet heeft plaatsgevonden kan verschillende oorzaken hebben. Onder andere: -De hulpverlener vond verdere inzage niet van belang voor de behandeling. -De hulpverlener stond onder tijdsdruk. (P.S. De situatie dat verdere inzage normconform is en tòch niet van belang voor deze hulpverlener is mogelijk doordat de term 'noodzakelijk' in artikel 457 lid 2 WGBO m.i. toegang tot een groter aantal gegevens impliceert dan achteraf noodzakelijk *blijkt* voor die behandeling. Zie voor deze problematiek: Oberendorff, L, *Regionale elektronische dossiers in de Geestelijke Gezondheidszorg, een lakmoesproef voor privacybescherming?*)

[8]Veroorzaakt normconform verstrekken uit papieren dossiers een ondoenlijke werklast? Zie artikel noot 7.

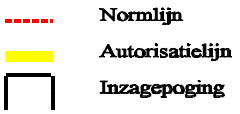
[9]Dat dat niet gebeurt is kan verschillende oorzaken hebben, nu met een zeer uiteenlopend karakter (zowel te goeder als te kwader trouw): o.a.
-De opvrager was hulpverlener en vond verdere inzage niet nodig voor de behandeling of bedwong zich op grond van (beroeps)ethiek of tijdsdruk.
-De opvrager bedwong zijn nieuwsgierigheid of verdere inzage leek niet interessant.

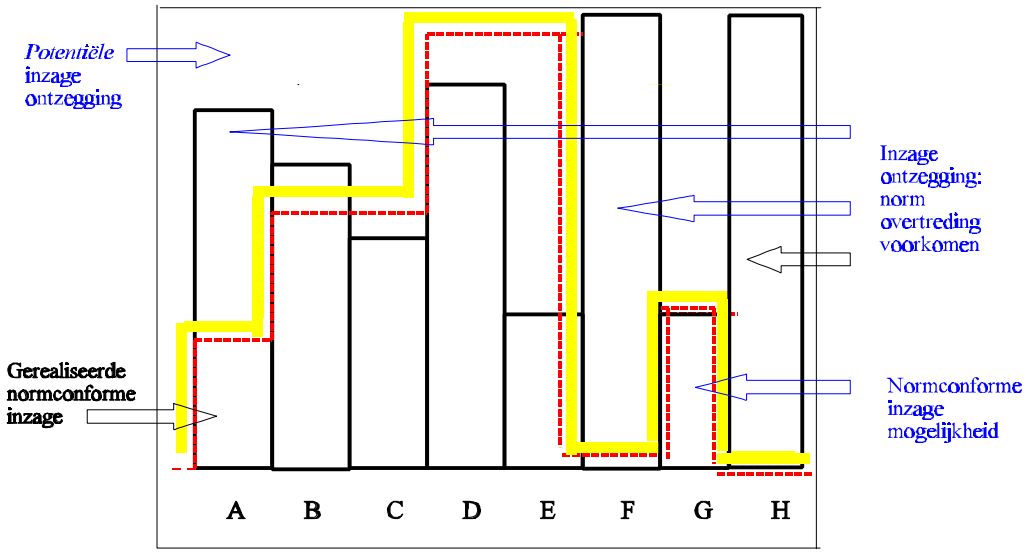
[10]De engelse term ‘need to know’ wordt gebruikt om dezelfde lading te dekken als lid 2 van artikel 457 WGBO.

[11]NB. Verdere uitleg en praktijkvoorbeelden zijn te vinden in de bijlage.

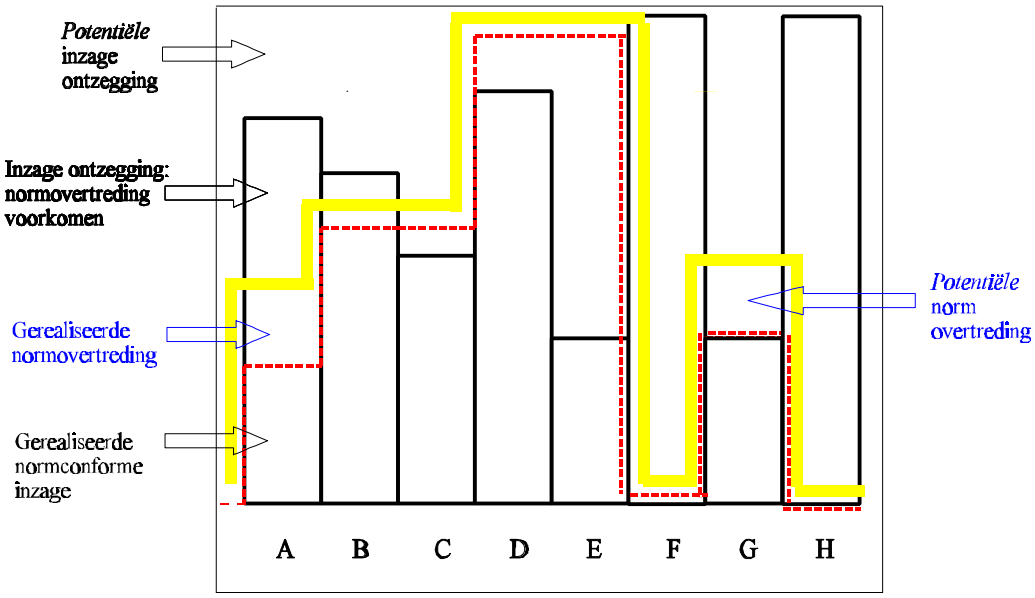


Figuur 1. Papieren traject.

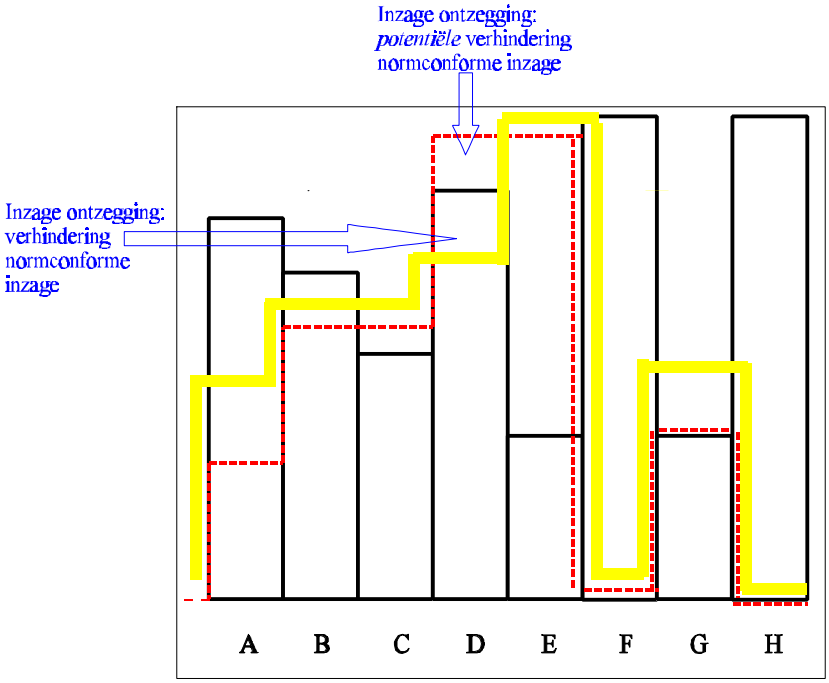




Figuur 2. Ideaal.



Figuur 3. Praktijk toekomst m.b.v. ICT (?)



Figuur 4. Gevaar.

-H. Hier wordt géén dossier verstrekt. Dat is terecht, de norm verbiedt welke verstrekking dan ook aan de aanvrager (veld “Inzage ontzegging: normovertreding voorkomen”). Dit had ook in geval F moeten gebeuren.

-G. Ook hier wordt geen dossier verstrekt. Het inzage verzoek wordt niet gehonoreerd doordat het dossier niet wordt uitgereikt. Een gedeelte van het dossier had echter mogen worden ingezien (veld “Inzage ontzegging: verhindering *normconforme* inzage”). Dit is een gevaarlijke situatie. Inzage kan immers dringend nodig zijn. Het is dan ook de vraag of dit een in de papieren praktijk vaak voorkomende situatie is. Meestal wordt aan iemand die bevoegd is een gedeelte van het dossier in te zien immers het gehele dossier uitgereikt. Dat hij daardoor veel meer gegevens in handen krijgt dan nodig wordt dan voor lief genomen.
Het is echter denkbaar dat mensen die maar een beperkt aantal gegevens nodig hebben toegang wordt ontzegd omdat men ze (praktisch gezien) slechts het gehele dossier kan meegeven.

