EERSTELIJNINCIJFERS

Juridische en organisatorische aspecten van het gebruik van medische persoonsgegevens voor Eerste Lijn in Cijfers

Hugo de Vos

April 2012 final version

Voswiz
Innovation in place

proigia
improving health care through information

JURIDISCHE EN ORGANISATORISCHE ASPECTEN VAN HET GEBRUIK VAN MEDISCHE PERSOONSGEGEVENS VOOR EERSTE LIJN IN CIJFERS

Een visiedocument over de verwerking van behandelgegevens in de Eerstelijnsgezondheidszorg

In opdracht van Eerste Lijn in Cijfers en Proigia BV

Voswiz
Ooststeeg 105
6708 AT Wageningen
hdevos@voswiz.nl

Juridische en organisatorische aspecten van het gebruik van medische persoonsgegevens voor Eerste Lijn in Cijfers

H. de Vos

Inhoudsopgave

Juridische en organisatorische aspecten van het gebruik van medische persoonsgegevens voor Eerste Lijn in Cijfers

1 Introductie

Huisartsen realiseren zich dat zij over een grote hoeveelheid behandelgegevens beschikken die de basis kunnen vormen voor analyses gericht op verbeteringen op het gebied van zorgkwaliteit, voor de ontwikkeling van zorgprogramma's, voor transparantie bij zorgverlening, alsook voor belangenbehartiging en wetenschappelijk onderzoek.

De dynamische ontwikkeling van de huisartsenzorg vraagt om geïnformeerde professionals die kunnen reflecteren op de eigen inhoudelijke zorg en op basis daarvan zorg kunnen verbeteren en beleid kunnen formuleren. Huisartsen, gezondheidscentra en zorggroepen krijgen steeds vaker een coördinerende functie (regie in de zorg). Overheid en toezichthouders stellen specifieke eisen aan administratieve informatiesystemen van huisartsen om verantwoording over de geleverde zorg (prestatie-indicatoren) beter mogelijk te maken. Beroepsverenigingen vragen accreditatie-informatie. En ook voor de onderhandelingen met de zorgverzekeraar is transparantie noodzakelijk.

Door deze verschillende ontwikkelingen neemt de informatiebehoefte in de eerstelijnsgeneeskunde sterk toe en wordt deze tevens complexer. In september 2011 hebben een aantal huisartsen en gezondheidscentra zich verenigd om gezamenlijk een ondersteunende dienst voor informatieverzameling en -analyse op te zetten onder beheer en verantwoording van de zorgverleners: "Eerste Lijn in Cijfers" (EIC)

Doelstellingen van de vereniging zijn:

1. Het in opdracht van zorgprofessionals beheren van een eerstelijns dataserver ter bevordering van kwalitatief hoogwaardige eerstelijns zorg,
2. Het ondersteunen van huisartsen, zorggroepen en gezondheidscentra (en eventueel andere zorgverleners) met management informatie functionaliteit die geheel blijft vallen onder het beheer van de aangesloten zorgverleners
3. Het faciliteren van de innovatie en doorontwikkeling van managementinformatiesystemen van de vereniging ten behoeve van haar leden
4. Het verrijken van deze data met externe gegevens en referentie gegevens (ondermeer ten behoeve van benchmarking)
5. Het kunnen verzorgen van rapportages waarmee belangenbehartigers in de eerste lijn (LHV/LVG, e.a.) en wetenschappelijk onderzoeksinstituten kunnen worden voorzien van informatie over ontwikkelingen in de zorgverlening.

Het EIC wil de eerstelijnsgegevens (nu HIS-data, maar op termijn ook andere gegevens) laten uitspoelen naar een centrale server. Deze data zijn (net als in een HIS) zo georganiseerd dat alleen zorgverleners de eigen praktijkdata op individueel niveau kunnen inzien en/of (laten) bewerken. De server die EIC onder haar beheer heeft is in deze zin niets anders dan een verlengde van het eigenlijke behandeldossier, en deze informatie is hier onder de controle van de zorgverlener

beschikbaar voor monitoring en kwaliteitsborging van zorg en voor het verschaffen van management aan praktijkhouders. Naast de data op praktijkniveau wil EIC voor praktijken mogelijk maken om met gegevens op geaggregeerd niveau (data op gemiddelden en indicator niveau) deel te nemen aan een onderlinge benchmark. Deze database die toegankelijk moet zijn voor deelnemers aan de benchmark bevat nooit gegevens op individueel patiënt niveau.

Het doel[1] van de gegevensverwerking door de leden van het EIC is het toevoegen van waarde aan de zorgverlening in de eerstelijn voor zowel patiënten als voor de direct bij een behandeling betrokken zorgverleners door:

1. Identificatie en monitoring van verschillende patiëntengroepen ter verbetering van de geleverde zorg (zowel zorginhoudelijk als bedrijfstechnisch), voor inzichtelijk maken van informatie met betrekking tot de eigen behandelpraktijk, voor interne scholing en kwaliteitsbevordering (zoals voorschrijfgedrag en verwijzingen)
2. Het vergelijken van bovenstaande informatie op geaggregeerd niveau tussen praktijken en/of zorggroepen (benchmarken voor kwaliteitsverbetering).
3. De publieke transparantie in de zorg te verbeteren door het als zorgverlener zelf op een betrouwbare manier kunnen presenteren van kwaliteitsindicatoren.
4. Eigen verantwoordingsinformatie te genereren voor externe private veldpartijen zoals de verzekeraars of subsidiegevers in het kader van bv. de GEZ gelden.
5. Beleidsrelevante rapportages te genereren betreffende efficiëntie van zorgproducten (zelf sturen op kosten-batenanalyses in plaats van alleen op kosten).
6. Het faciliteren van wetenschappelijk onderzoek met als doel de huisartsgeneeskunde op een "hoger plan" te brengen.

Omdat het hier gaat om medische persoonsgegevens moet de verwerking van deze behandelinformatie uiterst zorgvuldig plaatsvinden zodat voldaan wordt aan alle wettelijke privacy regels en voorschriften zoals die gelden voor uitwisseling, opslag en gebruik van deze bijzondere persoonsgegevens, zoals ook bij het HIS/bronsysteem het geval is. Op deze manier gelden de regels voor dossiervorming die gelden bij het HIS ook voor het EIC en moet de patiënt (net als bij het HIS) over het dossier en zijn rechten omtrent dit dossier worden geïnformeerd (zie verder 2.5). Een belangrijk uitgangspunt daarbij is dat moet worden gekozen voor een systeem waarbij de verwerking van behandelinformatie, in lijn met het medisch beroepsgeheim, blijft plaatsvinden onder de controle van de zorgverlener(s) die direct bij de behandeling betrokken is(zijn). Daarom moet bij oprichting en organisatie van het EIC in de praktijk vorm gegeven worden aan een systeem van informatieverwerking dat het minst ingrijpt op de privacy van patiënten en het beroepsgeheim van zorgverleners (subsidiariteit) en waarbij deze dataverwerking proportioneel is ten opzichte van haar doelen waarvoor deze informatie wordt gebruikt.

Op dit moment bestaan er verschillende ideeën voor het gebruiken van HIS gegevens voor bijvoorbeeld het verhogen van transparantie en leveren van stuurinformatie[2] (bv NIVEL, 2011; ZiZo, 2011; AGIS, 2010; Mondriaan 2010).

1 EIC i.o.Voorlopig Voorstel oprichting "Vereniging voor Kengetallen in de Eerste lijn" , juli 2011. Discussienotitie.
2 Zie bijvoorbeeld: NIVEL (2011) Haalbaarheidsstudie indicatoren huisartsenzorg en Etalage+-gegevens. Met NPA, Twynstra en Gudde en Medlaw consult. ; ZiZo (2011) Dataprotocol Chronische Zorg. Concept discussiestuk 15 juni 2011; AGIS (2010) Zorginkoopdocument 2a DiAgis, December 2010; pp10: 4.2.; Mondriaan (2011) The Mondriaan Project: The Dutch healthcare landscape as a

Veel voorstellen gaan uit van een centrale dataverzameling waarbij opslag, uitwisseling en gebruik plaats vindt buiten de controle en het beheer van professionals. De legitimiteit van een dergelijke opzet is uiterst problematisch omdat zo bij het gebruik van behandelinformatie niet kan worden toegezien op het vereiste van doelbinding. Dit probleem met betrekking tot de legitimiteit van de verwerking van behandelinformatie is bijzonder groot bij dataprojecten waarbij de doelstellingen van informatieverwerking in de planningsfase of achteraf worden opgerekt om tal van additionele gebruiksopties mogelijk te maken ("function creep"). Zo stelt: *Haalbaarheidsstudie indicatoren huisartsen zorg*" dat een optie voor een centrale database voor het genereren van kwaliteitsindicatoren interessant is voor "- nu wij toch gegevens verzamelen – *met name* wetenschappelijk onderzoek."[3]. In dit document spreekt het NIVEL echter terecht twijfels uit over de rechtmatigheid van deze mogelijkheid voor het additionele gebruik, als de bewerkingsgrond wordt opgerekt tot buiten het oorspronkelijke doel van de gegevensverzameling.

EIC meent dat het zelf analyseren van praktijkdata die al onder controle is en blijft van zorgverleners (in het HIS) een transparante en eenvoudige oplossing is waarmee tegemoet kan worden gekomen aan de toenemende vraag aan informatie voor sturing, verantwoording, kwaliteitsborging en een dynamische aanpassing van de zorgverlening. In feite is het EIC voor huisartsen een verlengde van het HIS. Door echter het EIC systeem niet in het HIS te bouwen wordt het mogelijk om: 1) direct zelf flexibel applicaties op de data te (laten) bouwen, 2) benchmarking met verschillende HISsen te doen en 3) op den duur geïntegreerde zorg van een zorginstelling of -traject als geheel te analyseren.

Praktisch heeft het systeem ook het voordeel dat professionals altijd toegang houden tot hun eigen data en niet afhankelijk zijn van onzekere goodwill arrangementen zoals bij "ruil van data voor rapporten". Het geeft de professionals in de verschillende segmenten van zorgverlening in de eerstelijn de mogelijkheid rapportages op te zetten en uit te voeren overeenkomstig criteria en wensen die passen bij de eigen praktijkvoeringen, dat is vaak uitest moeizaam in dataprojecten opgezet door externe partijen zoals commerciële IT partijen (zoals HISsen) en medische informatieprojecten die in ruil voor behandelinformatie vanuit hun informatiesysteem ook enige management informatie willen verschaffen aan zorgverleners. Rapporten van derde partijen geven vaak slechts een incidenteel beeld en geven de professionals een fragmentarisch inzicht en leiden vaak tot meer vragen, dan dat het de controle over datamanagement vergroot. Het in ruil voor behandelinformatie verstekken van management informatie aan praktijkhouders is soms ookmoeilijk en extra vragen worden niet of traag beantwoord. Door de controle bij de professionals te houden blijft ook de link naar de context en praktijk gegarandeerd wat van groot belang is voor interpretatie en gebruik van gegevens. Zo wordt een systeem opgezet dat de reflectie, het lerend vermogen en de nieuwsgierigheid van professionals verhoogd en dat direct aansluit op de vraag.

De door het EIC voorgestane werkwijze maakt het ook mogelijk om op legitieme wijze tegemoet te komen aan de vraag naar onderzoeksgegevens bij het NIVEL en academische centra omdat zorgverleners en hun patiënten gekend kunnen worden in het gebruik van behandelinformatie voor specifieke additionele doelstellingen.

'population laboratory'. *http://www.tipharma.com/projects/efficiency-analysis-drug-discovery-process/the-mondriaan-project.html*. en The Mondriaan Healthcare Data Repository, cornerstone of the population laboratory, projectvoorstel Value Creation Project TI Pharma, versie februari 2011.
3 NIVEL (2011):p 95.

Het voorliggende verslag is het resultaat van een studie voor EIC waarin door Proigia een juridisch-organisatorisch model is uitgewerkt dat de basis vormt voor de technisch-organisatorische opzet van een systeem voor de verwerking van behandelinformatie waarbij de controle over opslag, uitwisseling en gebruik blijft berusten bij zorgverleners die direct betrokken zijn bij een behandeling.

Het verslag gaat eerst in op de privacywetgeving en regels aangaande gegevensverwerking in de eerstelijn (2). Hierna zullen de consequenties voor het organisatiemodel van het EIC worden uitgewerkt. Tot slot zal een technische opzet worden gepresenteerd die voldoet aan criteria van zowel regelgeving als organisatorische inbedding (4). Aan het eind zal in de vorm van een aanbeveling een stappenplan worden gepresenteerd voor de organisatorische implementatie van het EIC (5).