Figuur 2.
In figuur 2 wordt de ideale situatie geschetst. Hierbij kunnen hulpverleners inzien wat ze moeten inzien, en wordt verdere of andere inzage ontzegd. De informatie komt alleen terecht bij mensen die de informatie ook nodig hebben, waardoor de privacy van de patiënten optimaal wordt gewaarborgd. De gele autorisatielijn loopt samen met de roodgestippelde normlijn: Daar waar de wet zegt dat verstrekking niet mag plaatsvinden[12] wordt inzage door de autorisatiestructuur ontzegd.

Figuur 3.
Een autorisatiestructuur voor een GEPD kan gebruik maken van diverse mogelijkheden die ICT biedt. Daardoor kan de autorisatielijn veel dichter bij de normlijn komen te liggen dan bij het papieren dossier het geval is. Hoe dichter de autorisatielijn de normlijn nadert hoe beter[13]: richting ideaal (figuur 2). Geheel aansluiten zal om praktische redenen echter niet lukken[14]. Daardoor blijven in beperkte mate normovertredingen mogelijk (-G: veld “Potentiële normovertreding”) en worden deze in beperktere mate ook gerealiseerd (-A veld: “Gerealiseerde normovertreding”).

Figuur 4.
Het gevaar van een *te strenge* autorisatiestructuur is dat deze legitieme inzage kan ontzeggen (-D: veld “Inzage ontzegging: potentiële verhindering normconforme inzage”). Daar waar een hulpverlener die informatie ook daadwerkelijk wil inzien (-D: veld “Inzage ontzegging: verhindering normconforme inzage”) kan dit gevolgen hebben. Immers de hulpverlener wordt informatie onthouden die hij nodig heeft voor de behandeling.

Bij het ontwerpen van een autorisatiestructuur voor een GEPD zal er voor moeten worden gewaakt dat deze geen normconforme inzage gaat ontzeggen (gele autorisatielijn onder roodgestippelde normconforme lijn). Daarnaast is niettemin duidelijk dat het autorisatie ‘plafond’ (gele autorisatielijn) omlaag moet. Wanneer het gaat om zoveel gevoelige gegevens van zoveel verschillende mensen die op zoveel verschillende plaatsen opvraagbaar zijn kan men zich niet meer dezelfde vrijheden permitteren als bij het papieren traject.

De uitgebreide autorisatiestructuur stuit op weerstanden van hulpverleners, daarbij wordt vaak het argument gebruikt dat een hulpverlener niet bij informatie kan die hij nodig heeft (zoals geschetst in figuur 4).

---

[12]Het wettelijke voorschrift valt per defenitie samen met de legitieme behoefte van de hulpverlener. Immers de gegevens noodzakelijk voor de door hem, in het kader van de behandeling, te verrichten werkzaamheden mag hij inzien.

[13]Er moet echter voor worden gewaakt dat de autorisatielijn niet onder de normlijn schuift (zie verderop onder figuur 4).

[14]Bijvoorbeeld niet omdat het systeembeheer nog toegang heeft op gegevensniveau (zie verderop). Of omdat de dagelijkse praktijk dusdanig veel hoedanigheden van hulpverleners kent dat deze niet allemaal kunnen worden uitgewerkt in het bevoegdheidsprofiel (zie verderop).

M.i. kan het autorisatie ‘plafond’ echter in ruime mate omlaag zonder (figuur 3) dat er gevaarlijke situaties zoals in figuur 4 ontstaan. Dat daarbij door de gebruiker extra handelingen moeten worden verricht is onvermijdelijk. Een groot deel van de weerstand heeft volgens mij te maken met deze extra werklast. Gebruikers moeten inzien dat dit een onontkoombaar aspect is van een GEPD (zie verderop onder “Gebruikers-inleveren op functionaliteit”).

1.3 Kwaliteit

Exclusiviteit van gegevens door uitwerking van bevoegdheids-profielen(I) en beveiliging(II) is niet alleen van waarde voor privacy bescherming in 'enge zin'(confidentiality bij inzage), maar ook voor kwaliteitsbewaking(integrity bij mutatie). De kwaliteit van de opgeslagen gegevens is van *cruciale* betekenis voor de kwaliteit van het systeem en de op deze informatie gebaseerde gezondheidszorg[15]. Een systeem waarin een grote mate van gedistribueerde gegevens-*be*-werking plaatsvindt kan niet zonder een nauwsluitende veranderingsbevoegdheids-structuur.

Om een voorstelling te maken kunnen we ons de zwarte staven uit de figuren 1 tm. 4 nu als *mutatie*poging (in plaats van een inzagepoging) voorstellen.

De maatregelen die je moet nemen om ervoor te zorgen dat informatie alleen door bevoegden kan worden veranderd kunnen ook worden gebruikt voor controle op inzage. Met andere woorden de inzage autorisatie kan deels gebouwd worden op dezelfde 'faciliteiten' als de mutatie autorisatie. Ik zeg met opzet gedeeltelijk. Men zou kunnen suggereren dat mutatiebevoegdheid met inzagebevoegdheid kan worden gelijkgeschakeld in die zin dat zonder inzagebevoegdheid in ieder geval geen mutatie kan plaatsvinden. Dat is waar, maar de uiteindelijke specifiteit van de bevoegdheidsprofielen blijkt echter telkens te worden veroorzaakt door privacyoverwegingen, zij nopen tot een nog verdere uitwerking van de bevoegdheids-profielen dan de kwaliteitseisen[16]. Anders gezegd 'integrity' vereist een minder verstrekkende bevoegdheidsprofielen-structuur dan 'confidentiality'. Voor wat betreft integrity speelt voornamelijk een rol of en wat voor hulpverlener een gebruiker is, en of hij met een patiënt een behandelrelatie heeft[17].

Dit onderscheid maak ik omdat instellingen de neiging hebben meer gewicht toe te kennen aan het integriteitsbelang dan aan het privacybelang. Terecht, aangezien deze integriteit nog directer ten koste gaat van de algemene kwaliteit van de zorg. Helaas komt de, door het privacybelang gedicteerde, verdere uitwerking van de bevoegdheden er dan vaak bekaaid van af.

---

[15]*Terzijde*: absolute aanrader in dit verband is de film 'the Net'.

[16]NB. dat wil niet zeggen dat er vaker mutatiebevoegdheid wordt uitgedeeld. Alleen dat de inzagebevoegdheid van specifiekere voorwaarden afhangt.

[17]Deze voorwaarden zijn ondermeer beperkt omdat elke mutatie als aanvulling wordt opgeslagen (=historisch archief mutaties). In weze wordt er dus niet echt veranderd maar aangevuld (NB:in eerste instantie is slechts de laatste aanvulling zichtbaar). De 'mutatie'voorwaarden kunnen hierdoor worden beperkt.

1.4 Bevoegdheidsprofielen:

In het eindrapport[18] wordt aangegeven op welke factoren de bevoegdheidsprofielen moeten zijn toegesneden. Logischerwijs volgen uit de wettelijke voorschriften:

persoon patiënt
behandelrelatie
persoon hulpverlener
functie hulpverlener
specialisme hulpverlener
rol hulpverlener binnen het behandelteam van de patiënt
soort/aard behandeling
WGBO of BOPZ behandeling
toestemming patiënt (eenmalig gebruik/opslag/hergebruik[19])
toestemming anderen
expliciet toevertrouwd
anderen
organisatie

Op grond hiervan kunnen de volgende bevoegdheden worden toegekend:
wijzigen(=aanvullen[20]), inzien, verwijderen en printen

Deze deelaspecten spelen vaak tegelijkertijd en grijpen in- en op elkaar.
Zo kan een ander informatie over de patiënt geven waarbij hij verdere verstrekking aan derden voorbehoudt.

Verder grijpen een aantal aspecten ‘meer op het gegevensinhoudelijke’ dan andere.
Zo geeft het aspect ‘behandelrelatie’ aan of een bepaalde hulpverlener überhaupt wel een behandelrelatie heeft met een patiënt. Die vraag is makkelijker te beantwoorden dan tot welke informatie, *op grond van de ‘aard van de behandeling’*, toegang wordt gegeven.