2 Wettelijke basis bewerking van medische persoonsgegevens

Voor de omgang met de medische dossiers zijn met name een tweetal wetten van cruciaal belang. De Wet op de Geneeskundige BehandelOvereenkomst (WGBO) en de Wet Bescherming Persoonsgegevens (WBP). In deze wetten worden in samenhang de belangrijkste plichten en rechten voor van behandelaars en patiënten beschreven met betrekking tot de verwerking van behandelinformatie, onder verwijzing naar de administratief organisatorische context waarbinnen de behandeling plaatsvindt. Omdat het voor de vertrouwensrelatie tussen patiënt en zorgverlener van grote betekenis is voor een goede professionele zorgverlening wil het EIC met haar organisatiemodel voorzien in een ontwerp waarin zorgvuldige omgang met behandelinformatie, een zorgvuldige verwerking van de informatie die wordt gedeeld in de spreekkamer, vanaf het begin is ingebouwd. Naast de WBP en WGBO is ook de voorgestelde Wet clientenrechten (WCZ) voor Zorginstellingen relevant voor het systeemontwerp van het EIC[4].

Hieronder zullen eerst de belangrijkste wettelijke randvoorwaarden worden beschreven voor een legitiem systeem voor de verwerking van behandelgegevens zoals die beschikbaar zijn bij zorgverleners direct betrokken bij een behandeling. In de daarop volgende hoofdstukken zal verder worden uitgewerkt hoe rekening houdend met wettelijke randvoorwaarden, waaronder een zorgvuldige afweging met betrekking tot subsidiariteit en proportionaliteit, een model voor informatieverwerking kan worden geformuleerd dat het professionals mogelijk maakt de bij hen beschikbare dossierinformatie van individuele patiënten te kunnen inzetten voor verbetering van de zorgverlening in het organisatieverband waarbinnen zij werkzaam zijn.

In de wetgeving zijn een aantal uitgangspunten en beginselen vastgelegd die van belang zijn voor de zorgvuldige bewerking van data. De volgende concepten zijn van belang:

- de doelen van de dataverwerking
- criteria voor delen van gegevens met anderen dan de zorgverlener en toestemming voor de bewerking van data
- criteria voor delen van data voor wetenschap
- de verantwoordelijke voor het dossier in HIS en EIC
- de bewerker van data in ASP situaties

2.1 de Doelen van de bewerking

In de wet op de geneeskundige behandelovereenkomst (WBGO) staat ondermeer welke informatie met betrekking tot een behandeling door zorgverleners moet worden verzameld en opgenomen in de eigen praktijkadministratie. In deze wet is onder andere de verdeling van rechten en plichten tussen patiënt en behandelaar vastgelegd en worden een aantal specifieke regels gegeven voor de wijze waarop individuele hulpverlener geacht worden om te gaan met medische gegevens van patiënten.

In artikel 454 lid 1 van de WGBO staat dat de *hulpverlener (...) een dossier in(richt) met betrekking tot de behandeling van de patiënt. Hij houdt in het dossier aantekening van de gegevens over de gezondheid van de patiënt en de te diens aanzien uitgevoerde verrichtingen en neemt andere stukken, bevattende zodanige gegevens, daarin op, een en ander voor zover dit voor een goede hulpverlening aan hem noodzakelijk is.*

4 NIVEL (2011) pp 90 e.v.

De doelen van de dataverzameling zijn van cruciaal belang voor de WBGO en het WBP.. Het dossier dient primair de goede zorgverlening en de gegevens die worden verzameld moeten hiervoor noodzakelijk zijn en een grondslag hebben in de WGBO of het WBP. Volgens het KNMG vervult het dossier ook een aantal afgeleide functies zoals kwaliteitsbewaking, afleggen van verantwoording en (onder specifieke omstandigheden) wetenschappelijk onderzoek[5]. Onder welke omstandigheden het dossier voor wetenschappelijke doelen mag worden gebruikt wordt later besproken.

Naast de verwerking van behandelinformatie voor een goede zorgverlening is de verwerking van behandelinformatie voor een aantal andere doelstellingen vastgelegd in een aantal andere wetten:

- De Wet Marktordening Gezondheidszorg (WMG) (artikel 38 lid 4)
- De Kwaliteitswet op de zorginstellingen (KWZi) (artikel 5)

> *"Zorgaanbieders maken informatie openbaar over de eigenschappen van aangeboden prestaties en diensten, op een zodanige wijze dat deze gegevens voor consumenten gemakkelijk vergelijkbaar zijn. Deze informatie betreft in ieder geval de tarieven en de kwaliteit van de aangeboden prestaties en diensten." (WMG:38:4).*

Hiermee zijn zorgverleners verplicht tot openbare verantwoording van de geleverde zorg, zorginstellingen kunnen dit alleen goed doen als zij de bij hen beschikbare behandelinformatie analyseren en bewerken. Bij publicatie, openbaarmaking van de resultaten is alleen toegestaan als behandelgegevens op zodanige wijze zijn gegeneraliseerd (samengevat) dat informatie in de rapportage niet meer herleid kan worden tot individuele patiënten.

De invulling van een deel van de informatieverplichting kan worden afgeleid uit de KWZi, die "zorginstellingen" verplicht tot het leveren van een kwaliteitsjaarverslag. "Zorginstellingen" voor deze wet zijn beperkt tot Gezondheidscentra en Huisartsengroepen voor zover ze staan geregistreerd als groep met een AGB code. Voor individuele huisartsen geldt de Wet op de Beroepen in de Individuele Gezondheidszorg (BIG). De KNMG merkt echter op "*… artikel [40] ..vereist van deze artsen (of andere hulpverleners) een aantal inspanningen dat vrijwel identiek is aan de verplichtingen die uit de Kwaliteitswet voor de instellingen voortvloeien. Opvallend verschil met de Kwaliteitswet is dat de solistisch werkzame hulpverlener niet de plicht heeft een jaarverslag over het gevoerde kwaliteitsbeleid op te stellen*"[6]. Met nieuwe wetgeving zoals het Wetsvoorstel Cliëntenrecht Zorg (WCZ) wordt de wettelijke basis gelegd voor het verplicht opstellen van een kwaliteitsjaarverslag door alle zorgverleners in de eerstelijn[7].