Het antwoord op de laatste vraag vergt medische kennis.
Een stap in de richting kan zijn het splitsen van gegevens in archief en werkgegevens. Daarnaast kan bij het archiveren ook een kerndossier worden gecreëerd:
Wanneer een patiënt voor de eerste maal wordt opgenomen worden gegevens opgeslagen als werkgegevens. Tijdens deze eerste behandeling werkt men met die werkgegevens-set. Aan het eind van de behandeling wordt bezien welke gegevens daarvan in de toekomst van belang kunnen zijn. Een gedeelte van de werkgegevens wordt weggegooid en de rest vormt het kerndossier[21] dat wordt gearchiveerd. Bij de samenstelling van dat kerndossier houdt de daarvoor verantwoordelijke (waarschijnlijk de hoofdbehandelaar) de vraag voor ogen: “Welke gegevens zijn mogelijkerwijs noodzakelijk voor de door hulpverleners bij *een* nieuwe behandeling te verrichten werkzaamheden.”. Wanneer de nieuwe behandeling zich aandient is duidelijker welke gegevens voor *die* behandeling noodzakelijk zijn. De werkset voor die behandeling is dus een selectie uit de gearchiveerde gegevens. Zo wordt de informatie beschikbaar gesteld op grond van de *‘aard van de behandeling’*.

[18]Zie blz.20 eindrapport.

[19]Zie verderop onder “Acceptatie - Toestemming”

[20]Zie noot 17.

[21]Deze werkwijze wordt bij het huidige papieren traject ook gebezigd.

1.5 Valkuilen bevoegdheidsprofielen

Noodzakelijk pas achteraf.
De hulpverlener is degene die de zeer vertrouwelijke gegevens in eerste instantie worden toevertrouwd. Hij is dan ook degene die, met inachtneming van zijn beroepsgeheim, na toestemming van de patiënt, bepaalt in hoeverre ze aan anderen in het kader van de behandeling worden verstrekt. Hij is degene die anderen m.b.t. bepaald informatie autoriseert/bevoegdheden geeft. Met name aan de hoofdbehandelaar wordt hieromtrent, ook in het eindrapport, een grote verantwoordelijkheid toebedeeld. Hij heeft een initiërende functie. Dat betekent dat deze in principe toegang heeft tot haast alle vastgelegde archief-gegevens van haast alle patiënten. Het is de vraag hoe het best kan worden gecontroleerd of hij geen misbruik maakt van die macht, met andere woorden of degene waarvan hij informatie opvraagt ook een patiënt is waarmee hij op dat moment een behandelrelatie heeft, of mogelijkerwijs gaat krijgen. Een oplossing zou kunnen liggen in het splitsen van bevoegdheden: een administratieve kracht die geen toegang heeft op gegevens inhoudelijk niveau initieert de behandelrelatie. Daarna kan de hoofdbehandelaar die slechts gegevensinhoudelijk toegang heeft (en dus geen 'behandelrelatie' kan initiëren in de zin van *zichzelf* toegang verschaffen tot alle opgeslagen gegevens), die gegevens uit het medisch verleden van de patiënt selecteren die hij voor de huidige behandeling noodzakelijk acht.

Verder moet de hulpverlener bepalen welke gegevens noodzakelijk zijn voor zijn werkzaamheden. Dat impliceert toegang tot meer gegevens (zie noot 7). Hij zal gegevens zelf op belang willen selecteren. In bepaalde mate zal hij dat ook moeten kunnen. De hoofdbehandelaar doet dat uit de grotere groep: medisch verleden (de opgeslagen kerndossiers: het archief). Een andere hulpverlener zal uit zijn doorsnede[22] van de door deze hoofdbehandelaar gecreëerde 'werkset' gaan selecteren.

Administratieve functies
Voor hulpverleners kan de bevoegdheid worden toegesneden op behandelrelatie. Dat geldt ook voor die administratieve krachten die de hulpverlener direct ondersteunen. Zo kunnen de bevoegdheden van een secretaresse[23] van een arts, worden gekoppeld aan de behandelrelaties van die arts. De secretaresse kan dan de gegevens van die patiënten die de arts *niet* behandeld überhaupt niet in zien[24].

Voor andere meer algemene administratieve functies kan de autorisatie niet gebaseerd worden op zorgrelatie. Die is er namelijk niet. Er moet voor worden gewaakt dat de administratie hierdoor ongelimiteerd toegang kan krijgen tot gegevens. Het systeem zou dan voor een hulpverlener 'mooi dicht' zitten, terwijl de administratie 'overal' bij kan. De overige bevoegdheden die dergelijke medewerkers t.o.v. informatie hebben moeten daarom worden beperkt. De taak die bijvoorbeeld de Medische Administratie heeft legitimeert geen 'totale toegang'. In het huidige papieren traject controleren zij onder andere of een hulpverlener het dossier volledig heeft ingevuld. Programmatuur zou een zelfde signalerende functie kunnen herbergen. De invoering van een GEPD kan dus voor verschillende instellingsonderdelen een heroriëntatie op hun functie met zich meebrengen[25].

[22]Met "zijn doorsnede" van de werkset wordt bedoeld die gegevens die hij op grond van zijn hoedanigheid mag inzien. De op de wettelijke norm toegesneden bevoegdheidsprofielen zorgen hiervoor.

[23]Of natuurlijk secretaris. (Zo ook verder in het rapport.)

[24]Deze behandelrelatie is *een* aspect van het bevoegdheidsprofiel van de secretarresse. Op grond van haar functie heeft ze natuurlijk andere bevoegdheden dan de arts.

[25] Met welk doel hebben zij toegang, in hoeverre kan dat doel ook zonder die toegang worden gerealiseerd.

Wat ook kan meehelpen aan betere waarborgen is het splitsen van bevoegdheden in meerdere categorieën. Bevoegdheden die betrekking hebben op gegevens*inhoud* (gegevensbeheer) naast bevoegdheden die betrekking hebben op het uitdelen van bevoegdheden (sleutelbeheer) aan anderen. Het uiteentrekken van deze bevoegdheden en ze vervolgens toekennen aan verschillende personen verkleint de kans op mis- of wangebruik. Een dergelijke uiteentrekking is niet voor elke gebruiker te realiseren, sommige gebruikers moeten over beide soorten bevoegdheden beschikken. Toch heeft deze werkwijze op belangrijke punten een grote waarde (zie hiervoor “Noodzakelijk pas achteraf”).

Praktisch
Het gevaar bestaat dat aan de hulpverlener toegekend sleutelbeheer en/of gegevensbeheer wordt overgedragen aan administratieve krachten. Hulpverleners zitten vaak niet op deze extra werkdruk te wachten. Wanneer sleutelbeheer onder verantwoordelijkheid van de hulpverlener door een administratief medewerker wordt uitgevoerd brengt dat minder gevaar met zich mee dan wanneer diezelfde medewerker *gegevensinhoudelijke* bevoegdheden voor de hulpverlener gaat uitvoeren. Het behoort in eerste instantie de hulpverlener te zijn die informatie bijvoorbeeld als uitermate vertrouwelijk classificeert.

Systeembeheer
Het systeembeheer heeft nu meestal toegang tot alle informatie. Op grond van de hoeveelheid gevoelige gegevens van zoveel verschillende mensen moet worden bekeken in hoeverre deze mogelijk kan worden beperkt. Het is de vraag in hoeverre systeembeheerders inzage en mutatiebevoegdheden moeten hebben t.a.v. medisch informatie (heroriëntatie functie). Wellicht kan toegang door systeembeheer worden voorkomen door bijvoorbeeld versleutelde opslag.

Over het overdragen van rechten
Een systeem dat bij functionele autorisatie vaak wordt gebruikt is het overdragen van rechten. Is de ontvanger van die rechten op zijn beurt weer in staat die rechten door te geven? Kan de doorgever de overdracht intrekken? Wat gebeurt er dan met de door de eerste ontvanger doorgegeven rechten? Wordt de doorgifte gelogd? Is er sprake van zuivere overdracht of behoudt de 'doorgever' zijn rechten?
Bij een dergelijk systeem is hoofdregel dat iemand in ieder geval nooit meer bevoegdheden kan doorgeven dan hij zelf heeft. Dat is geen bezwaar wanneer het om gelijksoortige bevoegdheden gaat. Hierboven werd echter duidelijk (uiteen trekken bevoegdheden) dat het geven van soorten bevoegdheden die men zelf niet mag uitoefenen niet per definitie bezwaarlijk hoeft te zijn. Zo werkte het geven van gegevensinhoudelijke toegang aan een hoofdbehandelaar door iemand van de administratie (die zelf deze gegevensinhoudelijke toegang nooit kan uitoefenen) privacy beschermend.

Koppeling naam/functie
Er moet worden uitgekeken met de veronderstelling dat een persoon bij één functie hoort. Het blijkt dat één persoon in verschillende hoedanigheden kan optreden. Ook kan het zijn dat een en dezelfde hulpverlener later in een andere hoedanigheid optreed t.o.v. een patiënt. Heeft hij dan de bevoegdheden t.o.v. een patiënt op grond van beide hoedanigheden?
Hoe zit dat met uitzend/oproepkrachten? En andere 'zwevende' hulpverleners?

Crisis scherm
Er bestaat de behoefte aan een crisisscherm binnen de programmatuur voor een GEPD. Van de opgenomen patiënten kan dan een aantal gegevens worden ingezien zonder dat een behandelrelatie behoeft te worden ingesteld (voor veel handelingen ontbreekt de tijd a.g.v. een noodsituatie).
Het verdient aanbeveling bij het gebruik van het crisisscherm een tekstveld voor verantwoording van het gebruik van die functie te reserveren. Daarnaast is het de vraag of alle beveiliging mag worden doorbroken in een noodsituatie. Is dat inclusief de afscherming van gegevens waarbij anderen voorbehoud hebben gemaakt? En inclusief uitdrukkelijk toevertrouwde informatie?

Informatiebehoeften
Bij het ontwerpen van functionele autorisaties merken instellingen dat men vaak geen idee heeft wie, wanneer, welke gegevens nodig heeft voor een behandeling. Dat komt omdat in het papieren traject vaak toegang bestond tot het gehele dossier (zie figuur 1). Het in kaart brengen van de informatiestromen binnen de instellingen die een GEPD gaan gebruiken is een logische eerste stap. Op grond van dergelijke behoeften kunnen software-producteisen worden opgesteld en later ook de functionele autorisaties worden ingedeeld.

'Grijpen' op informatie
Om de functionele autorisaties te laten grijpen op de aanwezige informatie is de manier waarop deze wordt gestructureerd en opgeslagen van belang. Ze moeten op een 'kleine korrel' kunnen werken.
Het is de vraag of beveiliging op veldniveau toereikend is. In het eindrapport wordt eigenlijk bevoegdheidsspecificatie op gegevens niveau aanbevolen. Het is niet duidelijk of dat ook technisch en praktisch haalbaar is. Het gaat er echter in wezen niet om hoe de vereiste bescherming wordt verwezenlijkt maar òf die wordt verwezenlijkt. Wellicht kan met het gebruik van speciale velden (bijvoorbeeld: "uitdrukkelijk toevertrouwd" en "anderen-uitdrukkelijk toevertrouwd") eenzelfde bescherming worden geboden. Of een dergelijke oplossing te grofmazig is zal uit nader onderzoek moeten blijken.

1.6 Opslag

Historische database
De logging van mutatie van gegevens verdient speciale aandacht. Een dergelijke functie is onontbeerlijk. Er zal moeten kunnen worden nagezocht wie wat veranderde, maar ook wat er daarvoor stond. Zo kan er bij eventuele schade en controle worden nagezocht wie wanneer wat opschreef. Deze gegevens mogen niet door mutatie kunnen verdwijnen.

Anderen
In medische dossiers en vooral in psychiatrische dossiers komt ook veel informatie m.b.t. anderen dan de patiënt[26] voor. 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. Dient deze informatie in het dossier te worden opgeslagen en steeds te worden verstrekt? Het systeem moet voorzien in mogelijkheden om restricties t.a.v. dergelijke gegevens aan te geven. Dat betekent ook dat aanwezige data m.b.t. anderen als zodanig moet zijn te herkennen.
Het niet merken van informatie als zijnde informatie van anderen heeft tot gevolg dat wanneer die informatie in het (kern)dossier wordt opgenomen deze door het systeem niet meer als zodanig te herkennen is. Ze kan dan ook nooit meer als zodanig gefilterd worden. Dat kan tot consequentie hebben dat men gegevens niet aan derden kan verstrekken. Dat zou immers een onevenredig grote inbreuk op de privacy van die ander kunnen zijn.[27] Het ligt dan ook in de rede informatie m.b.t. anderen *altijd* als zodanig te merken.

[26]Zie blz. 19 eindrapport.

[27] De term "evenredig" duidt op een belangen afweging. Hier mag nu echter niet alleen bij de belangen van de patiënt en van de ander stil worden gestaan. D.w.z. er moet ook meespelen dat de 'instelling iets aan het labelen had kunnen doen.' Niet labellen en dan onder druk van het patiëntenbelang toch verstrekken is niet de belangenafweging waar de wetgever op heeft willen aansturen.

1.7 Beveiliging

De exclusiviteit van informatie hing naast de definitie van bevoegdheden ook af van de beveiliging tegen toegang buiten deze bevoegdheden om[28]:

Logboek
Het logboek is een repressief middel (waarvan eveneens een preventieve 'afschrikkende' werking uitgaat): controle achteraf op de rechtmatigheid van gegevensverwerking. Deze informatie is niet alleen van belang i.v.m. de privacybescherming maar ook met *aansprakelijkheid*[29] en *kwaliteitsbewaking*.
Wettelijk voorgeschreven opslag van gegevens[30] in een logboek en de aanbevolen opslag van gegevens[31] resulteert in enorme log bestanden. Actieve controle op grond van de gegevens in het bestand wordt daardoor moeilijk, het verdient daarom aanbeveling de log gegevens die mogelijkerwijs met misbruik te maken hebben te scheiden van de reguliere login gegevens door middel van bijvoorbeeld een apart log-bestand of door ze makkelijk opspoorbaar te maken. Zo zijn verstrekkingen die gedaan zijn via de achterdeur 'noodtoestand' altijd verdacht en er zal standaard verantwoording voor moeten worden afgelegd (zo mogelijk binnen de GEPD programmatuur zelf). Op een dergelijke manier wordt een efficiënte en effectieve controle met behulp van de log bestanden mogelijk.

Identificatie & Authenticatie
Om slechts volgens de bevoegdheidsprofielen te ontsluiten moet eerst aan het systeem kenbaar zijn wie informatie opvraagt (identificatie), daarna moet gecontroleerd worden of degene die zich als een hulpverlener kenbaar maakt ook inderdaad die hulpverlener is (authenticatie). Normaliter wordt voor de identificatie de naam of login gebruikt, en voor authenticatie een bijbehorend wachtwoord.
Vraag is of een systeem dat valt in een categorie uit het beveiligingsrapport[32] van de Registratiekamer die de zwaarste vorm van beveiliging behoeft[33], kan volstaan met een dergelijke eenvoudige procedure.

"The nature of communications networks today makes the continued reliance on traditional, reusable passwords for user authentication totally unacceptable."
- Computer Security Institute, San Francisco, California

"As you look at different (security) solutions, be realistic.... Sooner or later, your weakest link is someone who works for you, not the hardware and software."
- Marcus Ranum, DEC SEAL Internet Firewall Architect

Vandaar dat in het rapport de mogelijkheid van een fysiek hulpmiddel (token) wordt aangegeven. Bij het gebruik van een “token” kan men bijvoorbeeld denken aan een chipkaart die de hulpverlener identificeert en

---

[28] Deze combinatie van controle achteraf met beperkingen vooraf resulteert in betere waarborgen.

[29] Zie blz.15 eindrapport.

[30] O.a. derden-verstrekkingen na opvraag van geregistreerde(zie blz.28 eindrapport) of voor doorgeven van correcties (zie verderop onder “Correctierecht”).

[31]Zoals verderop blijkt de opname van wie, wanneer, wat, van welke patiënt, opvroeg, toevoegde, veranderde, wiste, printte te worden aanbevolen (of zelfs vereist als uitwerking van de beveiligingsplicht van artikel 8 WPR).

[32]TA reeks, november 1994. ISBN 90 346 31 230, met name blz. 19 tm. 33.

[33]Door de aard van de gegevens (psychologisch/medisch), het informatiegehalte (het aantal geregistreerden en de inhoud en hoeveelheid opgenomen gegevens=>de mate waarin een gedetailleerd beeld van de geregistreerde wordt geschetst), het gebruik (frequentie waarmee de gegevens worden geraadpleegd, het aantal personen dat toegang heeft, aantal lokaties waar rechtstreekse toegang mogelijk is) en de mogelijke gevolgen die misbruik kan hebben.

authenticeert[34] en eveneens de sleutel bevat voor het ontcijferen van de gecodeerde gegevens 'aan de terminal'. Deze zou de hulpverlener dan naast een wisselend password kunnen gebruiken. Gegevens blijven slechts leesbaar op de terminal wanneer de kaart is ingevoerd.
Een dergelijke kaart zou een zeer belangrijke bijdrage aan de privacybescherming leveren, praktisch gezien vormt ze een ideale combinatie tussen gebruiksgemak en bescherming.