De WMG stelt verder dat de NZa informatie over de kwaliteit van de zorg zelf openbaar kan maken, behalve als.. " *…anderen reeds in voldoende mate in openbaarmaking van de daar bedoelde informatie voorzien.*" (WMG: 38;sub 5). NZa heeft hiermee een "stok achter de deur" als de sector zelf niet regelt dat noodzakelijke informatie beschikbaar komt. De NZa zal uiteraard wel regels stellen aan de "informatievoorziening, bedoeld in het vierde lid, met het oog op de doeltreffendheid, juistheid, inzichtelijkheid en vergelijkbaarheid daarvan" (sub 7). NIVEL stelt voor dat belanghebbenden een keuze moeten maken voor een decentraal (zelf laten maken van indicatoren door behandelaars) of een centraal model (ZiZo of anderen zetten een centrale gegevensverwerking op via een

5 KNMG (2004) Van wet naar praktijk. Implementatie van de WGBO. Deel 3 Dossier en bewaartermijnen. Pp. 17-18.
6KNMG (1998) Arts en Wet BIG. pp 22
7 NIVEL (2011); p92.

TTP)[8]. Later (hoofdstuk 3) zullen we terugkomen op de keuze voor een centrale of decentrale datavoorziening. Het EIC kiest duidelijk voor een decentraal model, waarin professionals zelf data genereren en verantwoordelijk blijven voor het publiceren van de gegevens.

2.2 Verantwoordelijke voor dossiers

De Wet Bescherming Persoonsgegevens (WBP) definieert het begrip 'de verantwoordelijke' voor het verwerken van persoonsgegevens als: " *.. degene die bepaalt wat er met de gegevens gebeurt. Binnen een gezondheidsinstelling is de Directie of de Raad van Bestuur vaak de 'verantwoordelijke' in de zin van de WBP. Dit betekent dat die het beleid vaststelt voor beheer en instandhouding van het informatienetwerk en de gegevensbestanden. Ook de wijze van dossiervoering binnen een instelling valt hieronder. Onder dossiervoering wordt verstaan: het dossierbeheer vanaf het moment van vastlegging van de gegevens in het dossier tot het moment van vernietigen. De hulpverleners die binnen de instelling werkzaam zijn, zijn geen 'verantwoordelijke' in de zin van de WBP. Ze zijn echter wel verantwoordelijk voor en aanspreekbaar op de inhoud van het dossier en de gegevensverstrekking door of namens hen aan anderen."*[9]. In geval van zelfstandige hulpverleners is de hulpverlener wel meteen verantwoordelijke in de zin van het WBP.

De WBP legt aan de 'verantwoordelijke' een aantal plichten op.

De belangrijkste en hier relevante plichten zijn[10]:
• de informatieplicht: De 'verantwoordelijke' moet de patiënt van wie gegevens worden verwerkt ('de betrokkene') (ofwel zijn vertegenwoordiger) inlichten over wie de 'verantwoordelijke' is, het doel of de doelen van de gegevensverwerking, de wijze waarop de verwerking plaatsvindt en wie eventuele medegebruikers of ontvangers van de gegevens zijn.
• de beveiligingsplicht: De 'verantwoordelijke' moet voor 'passende organisatorische beveiligingsmaatregelen' zorgen. Dat betekent onder meer dat hij duidelijk moet maken - bijvoorbeeld via een overzicht -, welke personen op de diverse afdelingen binnen de instelling toegang hebben tot welke gegevens. De NEN richtlijn geeft handvaten voor informatiebeveiliging in de zorg.
• de meldingsplicht.: De 'verantwoordelijke' is verplicht om vastlegging en gebruik van geautomatiseerde en deels geautomatiseerde dossierbestanden bij het College Bescherming Persoonsgegevens (CBP) in Den Haag te melden.

Individuele beoefenaren in de gezondheidszorg hoeven de bewerking niet te melden mits de doelen van bewerking direct zijn gerelateerd aan de beroepsuitoefening[11]. In het geval van de EIC hangt het af van de aangesloten leden (individueel of zorginstelling) of er een meldingsplicht geldt voor zijn/haar specifieke database. Melding van verwerking lijkt echter verstandig en kan plaatsvinden bij het CBP dan wel bij een "Functionaris voor Gegevensbescherming", die aangesteld kan worden voor toezicht op de informatieverwerking in bijvoorbeeld een zorgregio[12]. In alle gevallen zal onderzocht moet worden of een dergelijke functionaris al bestaat in een zorgregio dan wel door wie een dergelijke functionaris aangesteld zou kunnen worden binnen een specifiek bereik van de zorg in de eerstelijn.

[8] NIVEL (2011) p103
[9] KNMG (2004) p 27.
[10] KNMG (2004)
[11] CBP (2011) Handreiking vrijstellingsbesluit. Paragraaf 4 Zorg en Welzijn. *http://www.cbpweb.nl/hvb_website_1.0/vwc16.htm*
[12] KNMG (2004) Van wet naar praktijk. Implementatie van de WGBO. Deel 4 Toegang tot Patiëntengegevens p40

Om er voor te zorgen dat de verwerking van behandelinformatie kan blijven plaatsvinden onder de controle en verantwoordelijkheid van patiënt en direct bij de behandeling betrokken zorgverlener (zoals voorgestaan door het CBP) kan het EIC niet optreden als verantwoordelijke in de zin van de WBP. Bij de verwerking van individuele behandelgegevens functioneert het EIC – net als ASP HIS-systemen- uitsluitend als een dienstverlener die medische informatie verwerkt onder verantwoordelijkheid van de aangesloten individuele leden/zorgverleners. Deze werkwijze komt zowel tot uitdrukking in de organisatorische opzet van het EIC als in de opzet en vormgeving van de technische infrastructuur.

Omdat behandelinformatie (net als bij een HIS) wordt beheerd door een derde (het EIC) is het belangrijk de huidige discussie over de relatie "verantwoordelijke"en "bewerker" in de zin van het WBP goed mee te nemen in de organisatorische vormgeving van het EIC omdat daaruit kan worden geleerd hoe privacy gevoelige informatie op een zorgvuldige manier kan worden opgeslagen, uitgewisseld en verwerkt voor verschillende doelstellingen zonder dat men de controle verliest over het eigen dossiers.

2.3 "De bewerker" en de verantwoordelijke

"Een ieder is verplicht geheimhouding in acht te nemen ten opzichte van al datgene wat hem bij het uitoefenen van zijn beroep op het gebied van de individuele gezondheidszorg als geheim is toevertrouwd, of wat daarbij als geheim te zijner kennis is gekomen of wat daarbij te zijner kennis is gekomen en waarvan hij het vertrouwelijke karakter moest begrijpen."(Wet BIG, artikel 88).