Waarborgen exclusiviteit
In hetzelfde rapport beschrijft de Registratiekamer duidelijk welke gevolgen de inschaling in deze catatonie heeft. Hierbij noemt zij niet slechts aspecten die te maken hebben met beveiliging *pur sang* maar richt haar aandacht op het meer algemene: *waarborgen van exclusiviteit*.

Ik wil er hier enkele uitgebreid noemen.

Allereerst t.a.v. de beveiliging:

I. De toegangscontrole:
- Er moet een beperking worden gesteld aan het aantal keren dat onbevoegd wordt geprobeerd toegang te krijgen tot een registratie. Afwijkingen moeten worden gesignaleerd en onderzocht (=>*logboek*).
- Bij het verkrijgen van toegang dient de fysieke plaats van de gebruiker zo nauwkeurig mogelijk geïdentificeerd en gecontroleerd te worden.
- De toegang tot lokaties waar toegang tot de persoonsregistratie kan worden verkregen moet worden gecontroleerd en worden beperkt tot personen die bevoegd zijn.
- Het bevoegd gebruik is afhankelijk van meer dan alleen user-id en wachtwoord; maar ook van het tijdstip, de plaats van handelen en de technische omgeving. Hiernaast dient een additionele identificatie en authentificatie procedure plaats te vinden. De procedure voor het eenduidig vaststellen van de authenticiteit van de gebruiker kan het gebruik van fysieke middelen (tokens) vereisen.
- Een registratie van verleende toegang dient te waarborgen dat de verantwoordelijkheid van de gebruiker voor de uitgevoerde handelingen achteraf eenduidig vastgesteld kan worden (=>*logboek*).

II. Het vastleggen van handelingen van de gebruikers:
- De toegang tot een persoonsregistratie dient te worden vastgelegd, evenals het vastleggen van een aanduiding van de gegevens die zijn bevraagd of bewerkt. De vastgelegde gegevens dienen regelmatig met de toegekende bevoegdheidsprofielen te worden vergeleken (=>*logboek*).

III. Het gebruik van randapparatuur en beeldschermen:
- Er mag alleen worden gewerkt met randapparatuur die onder direct toezicht van de betreffende medewerker staat.
- Alleen op beeldschermen die daarvoor expliciet zijn aangewezen mogen persoonsgegevens opgevraagd worden.
- De gegevens mogen niet langdurig op het beeldscherm zichtbaar zijn.

IV. De in- en uitvoer van gegevens en de datacommunicatie:
- Gegevens dienen zodanig te worden getransporteerd en beschikbaar te worden gesteld, dat uitsluitend de gerechtigde ontvanger de uitvoer kan interpreteren: gegevens dienen versleuteld te worden verzonden. De gebruikte encryptie-technieken mogen geen risico's inhouden voor onbevoegde ontsluiering.
- De juiste identiteit van de betrokken zend- en ontvangstpunten bij het opzetten van een verbinding met de centrale databank dient verzekerd te zijn (terugbelsystemen, terminal identificatie).
- Gegevens over wie wat in bezit heeft of heeft gehad moeten worden vastgelegd (=>*logboek*).

[34]In chipcard context ook bekend als: "zorgprofessional kaart".

En als laatst t.a.v. het bevoegdheidsprofiel:

V.

- De houder dient een procedure vast te leggen voor het verstrekken, uitvoeren en controleren van de toegang tot, en het gebruik van, de persoonsregistratie. Gewaarborgd dient te zijn, zowel in de organisatie als in de geautomatiseerde voorzieningen, dat de toegekende bevoegdheid volledig en juist in de toegangscontrole is geïmplementeerd. De houder moet vast kunnen stellen of de vereiste toegangscontrole effectief functioneert.
- Een bevoegdheidsprofiel dient zo nauwkeurig mogelijk te worden samengesteld en op een minimale verzameling van bevoegdheden betrekking hebben. Bij ontslag, vertrek, wijziging van functie of bij verlies van bevoegdheid om andere redenen moeten de bevoegdheden aan de functionaris met onmiddellijke ingang worden ontnomen.
- Van personeel van derden dient voor het definiëren van bevoegdheden dezelfde procedure als voor het eigen personeel te worden toegepast.
- Alle toegekende bevoegdheidsprofielen dienen per persoon schriftelijk te zijn vastgelegd.
- Iedere werknemer die een bevoegdheidsprofiel krijgt toegewezen dient een aparte geheimhoudingsverklaring te ondertekenen. Disciplinaire maatregelen dienen te worden opgesteld voor nalatigheid en schending van de geheimhoudingsplicht. Voor personeel van derden dient de geheimhouding contractueel te worden vastgelegd.
- Een bevoegdheidsprofiel is slechts geldig voor een van tevoren vastgestelde periode. Vervolgens kan, indien nodig, opnieuw een bevoegdheidsprofiel worden toegekend. Op basis van het bevoegdheidsprofiel en de vastlegging van het gebruik kan de betreffende persoon achteraf verantwoordelijk worden gesteld voor het gebruik dat is gemaakt van het bevoegdheidsprofiel (=>*logboek*).

Daar wil ik zelf aan toevoegen:

Ad. III. -Domme terminals

Met ‘domme’ terminals[35] zonder diskettestation is de kans op lekken (en virussen) aanzienlijk kleiner dan bij pc’s met harddisk, knip en plakfuncties, en diskettestation (zie verder “Gebruikers - Inleveren op functionaliteit”)

-Het Printen van gegevens

De mogelijkheid tot uitprinten van gegevens moet worden beperkt. Het mag niet zo zijn dat hierdoor een oncontroleerbaar aantal kopieën ontstaat. Er kan gedacht worden aan het beperken van de mogelijkheid tot bepaalde personen of functies, en aan een beperkt aantal kopieën welke na een bepaalde tijd moeten worden vernietigd[36]. Wanneer door wie welke uitdraai is gemaakt kan worden vastgelegd in een logboek. Ook kan de naam van de gebruiker die de printopdracht gaf worden afgedrukt op elke uitdraai.

Ad. IV. Alhoewel de Privacy Enhancing Technologies (PET), die gericht zijn op het zoveel mogelijk ontkoppelen van de identiteit van de geregistreerde van de rest van de aanwezige gegevens, voor de *direct bij de behandeling betrokkenen* van ondergeschikte betekenis zijn[37], kunnen zij voor ‘tussenliggende trajecten’ wel van betekenis zijn. Bij een aantal algemene administratieve handelingen is deze ontkoppeling eveneens goed mogelijk.

---

[35]Of een ‘moderne variant’ ervan: de netcomputer.

[36]Een dergelijke methode past goed in het systeem waarin wordt gestreeftd naar een uiteindelijk geheel geautomatiseerde werkwijze.

[37]Voor de meeste direct bij de behandeling betrokkenen is de persoon en identiteit van de geregistreerde namelijk van direct belang. Voor bijvoorbeeld een laborant is de naam van een patient echter van gering belang, hier zou deze dan ontkoppeld kunnen worden van de wel benodigde gegevens.

2. Acceptatie

2.1 Toestemming

Patiënt
Slechts acceptatie van het systeem door de geregistreerden zal resulteren in de voor het gebruik van de gegevens in het GEDP benodigde toestemming[38]. Het verdient aanbeveling elke toestemming, evenals die voor de behandelingsovereenkomst, steeds expliciet schriftelijk vast te leggen. De instelling kan de toestemming van de patiënt dan zo nodig aantonen.
Toestemming voor het gebruik van gegevens kan worden gesplitst[39] in:

- toestemming voor de opslag van nieuwe gegevens in het GEPD voor gebruik tijdens de huidige behandeling
- toestemming voor de opslag van gegevens in het (archief van het) GEPD voor gebruik tijdens een mogelijke volgende behandeling
- toestemming voor het gebruik van, tijdens een eerdere behandeling vastgelegde, gegevens uit het (archief van het) GEPD tijdens de huidige behandeling

Om zo veel mogelijk voorwaarden voor een vrije keus te creëren moet de toestemming voor het gebruik van gegevens losgekoppeld worden van de rest van de behandelovereenkomst. M.a.w. geen algemene voorwaarde daarvan vormen.
Overleg met patiëntenorganisaties in de ontwerpfase leidt waarschijnlijk tot een snellere acceptatie. Ook de Registratiekamer hecht veel waarde aan een dergelijk overleg.
Toestemming kan slechts worden verkregen na uitgebreide voorlichting. Transparantie van het systeem is noodzakelijk voor de rechtsgeldigheid van de toestemming. Er kan gedacht worden aan een folder waarin ook het reglement is opgenomen. Het is echter zaak dat de informatie op een voor de patiënt begrijpelijke wijze wordt gepresenteerd. In de folder kan eveneens het contact adres van de houder, de adressen van de deelnemende instellingen, de ‘privacyfunctionaris’(zie verderop) e.d. worden aangegeven.
Mocht de patiënt desondanks toestemming weigeren dan zal er een alternatief traject, bijvoorbeeld het oude papieren traject, moeten worden gevolgd. Geen toestemming mag niet betekenen niet behandelen, zelfs als de patiënt wil dat zijn gegevens in het geheel niet worden vastgelegd of direct weer worden vernietigd zal deze wens moeten worden gerespecteerd.

Anderen
Wanneer informatie door anderen zelf wordt gegeven verdient het aanbeveling:

- Deze ander duidelijk te maken hoe deze informatie zal worden gebruikt (bijvoorbeeld mogelijkerwijs bij een nieuwe behandeling).
- Ook deze ander schriftelijk om toestemming te vragen.

[38] *Terzijde:* Het ligt in de rede dat wanneer de patiënt vertegenwoordigd kan worden t.a.v. beslissingen omtrent het behandelplan deze vertegenwoordiging *dan* ook kan plaatsvinden t.a.v. de toestemming i.d.z.v. art. 457 WGBO.

[39] Op deze wijze kan de patient bijvoorbeeld aangeven dat zijn gegevens slechts voor de huidige behandeling mogen worden gebruikt.

2.2 Gebruikers

Inleveren op functionaliteit
Ook al biedt de technologie talloze aanlokkende mogelijkheden, onder druk van privacy zal aan gebruiksgemak moeten worden ingeleverd. Knippen & plakken en integratie van verschillende toepassingen[40] zodat ze kunnen werken 'op' dezelfde informatie zijn wellicht heel handig, toch brengen deze mogelijkheden grote risico's met zich mee. Jammer genoeg zijn dergelijke voorzieningen vaak een essentieel onderdeel van de implementatiestrategie. Hiermee worden 'twijfelende' hulpverleners over de streep getrokken.
Ook is het privacybelang hier strijdig met het efficiency doel. Het privacybelang verhindert immers een mogelijkheid om sneller te werken.

Gevolgen systeem zonder waarborgen exclusiviteit
Wanneer privacy beschermende maatregelen dergelijk functionaliteitsverlies veroorzaken of op een andere manier moeilijk te verwezenlijken zijn, is het altijd goed voor ogen te houden wat de consequenties zouden zijn wanneer het systeem zonder deze maatregelen in gebruik zou worden genomen. Zo zouden bijvoorbeeld knip & plak functies gegevens makkelijk kunnen onttrekken aan de zorgvuldig ontworpen autorisatiestructuur. De gegevens kunnen dan zonder limiet worden geprint en verstrekt[41]. Het toekennen van 'behandelinitiatie' bevoegdheid aan iemand die ook grote gegevensinhoudelijke bevoegdheden heeft (hoofdbehandelaar) leidt tot toegang tot vrijwel alle (in het GEPD archief) aanwezige informatie van alle (ex) GGz patiënten. Het blijven gebruiken van statische zelfverzonnen wachtwoorden brengt het gevaar met zich mee dat iemand anders zich relatief eenvoudig voor de in de vorige zin bedoelde persoon kan uitgeven. Het niet afhankelijk maken van bevoegdheden van behandelrelatie resulteert in toegang tot alle (aanwezige) patiënten. Enzovoort.

Privacybewustzijn
Ook al worden er verschillende privacy beschermende mogelijkheden in het systeem geïmplementeerd, de daadwerkelijke bescherming staat of valt met de houding van de gebruikers. Zij zullen immers gebruik maken van het systeem en zullen deze mogelijkheden moeten benutten. Iedereen die werkt met het GEDP moet een uitgebreide toelichting op de maatregelen voor beveiliging hebben gehad. Slechts personen die kennis hebben van de maatregelen voor beveiliging zijn bevoegd bewerkingen uit te voeren. De toelichting kan het belang van de afschermingsmaatregelen benadrukken[42] en daarmee acceptatie stimuleren.

Bij de acceptatie van het systeem door de betrokken hulpverleners kan het volgende worden opgemerkt:
Elke hulpverlener heeft een individuele actieve zorgplicht t.a.v. de geheimhouding van de aan hem, in het kader van een behandeling, toevertrouwde gegevens. Wanneer de hulpverlener het systeem wat dat betreft niet vertrouwd mag hij dergelijke gegevens er niet aan blootstellen. Een dergelijke pat stelling kan slechts worden doorbroken door het vertrouwen van de hulpverlener in die bescherming te winnen. Hierbij zal hij voor ogen moeten houden dat hij een afweging zal moeten maken tussen het systeem, en het papieren traject *zoals dat zou moeten zijn*. Het papieren traject valt onder de nieuwe wet bescherming persoonsgegevens maar ook, nu al, onder de WPR[43]. Informatie technologie biedt verdergaande mogelijkheden om gegevens af te grendelen. Wanneer hij informatie met andere hulpverleners wil delen zal hij dat slechts via het papieren traject mogen doen wanneer dat voldoende waarborgen biedt. Vast staat dat de *huidige* papieren werkwijze en bijvoorbeeld de fax in dat opzicht ook niet voldoen. Wat dat betreft is het papieren traject *zoals dat zou moeten zijn* niet te vergelijken met het huidige papieren traject.

---

[40]Met knippen en plakken wordt bedoelt de functionaliteit van een operating systeem om in of tussen applicaties gegevens uit te wisselen d.m.v. copie. In geïntegreerde programmaomgevingen (bijv. Corel Perfect Suite) is dit eveneens, maar ook op andere manieren mogelijk.

[41]"Patientendossiers worden gefaxt en *ge E-maild* dat het een lieve lust is." Bruyn, G.A.W., Informatietechnologie. *Een potentiele bron van conflicten voor de arts- patiëntrelatie.* Medisch Contact, jaargang 51, 17 mei 1996, blz.682.

[42]Niet alleen voor privacybescherming maar ook voor kwaliteitsbewaking.

[43]Dat de huidige dossiers niet onder de WPR vallen is een wijdverbreid misverstand.

3. Overige aandachtspunten

3.1 Bewaartermijn

Aansluitend op de *kwaliteit van de gegevens* en het *logboek* kan over het bewaren van gegevens worden opgemerkt dat

- de WGBO voorschrijft dat medische gegevens in den regel[44] slechts bewaard worden gedurende een periode van tien jaren te rekenen vanaf het tijdstip waarop ze zijn vervaardigd.

- het besluit patiëntendossier BOPZ voorschrijft dat “de bescheiden bedoeld in het eerste en tweede lid”[45] in den regel[46] worden bewaard gedurende vijf jaren te rekenenen vanaf het tijdstip waarop de BOPZ behandeling is beëindigd.

Er zijn dus in principe twee verschillen:

I. Termijn: WGBO gegevens worden in den regel 10 jaar bewaard, BOPZ gegevens in ieder geval 5 jaar.

II. Ingang termijn: bij WGBO gegevens begint de termijn wanneer ze zijn vervaardigd, bij BOPZ gegevens wanneer de BOPZ behandeling is beëindigd.

Om praktische redenen is besloten voor de ingang van de termijn van WGBO-gegevens eveneens het tijdstip waarop de behandeling wordt beëindigd te gebruiken.

Voor het systeem zal dus van elk gegeven duidelijk moeten zijn of het in het kader van BOPZ of van WGBO is verzameld. Zodat een ‘opschoningsmechanisme’ hier rekening mee kan houden.

-Anonimiseren van gegevens
NB. Het anonimiseren van gegevens is lastiger dan het verwijderen van naam en adres. Gegevens mogen redelijkerwijs niet meer tot een persoon herleidbaar zijn. Het onherleidbaar zijn van een gegeven wordt niet licht aangenomen.