Het medisch beroepsgeheim is geformuleerd als een verbodsbepaling. Een zorgprofessional mag geen data delen met anderen die in de zorgrelatie wordt vastgelegd, anders dan na toestemming van de patiënt[13]. Data mag alleen worden gedeeld door "rechtstreeks betrokkenen" in de zorgrelatie en degene die optreed als diens plaatsvervanger, voor zover noodzakelijk voor het uitvoeren van de werkzaamheden. De WGBO kent een tweeledige criterium:

1) het moet gaan om personen die *rechtstreeks betrokken* zijn bij de uitvoering van de behandelingsovereenkomst
2) de toegang tot data is slechts toegestaan voor zover het *noodzakelijk* is voor de door hen te verrichten werkzaamheden.

Wie zijn nu de mensen met wie een behandelaar data mag delen? Het KNMG[14] zegt hierover:

> "*Over het algemeen zijn de personen die tezamen als behandelteam, op directe en gelijkgerichte wijze, betrokken zijn bij het doel waarvoor de gegevens worden verstrekt, rechtstreeks betrokken bij de uitvoering van de behandelingsovereenkomst. Zo zullen verpleegkundigen, doktersassistenten, fysiotherapeuten en artsen die gezamenlijk in een gezondheidscentrum werken hieronder kunnen vallen. Daarnaast kunnen bijvoorbeeld ook co-assistenten, medisch studenten, biochemici, fysici, paramedici, diëtisten, spelbegeleiders op een kinderafdeling…"*

Daarnaast kan het noodzakelijk zijn voor de uitoefening van de zorg derden in te schakelen voor het bewerken van gegevens. Er kan niet verwacht worden dan iedere zorgverlener alle administratieve financiële of IT taken uitvoert.

---

[13] Idem: p17

[14] KNMG (2004) Van wet naar praktijk. Implementatie van de WGBO. Deel 4 Toegang tot Patiëntengegevens p18 en 19.

De WBP definieert de bewerker als: "degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen".

Bij elke bewerking moet worden nagegaan of *de aard van de gegevens* expliciet gedefinieerd/gelimiteerd en er rekening is gehouden met de gevolgen voor de personen van wie gegevens worden doorgegeven (proportionaliteit) en er zijn *geen redelijke alternatieven* (subsidiariteit) voor het bereiken van het doel.

Het CBP stelt over bewerkers: "*Het hoeft niet per se te gaan om hulpverleners op wie een eigen beroepsgeheim rust, maar wel om werkzaamheden waarover de hulpverlener controle heeft en om een daarin concreet afgebakende taak. Voor degenen die dergelijke werkzaamheden verrichten geldt namelijk een afgeleid beroepsgeheim, terwijl de hulpverlener nog steeds aansprakelijk is als een dergelijke 'rechtstreeks betrokkene' in strijd met de geheimhoudingsplicht gegevens zou verwerken* "[15].

Of een bewerker kan worden aangemerkt onder de controle van de verantwoordelijke te handelen en dus gerechtigd is persoonsgegevens te bewerken hangt af van: "*verschillende factoren een rol, zoals de mate waarin inschakeling van de betreffende persoon of instelling binnen de kring van beroepsgenoten wordt aanvaard, de vraag of redelijke alternatieven voorhanden zijn, de zeggenschap van de arts over de werkzaamheden van de betrokkene (met name wanneer het niet-medici betreft) en de maatregelen die zijn getroffen ter bescherming van de persoonlijke levenssfeer van de patiënt. Ook de kenbaarheid voor de patiënt is van betekenis, terwijl voorts mee weegt of het belang van de patiënt erdoor wordt gediend"[16].*

In een advies over de doorstart van het EPD heeft het CBP belangrijke uitspraak gedaan over de bewerking in complexe systemen[17]. In de door Nictiz voorgestelde private doorstart van het EDP worden gegevens deels verwerkt door een op te richten vereniging van zorgaanbieders (VVZ) die zorgt voor de koppeling van verschillende dossiers. Deze vereniging wordt gepresenteerd als verantwoordelijke voor dat deel van de bewerking die koppeling van persoonsgegevens mogelijk maakt en daarmee beheert deze vereniging feitelijk de verwerking van deze persoonsgegevens. Het CBP oordeelt hierover : "*Ten aanzien van het in het Doorstartmodel geschetste scenario moet worden geconstateerd dat het bij het onder het beheer van VZZ vallend schakelpunt gaat om grootschalige, risicovolle verwerking van bijzonder gevoelige gegevens. In een dergelijke grootschalige context raakt de verwerking van patiëntgegevens feitelijk buiten de sfeer waarover de hulpverlener nog geacht kan worden feitelijk, daadwerkelijk controle te kunnen uitoefenen. De eventuele invloed die de hulpverlener als lid van VZZ en getrapt via de Gebruikersraad geacht kan worden uit te oefenen op de gegevensverwerking door VZZ is hoogstens indirect, want gericht op de werkwijze in algemene zin en houdt geen feitelijke controle(-mogelijkheden) over de verwerking van 'eigen patiëntgegevens' in.*"[18]

Dit advies bevat twee belangrijke punten die voor het EIC van groot belang zijn:
1. Op het moment dat bij grootschalige bewerking het risico groot is dat de hulpverlener de regie dreigt te verliezen kan niet meer worden gesproken van

[15] CBP (2011) Zienswijze CBP over doorstartmodel voor landelijke uitwisseling medische gegevens, 9 augustus 2011: p 9
[16] Registratiekamer (1994) De rekening van de arts, Den Haag in: P.J. Hustinx, Informatietechnologie in de gezondheidszorg, Preadvies voor de Vereniging voor Gezondheidsrecht, Utrecht: Vereniging voor Gezondheidsrecht 1999.
[17] CBP (2011)
[18] CBP (2011) p10.

een "bewerkers-relatie"in de zin van de WBP. Hieronder zullen we de vraag bekijken of een ASP model aangemerkt kan worden als een voldoende afgeperkte databewerking in de zin van de WBP.

2 Een verenigingsmodel is op zichzelf onvoldoende voor het uitoefenen van directe controle op gegevensbewerking door die vereniging in de vorm van ICT ondersteunende partij. Er moet directe verantwoording en controle blijven bestaan op de verwerking van gegevens door de verantwoordelijke.