3.2 Beperkingen inzagerecht

Werkaantekeningen
Dit aspect is eveneens van belang wanneer het gaat om het inzagerecht van de patiënt. Dat strekt zich namelijk niet uit tot de werkaantekeningen van de hulpverlener. Mocht GEPD-programmatuur een werkaantekeningen-voorziening behelzen dan dient deze *desgewenst* van inzage door de patiënt te kunnen worden afgeschermd. Naar hun aard mogen die werkaantekeningen *alleen* door de auteur worden ingezien. Opgemerkt dient wel te worden dat de wetgever bij werkaantekeningen eerder een notitieblok voor ogen had dan een aan het dossier gekoppelde, in een databank vastgelegde file. De verleiding zou kunnen bestaan aantekeningen in dat 'veld' te

---

[44]Of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit.

[45]De normale medische gegevens die in het kader van een BOPZ behandeling worden gegenereerd vallen ook onder de vijf jaar termijn. Immers in lid 3 van artikel 2 Besluit patientendossier BOPZ wordt verwezen naar lid 1 en 2 waarin naast specifieke BOPZ gegevens (zoals die genoemd worden in de wet BOPZ zelf, of adviezen en aantekeningen als bedoel in art.509o, tweede lid, Wetboek van Strafvordering) ook “de overige gegevens omtrent de gezondheid van de patient en te diens aanzien uitgevoerde verrichtingen, een en ander voor zover dit voor een goede hulpverlening aan hem noodzakelijk is” worden genoemd. De ratio van deze *specifieke* regeling ligt wellicht in het feit dat het gaat om een gedwongen behandeling, er is geen sprake van een behandelings*overeenkomst*.

[46]Of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit.

gaan onderbrengen die er niet thuishoren. Dat is iets om bij stil te staan wanneer wordt overwogen een dergelijke functie te implementeren. Aan de andere kant behoudt een hulpverlener natuurlijk zijn eigen verantwoordelijkheid.

Wersch, P.J.M. van, *Inzagerecht en bewaartermijnen.* Medisch contact, nummer 43, 25 oktober 1991, blz 1291-1292: "De persoonlijke werkaantekeningen van de hulpverlener maken geen deel uit van het patiëntendossier, waarover het inzagerecht zich uitstrekt. Maar wat zijn nu precies 'persoonlijke werkaantekeningen'? Door sommigen wordt dit begrip zo ruim uitgelegd dat een groot deel van het dossier als persoonlijke werkaantekeningen wordt beschouwd. Dat is in elk geval niet de bedoeling. In het Memorie van Toelichting wordt dit begrip als volgt omschreven: 'In de praktijk plegen hulpverleners, naast de voor een goede hulpverlening noodzakelijke aantekeningen van de geneeskundige gegevens omtrent de patiënt, werkaantekeningen te maken welke dienen als geheugensteun voor de eigen gedachtevorming. Bij deze zogenoemde persoonlijke werkaantekeningen gaat het niet om het aantekenen van gegevens, maar van indrukken, vermoedens, of vragen die bij de hulpverlener leven.' Of met deze omschrijving alle verwarring is opgelost valt te betwijfelen. In sommige rechterlijke uitspraken, waarin ook over de rijkwijdte van dit begrip wordt gestreden, zijn persoonlijke werkaantekeningen gelijkgesteld met strikt subjectieve meningen van de hulpverlener. Het criterium 'al of niet subjectief' lijkt mij niet juist en evenmin is naar mijn mening beslissend of het gaat om 'indrukken, vermoedens of vragen die bij de hulpverlener leven'. Beslissend lijkt mij of de werkaantekeningen inderdaad uitsluitend voor persoonlijk gebruik zijn bestemd, dat wil zeggen niet bedoeld om onder ogen van derden te komen. Zodra de hulpverlener die aantekeningen ter inzage geeft aan anderen of de inhoud daarvan mondeling mededeelt, bijvoorbeeld in een teambespreking, gaat het niet langer om *persoonlijke* werkaantekeningen."

Dat er een spanning bestaat tussen het inzagerecht en werkaantekeningen, en dat daardoor de aard van de werkaantekeningen van belang wordt blijkt uit het volgende: Vencken, L.M., *Werkaantekeningen en de WGBO. Een tegenstrijdigheid in de wet.* Medisch Contact, nummer 46, 18 november 1994: "De hulpverlener heeft de plicht de patiënt te informeren over wat hij als behandelaar van plan is en waarom hij dat zo wil doen. Dus moet hij de patiënt ook inlichten over de diagnose en wat daarmee samenhangt. Werkaantekeningen kunnen daarbij van groot belang zijn: ze horen bij wat de patiënt volgens de wet 'redelijkerwijs' dient te weten".

Privacy van een ander

Een andere uitzondering op het inzagerecht is de privacy van derden. Dat is de belangrijkste[47] beperking op het inzagerecht. Inzage mag immers niet worden verleend 'voor zover dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander'. "Hier kan sprake zijn van een botsing van het recht op privacy van de patiënt met hetzelfde recht van een ander. Wiens recht gaat dan voor? In de Memorie van Toelichting wordt hierover opgemerkt: 'Indien kan worden voorzien dat verstrekking van inzage of afschrift van bepaalde gegevens aan de patiënt de persoonlijke levenssfeer van een ander zou schaden, en diens belang een overwegend karakter heeft, dient de hulpverlener de verstrekking achterwege te laten'. Dus het feit, dat sommige in het dossier vermelde gegevens over de patiënt afkomstig zijn van derden of dat het dossier ook informatie over derden bevat, is op zichzelf niet voldoende om inzage te weigeren. De persoonlijke levenssfeer van die derde moet daardoor worden geschaad en het belang van die derde bij de bescherming van zijn privacy moet een overwegend karakter hebben, dat wil zeggen zwaarder wegen. Het zal voor een hulpverlener in de praktijk niet altijd eenvoudig zijn deze belangenafweging te maken."[48]

[47]Wersch, P.J.M. van, *Inzagerecht en bewaartermijnen.* Medisch contact, nummer 43, 25 oktober 1991, blz 1291-1292.

[48] Ibid.

3.3 Organisatorische indeling

Voor de WPR, de WGBO en een aantal kwaliteitswetten op het gebied van de Gezondheidszorg is eveneens de organisatorische indeling van belang. Zijn de deelnemende instellingen gefuseerd of blijven zij autonoom 'los van elkaar' bestaan. Zo is bij de WPR van belang of een instelling houder is, maar ook of zij wellicht voor een andere instelling bewerker wordt. Een instelling die bewerker is voor een andere instelling mag bijvoorbeeld niet enkel en alleen op grond hiervan inhoudelijke toegang tot deze gegevens hebben.
De programmatuur voor een GEPD zal met deze verschillende organisatorische indelingen overweg moeten kunnen. Deze indeling kan duidelijk haar weerslag hebben op de bevoegdheidsprofielen en andere autorisatieaspecten.

3.4 Functionaris Privacybescherming

Het is te overwegen in elke instelling een onafhankelijk persoon[49] aan te stellen die in de dagelijkse praktijk toezicht houdt op de naleving van de privacyvoorschriften. Wellicht kan hij daarvoor onder meer gebruik maken van zojuist genoemd logboek. Het is van belang dat het een voor geregistreerden laagdrempelige voorziening is. Deze functionaris zou deze taak krijgen náást de verantwoordelijkheid die eenieder t.a.v. de privacy heeft en degenen die op grond van hun bevoegdheden normaliter een toezichthoudende functie hebben.

3.5 ‘Oude’ gegevens

Het verdient aanbeveling oude gegevens[50] pas na expliciete toestemming van de patiënt, bij voorkeur pas wanneer sprake is van een nieuwe behandelovereenkomst, op te nemen in het (archief van het) GEDP.

[49]Helmer,F.M.M., *Patiëntenrechten in de praktijk. Het belang van centrale coördinatie bij de effectuering van direct toepasbare patiëntrechten in een ziekenhuis.* Medisch Contact jaargang 49 nummer 18, 1994, blz.614-616.

[50]D.w.z. vroeger, voor het bestaan van het GEPD, vastgelegde gegevens.

3.6 Interchange agreement

Er moeten afspraken worden gemaakt over onder welke voorwaarden gegevens aan elkaar worden verstrekt. R. van Esch heeft de karakteristieke elementen van dergelijke afspraken in de (handels) EDI sfeer onderzocht en beschreven in: *"Interchange Agreements.* The EDI Law Review 1. Kluwer, 1941, pp. 3-41." Voor het GEDP zullen een groot aantal gelijksoortige afspraken gemaakt moeten worden.
Zeker bij de decentrale variant uit het eindrapport bestaan die afspraken in de vorm van een 'Uitwisselings overeenkomst', gevormd door een contract en appendices (met daarin technische specifiteiten) als integraal onderdeel van de overeenkomst.
Basisafspraak moet zijn dat elk (evt.autonoom) systeem bij iedere deelnemende instelling voldoet aan de voorschriften uit WGBO en WPR. Een secundaire voorwaarde moet o.a. zijn dat bij het overzetten van gegevens naar een ander systeem het oorspronkelijke beschermingsniveau gehandhaafd blijft. Ook zal een verstrekkende partij contractueel gebonden moeten worden rectificaties door te geven. Verder onderscheidt van Esch *in de overeenkomst* o.a.:

* technische aspecten
  - -type/standaard berichten (i.c. verstrekkingen)
  - -hardware
  - -software
  - -communicatie protocollen
  - -communicatie netwerken
  - -value added services
* beveiligings aspecten[51]
  - -bescherming van het systeem
    - o.a. er zou kunnen worden bepaald dat de beveiligingsaspecten van het systeem regelmatig door een derde partij zou kunnen worden gecontroleerd
  - -bescherming van het bericht
    - -maatregelen om de afkomst van een bericht (ook een verzoek) vast te stellen
    - -maatregelen om de integriteit van een bericht vast te stellen
    - -maatregelen om het verloren gaan van een bericht vast te stellen
    - -maatregelen om het 'afdwalen' van een bericht vast te stellen
  - -bescherming van de uitwisselingsprocedure
* juridische aspecten
  - -verantwoordelijkheid van de zender
  - -ontvangstbevestiging
  - -bewijs
  - -aansprakelijkheid
    - -aansprakelijkheid voor fouten in de overdracht
    - -risicoverdeling

[51]De kwaliteit van de bescherming wordt bepaald door de zwakste schakel in de ketting.

3.7 Correctierecht

De geregistreerde moet het hem in de WPR[52] toegekende correctierecht kunnen uitoefenen. Al eerder werd aangegeven dat het logboek daarom moest bijhouden aan welke derden gegevens zijn verstrekt. Deze moeten daarvan op de hoogte worden gesteld[53]. Bij de manier waarop gegevens worden opgeslagen en mogelijkerwijs worden hergebruikt zal hier rekening mee moeten houden. Correctie kan worden onderscheiden van verschil van inzicht (tussen bijvoorbeeld arts en patiënt, hiervan kan een aantekening worden toegevoegd) of van veranderd inzicht (een arts denkt later wat anders). Correctie van gegevens gaat in eerste instantie om het verbeteren van feitelijk onjuiste gegevens.
De correctie moet op alle plaatsen worden doorgevoerd. Het mag niet zo zijn dat de foute gegevens later weer 'als zijnde waar' opduiken. Daarbij kan het best worden aangegeven dat deze informatie op grond van het correctierecht is gewijzigd, later kan men zo, hierdoor geattendeerd, met behulp van het historisch archief nog nagaan dat en welke informatie op dat tijdstip voorhanden was (bijv. i.v.m. aansprakelijkheid).

3.8 Verschillende verstrekkingspolitiek

De verschillende typen van het REMD genoemd in het eindrapport zijn niet alleen verschillend in de manier waarop ze worden ingericht (centraal en decentraal), maar ook qua verstrekkingspolitiek. Bij de centrale variant is het aantal verstrekkingen aan deelnemende instellingen waarschijnlijk vele malen groter dan bij de decentrale variant. Bij de centrale variant werken de instellingen functioneel gezien met dezelfde databank (gedistribueerde databank). Elk gebruik van het EMD betekend automatisch het gebruik van het R-EMD.
Bij de decentrale variant gebruiken de instellingen hun eigen EMD, slechts om gegevens uit andere instellingen op te vragen maakt men gebruik van de regionale infrastructuur. De aard van de verstrekking is afhankelijk van de opvrager (functie/hoedanigheid enz.).

3.9 Standaardisatie

Met de ontwikkeling van GEPD's worden "standaardisatie" en "open infrastructuur" vaak in een adem genoemd. Privacymarkeringen zullen ook bij standaardisatie moeten worden betrokken. Het mag niet zo zijn dat gegevens, prima beschermd binnen het ene EPD, door verstrekking aan een ander EPD opeens aan bescherming verliezen. Dat risico is wel aanwezig: ze worden immers buiten de eerste autorisatiestructuur gebracht.

3.10 Ontbreken privacy-standaardisatie en verstrekkingspolitiek

Bij het ontbreken van dergelijke privacy standaardisatie zal de keus die wordt gemaakt tussen een centraal of een decentraal opgezet GEPD, naast de manier van inrichten andere gevolgen met zich mee brengen.
Wanneer men kiest voor een decentraal opgezet GEPD kiest men eveneens voor het buiten de oorspronkelijke autorisatiestructuur brengen van informatie. Als gevolg hiervan kan men slechts zeer gericht verstrekken[54], men kan niet meer gegevens 'alvast voor mogelijk toekomstige ontsluiting' mee verstrekken zoals dat bij een centraal opgezet GEPD gebeurt. Immers bevoegdheden ten opzichte van die informatie zouden weer helemaal opnieuw moeten worden gedefinieerd.

---

[52]Artikel 31 WPR.

[53]Artikel 35 WPR.

[54]Op grond van die aspecten uit het bevoegdheidsprofiel van de aanvrager die bij de verstrekkende instelling bekend zijn.

Bijlage

Figuur 1.

-D en E.

In de tekening: -wordt dat gevisualiseerd doordat de zwarte inzage staaf zowel onder de roodgestippelde normlijn blijft, als onder gele autorisatielijn. Verder lopen de normlijn en de autorisatielijn gelijk.

Voorbeeld: Bij situatie D zou een opererend chirurg kunnen passen die het dossier inziet van een patiënt die voor het eerst in het ziekenhuis wordt opgenomen op de dagbehandeling. Mogelijkheid tot kennisname van de gehele dossierinhoud was noodzakelijk voor de door hem te verrichten werkzaamheden in het kader van die behandelovereenkomst. De daadwerkelijke inzage strekte zich echter niet uit tot het gehele dossier.

-A en B.

In de tekening: de zwarte inzage staaf wordt doorsneden door de roodgestippelde normlijn.. De inzage wordt echter totaal niet '*afgesneden*' door de autorisatielijn.

Voorbeeld: In situatie A leest een nachtverpleegkundige, benieuwd naar de enkele jaren geleden aangebrachte cosmetische aanpassingen van een patiënt, verder dan noodzakelijk voor de door haar te verrichten werkzaamheden; ze had het klinisch dossier toch bij de hand voor het maken van een uittreksel t.b.v. het verpleegkundig dossier. Alhoewel ze best nog verder had willen lezen voor welke complicaties de lekkende prothesen zorgden, leest ze niet verder omdat ze wordt opgeroepen.

-C.

In de tekening: de zwarte inzage staaf loopt onder de roodgestippelde normlijn. De inzage wordt niet '*afgesneden*' door de autorisatielijn. Normlijn en autorisatielijn lopen echter niet gelijk: de normlijn ligt onder de autorisatielijn.

Voorbeeld: Bij situatie C ziet een anesthesist het klinisch dossier in van iemand die al meerdere malen met zeer uiteenlopende klachten is opgenomen in het ziekenhuis en nu door hem wordt bewaakt tijdens de operatie. Hoewel hij voor zijn behandeling meer had mogen zien beperkt hij zich tot hetgeen hij op dat moment nodig acht. Wanneer hij had gewild had hij het gehele dossier kunnen inzien.

-F.

In de tekening: de roodgestippelde normlijn doorsnijdt de zwarte inzagepoging bij de wortel. De gele autorisatielijn echter blijft boven deze zwarte inzage staaf.

Voorbeeld: Een man ziet na het bezoekuur in een kar op de gang het dossier van zijn huisarts. Nieuwsgierig naar de ernst van zijn ziekte kan hij het niet nalaten het dossier door te bladeren.

-H.

In de tekening: de gele autorisatielijn loop samen met de rode normlijn. Ze snijden de inzage poging bij de wortel af.

Voorbeeld: Situatie H zou de poging van een bezoeker kunnen schetsen om in de onbewaakte avonduren een dossier van zijn ex-vriendin te bemachtigen. Doordat de deur van het centraal archief op slot zit strand deze poging. De norm verbood elke inzage. De geboden autorisatiebescherming was dit maal adequaat.

-G.

In de tekening: de gele autorisatielijn ligt *onder* de rode normlijn.