Het College Bescherming Persoonsgegevens schreef in december 2009 een brief over ASP-diensten in de zorg aan het VWS met daarin een analyse over de mogelijkheden en risico's van deze manier van werken:

- Het risico bestaat dat gegevens door derden kunnen worden gezien
- De afhankelijkheid van één dienstverlener is zeer groot omdat deze de database beheert en overstappen uiterst kostbaar en moeilijk wordt (vendor lock) Hierdoor bestaat het risico dat de zorgverlener feitelijk zijn zeggenschap over de data kwijtraakt
- Een ASP kan de veiligheid van informatieverwerking in IT systemen vergroten.

Het CBP stelt dat ASP bewerkers kunnen worden beschouwd als rechtstreeks betrokkenen: "*….anderen dan zorgverleners kunnen "rechtstreeks betrokken" zijn. Uit de wetsgeschiedenis blijkt bijvoorbeeld dat hiertoe ook behoren "degenen die onder toezicht en verantwoordelijkheid van de betrokken beroepsbeoefenaars zijn belast met het feitelijk beheer van de patiëntendossiers. De kring van rechtstreeks betrokkenen is dus niet per se beperkt tot diegenen die handelingen verrichten op het gebied van de geneeskunst. Anderzijds is het gezien de tekst van de wet niet evident dat bedoelde ICT-dienstverleners rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst."*[19]

Omdat in de praktijk ASP nu al veel gebruikt worden en omdat niet van een hulpverlener kan worden verwacht dat hij zijn eigen systeem beheerder is, is het CBP geneigd positief te staan tegenover ASP's als "bewerker". Het CBP plaatst wel een belangrijke kanttekening: "*Vanwege het medisch beroepsgeheim dienen daarbij hoge eisen te worden gesteld aan de uitbestede gegevensverwerking. Er zullen stevige waarborgen moeten worden geboden voor een veilige en discrete verwerking bij de dienstverlener. Uitbesteding mag er immers nooit toe leiden dat op ongerechtvaardigde wijze gegevens aan personen of instellingen buiten de gezondheidszorg worden gebracht"*[20].

Het EIC model zal rekening moeten houden met bovenstaande. Het voor het EIC ontwikkelde model voorziet in een zeer consequent opgebouwde "bewerkers-relatie" tussen hulpverlener en databeheerder. De nadere uitwerking van dit model raakt zowel aan de organisatorische opzet van het EIC als aan de gebruikte informatietechnologie die er voor moet zorgen dat direct bij de behandeling betrokken zorgverleners de controle behouden over opslag, uitwisseling en gebruik van behandelinformatie op individueel niveau. In hoofdstuk 3 en 4 zal meer gedetailleerd worden ingegaan op de organisatorische en technische die nodig zijn om dit te realiseren.

2.4 Regels aangaande delen informatie met derden en voor wetenschappelijk onderzoek

Bij de opzet van het EIC hebben een tweetal overwegingen centraal gestaan waar het gaat om het delen van informatie. Enerzijds wil het EIC het delen van

[19] CBP (2009) ASP's in de zorg. Brief aan Minister van VWS, z2009-765. p2.
[20] Idem: p 3

informatie in samenwerkingsverbanden van zorgprofessionals gericht ondersteunen en faciliteren en anderzijds wil het EIC ook bevorderen dat relevante behandelinformatie beschikbaar komt voor wetenschappelijk onderzoek en statistiek.

Binnen de ketenzorg is de variatie van samenwerking, uitwisseling van gegevens en ICT hoog[21]. Of en hoe gegevens mogen worden uitgewisseld hangt af van de samenwerkingsrelatie en de "bewerkers" die de opdracht uitvoeren. Belangrijk is te kijken naar de praktijk van beoordeling binnen bestaande samenwerkingen zoals bij huisartsenposten en regionale schakelpunten en het EPD[22].

In de discussies over delen van informatie op grond van complexe samenwerking is het CBP de afgelopen jaren kritisch geweest. Zelf voor een huisartsenpost, waarin dossiers van te behandelen patiënten worden geraadpleegd, was het niet voldoende aan te nemen dat een zorgrelatie voldoende garanties gaf tot inzage in een dossier van een zorgverlener. Sleutel bij de beoordeling is dat garanties moeten bestaan dat[23]: 1) er daadwerkelijk sprake is van een zorgrelatie (hoe zorg je er voor dat uitsluitend voor de behandeling relevante informatie over de betreffende patiënt wordt gedeeld), 2) snuffelgedrag en misbruik kan worden voorkomen en gedetecteerd en 3) de patiënt van te voren toestemming heeft gegeven voor het laten opnemen van de gegevens in een nieuwe database die gedeeld wordt met derden.

Tijdens het NEDHIS congres in 2011 adviseerde Hooghiemstra als praktische oplossing dat zorggroepen er simpelweg voor moeten zorgen dat ze geen persoonsgegevens hebben/delen[24]. Een zorggroep kan ook op basis van geaggregeerde gegevens beleid bepalen en zorgprogramma's aansturen. Uiteraard kan wel *samen* met individuele zorgverleners wel worden gekeken naar patiëntenlijsten, waarbij de zorgverlener zelf zorgt voor het beschikbaar hebben van informatie. De voorgestelde werkmethode en database van EIC kunnen hier een bijdrage aan leveren. Een andere oplossing zou kunnen zijn een zorggroep als zorgverlener te beschouwen en voor overdracht van dossiers met uitsluitend de behandeling noodzakelijke informatie expliciet toestemming te vragen van de patiënten. Het delen van informatie binnen samenwerkingsrelaties kan binnen het EIC model worden uitgewerkt.

Voor delen van informatie met wetenschappelijke instituten gelden ook regels. De WBGO maakt een speciale uitzondering op het doorleveren van informatie zonder expliciete toestemming van de patiënt voor wetenschap en statistiek: hier mag wel data worden doorgeleverd indien:

1. Onderzoek een dringend algemeen belang dient
2. Het onderzoek niet zonder deze gegevens kan worden uitgevoerd
3. Voor zover betrokken patiënt geen bezwaar heeft gemaakt

Én A.

- vragen van toestemming aan patiënt niet mogelijk is *Én*
- waarborgen zijn ingebouwd dat de privacy van individuen is gewaarborgd

Of B.

- Het vragen van toestemming in redelijkheid niet kan worden verlangd *Én*
- Hulpverlener heeft gezorgd voor gegevensverstrekking zodanig dat herleiding tot individuele personen redelijkerwijs wordt voorkomen.

---

[21] De eerstelijns #4 mei 2010. Handvatten voor ICT keuzes in de ketenzorg.

22 KNMG (2010) Privacy bij regionale uitwisseling van patiëntgegevens: Handreiking naar aanleiding van bevindingen van het CBP bij twee regionale situaties. & CBP (2011).

23 KNMG (2010)

24 Hooghiemstra (2011) Privacy bij gegevensoverdracht. Keynote presentatie Nedhis 2011.

In de beide laatste gevallen is de zorgverlener verplicht een aantekening in het dossier te plaatsen dat gegevens voor onderzoek zijn doorgeleverd. De KNMG heeft hiertoe richtlijnen opgesteld[25]. Hoewel de discussie over TTPs en Privacy Enhancing Technology nog steeds voortduurt zijn verschillende partijen bezig via de TTP constructie grote databases op te bouwen. Zoals eerder gesignaleerd gebruiken academische instellingen een ruilsysteem van rapporten tegen data als middel om huisartsen er toe te brengen data voor wetenschappelijk onderzoek beschikbaar te stellen. Zoals al eerder gemeld acht NIVEL de kans groot dat de vorming van een centrale database met behandelinformatie op individueel-/celniveau op grote weerstand zal stuiten bij zowel huisartsen als het grote publiek.

Het EIC kan voor verschillende wetenschappelijke partijen een oplossing bieden voor het moeilijke proces van dataverzameling en voor de legitimiteit. Daarnaast kan omdat terugkoppeling van data niet meer noodzakelijk is in bepaalde gevallen worden volstaan met anonimisering van gegevens. Verder kan EIC helpen bij het maken van subselecties zodat op de minst privacy gevoelige manier voldaan kan worden aan doelbinding, het noodzakelijkheidscriterium en het subsidiariteitsbeginsel[26].

Veen (2011)[27] stelt dat TTP op zich nooit voldoende zijn voor een garantie op zorgvuldige omgang met data voor wetenschappelijk onderzoek. De hele context en organisatie rondom de datapseudonimisering, verzending, opslag en verwerking moet zo worden opgezet dat er garanties worden ingebouwd die zorgvuldigheid garanderen. Voor het EIC is relevant dat er in bestaande modellen voor het gebruik van huisartsendata en apothekersdata voor wetenschappelijk onderzoek, op verschillende manieren toezicht wordt uitgeoefend op doelbinding en gebruik van data via commissies en raden van toezicht. Op dit toezicht zal in hoofdstuk 3 nog verder worden ingegaan.

2.5 Informatieplicht en patiëntenrecht

Patiënten hebben bepaalde rechten aangaande het dossier dat een zorginstelling bewaard (KNMG, 2004). Dit zijn

- Recht op inzage en afschrift
- Recht op aanvulling of correctie en afscherming
- Recht op verwijdering en vernietiging

Zoals eerder aangeven kan het EIC dossier van een behandelaar worden gezien als het verlengde van het originele dossier. Hiermee kan worden beredeneerd dat dezelfde rechten volledig van toepassing zijn op het EIC dossier. In geval patiënten van hun recht gebruik maken moet automatisch de implementatie van de actie op beide systemen kunnen worden toegepast. EIC zal hiermee rekening dienen te houden bij de nadere uitwerking van haar systeem, zodat de praktijk/zorgverlener directe en daadwerkelijke controle kan blijven uitoefenenen op EIC als bewerker.

In het verlengde van bovengenoemde rechten van patiënten heeft de zorginstelling een informatieplicht met betrekking tot het gebruik van medische gegevens. Deze informatieplicht geldt nu al voor de omgang met gegevens in bijvoorbeeld een HIS[28]. Bij deelname aan het EIC kan een praktijk worden ondersteund bij het maken van voorbeeld voorlichtingsmateriaal over

25 FMWV (2004) Gedragscode Gezondheidsonderzoek; concept versie 4 def. April 2004.
26 Te denken valt hierbij aan bijvoorbeeld het werken volgens representatieve steekproeven van huisartsendata in geografische zin, zoals nu in zeker zin het NIVEL al functioneert.
27 Veen, E.B>van (2011) Patient data for health research A discussion paper on anonymisation procedures for the use of patient data for health research. October 2011. Medlaw consult.
28 KNMG (2004) deel 3. p28

informatiebeheer en gebruik in zowel HIS als het EIC systeem. Het KNMG heeft richtlijnen geformuleerd voor de inhoud van dit type voorlichting. Hierin moet in ieder geval informatie instaan over inzagerecht, recht op correctie, recht op vernietiging en recht op bezwaar voor gebruik van informatie voor andere doelen dan de directe zorg.

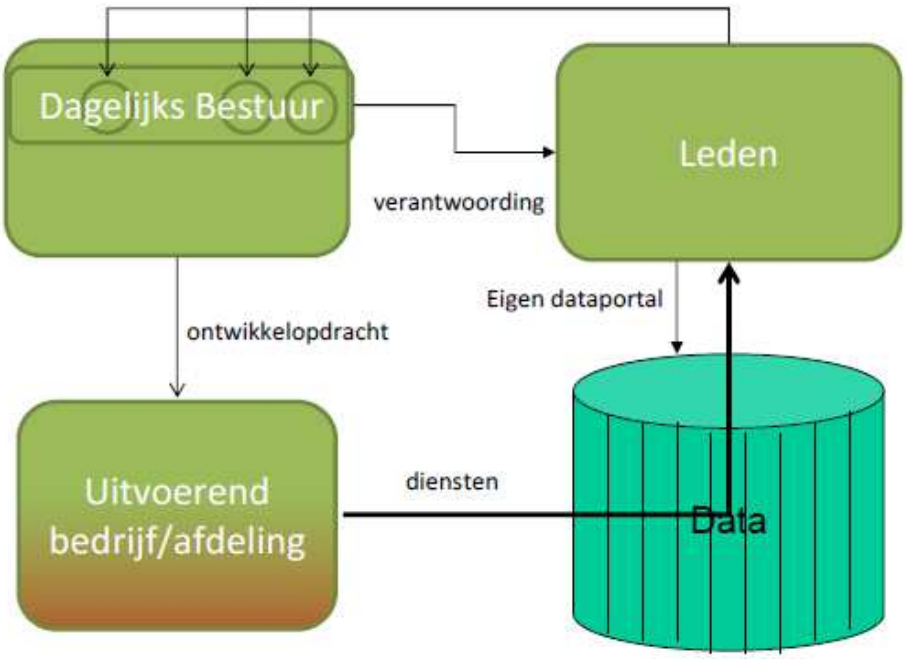
EIC zal van aangesloten leden vereisen in ieder geval een optie op bezwaar voor deelname van patiëntgegevens op te stellen, zodat patiënten in ieder geval hun recht op bezwaar expliciet hebben kunnen laten gelden.

Daar waar praktijken betrokken zijn bij de doorlevering van gegevens voor wetenschappelijk onderzoek zal per onderzoek informatie over dit gebruik en de daarmee verbonden informatie doorleveringen expliciet onderdeel moeten uitmaken van deze voorlichting.

3 Organisatiemodel EIC en wettelijke basis

3.1 Introductie

HET EIC is opgezet als een Vereniging met een Dagelijks Bestuur voor de dagelijkse gang van zaken. Het Bestuur stuurt een ondersteunende dienst aan voor het opzetten van het beheer en voor het ontwikkelen van diensten, die leden op individuele basis kunnen afnemen/contracteren.



Figuur 3.1 Data beheer en toegang onder verantwoording van leden EIC.

De data wordt door individuele leden in een centrale database gezet (zie 4 voor een technische uitwerking), en toegankelijk gemaakt via de dienstenstructuur voor analyse.

De dagelijkse aansturing van productontwikkeling en beheer wordt gedaan door een dagelijks bestuur. Het is goed statutair vast te leggen hoe de verdeling van zetels zo wordt geregeld dat:

a. huisartsen (en op termijn andere zorgverleners in de eerste lijn) controle houden op het verantwoordingsproces
b. de expertise voor ontwikkeling en beheer van het systeem wordt vertegenwoordigd in de dagelijkse leiding en
c. de kwaliteit van data-analyse wordt geborgd door deelname van de wetenschappelijke sector aan het bestuur. Het is daarnaast belangrijk ook te voorzien in betrokkenheid van het NHG, van vertegenwoordigende organisaties en van HIS leveranciers in bijvoorbeeld een raad van advies.

Het ontwikkelde model vereist dat in de statuten en de uitvoering van de vereniging nadrukkelijk wordt vastgelegd dat noch het Dagelijks Bestuur noch de technische uitvoerders verantwoordelijke worden in de zin van het WBP. De

verantwoording van het Dagelijks Bestuur naar de leden betreft het management van de organisatie en de inzet van middelen en tarieven voor ontwikkeling en onderhoud van het EIC-informatiesysteem als een efficiënte, faciliteit voor de verwerking van beschikbare behandelinformatie voor verschillende doelstellingen.

De leden/zorgverleners behouden, geheel in lijn met hun beroepsgeheim, de controle over de verwerking van gegevens binnen het EIC-informatiesysteem door:

- zelf (laten) aanleveren van gegevens naar de eigen database
- zelf (laten) analyseren van data middels software tools dan wel eigen tools
- via pushmodellen beslissen of en aan wie data doorgeleverd wordt.

3.2 De doelen

De primaire doelen van de gegevensverwerking via het EIC-informatiesysteem zijn verbonden met verbetering van de zorg aan de patiënten, of is daar direct van afgeleid[29] en wordt gelegitimeerd in de WMG en KWZi/BIG en mogelijk in de toekomst ook door de WCZ (zie hoofdstuk 2). Het faciliteren van onderzoek is onder omstandigheden en met inachtneming van randvoorwaarden en restricties ook mogelijk volgens de WBP.

De afgeleide doelen van wetenschappelijk onderzoek kunnen juist in een EIC model op een zorgvuldige wijze worden bediend, waarbij zorgverleners hun wettelijke verantwoordingsplicht kunnen uitoefenen.

3.3 Bewerkersrelatie

Of de relatie tussen bewerker en leden kan worden beschouwd als een "betrokken"relatie in de zin van het WBP moet worden bekeken in de context van het beoogde doel. Om tot een aantal criteria te komen waaraan zo'n bewerkersrelatie zou moeten voldoen kunnen we kijken naar het advies van de KNMG over de implementatie van de WGBO (2004). De KNMG stelt een aantal praktische vragen op voor aanname van betrokkenheid[30]:

a. Is het gebruikelijk in de beroepsgroep om deze andere hulpverlener op deze wijze bij de behandelingsovereenkomst te betrekken?
b. Zijn er redelijke alternatieven?
c. Heeft de hulpverlener zelf voldoende zeggenschap?
d. Zijn privacybeschermende maatregelen getroffen?
e. Is deze werkwijze kenbaar bij de patiënt?
f. Is deze werkwijze in het belang van de patiënt?
g. Is de omvang van de samenwerking voldoende beperkt?

Voor het EIC zijn deze vragen positief te beantwoorden en hebben de vragen direct consequenties voor het organisatorisch en technologisch model zoals later in dit document zullen wordt uitgewerkt.

a. Het EIC kan worden vergeleken met het model dat het SFK hanteert. Dit systeem ondersteunt apothekers met informatie management. In zekere zin kan het organisatiemodel van het EIC ook gezien worden als een ASP-achtige service vergelijkbaar met een ASP HIS.

b. Alternatieven zoals voorgesteld door het NIVEL, ZiZo of academische initiatieven die tot doel hebben informatie aan huisartsen te leveren zijn allen veel complexer en méér ingrijpend in de zin van privacyrisico's dan het EIC model. In de praktijk blijken academische initiatieven gericht op de verwerking

29 KNMG (2004) deel 3: p17
30 KNMG (2004) deel 4: p19

van behandelinformatie primair georiënteerd op verkrijgen van medische gegevens voor wetenschappelijk onderzoek en wordt de service geleverd aan huisartsen meer als ruilmiddel ingezet voor het verkrijgen van deze gegevens. De opzet en werkwijze van het EIC kan in zekere zin ook een oplossing vormen voor deze oneigenlijke praktijk (zie hieronder).

Een gedeelte van de informatiedoelstellingen die vanuit het EIC-informatiesysteem kunnen worden bediend zou ook gerealiseerd kunnen worden door een aantal analyse tools te bouwen op het HIS. De dienstverlening zoals die wordt aangeboden door Magistro, Rave of Proigia zijn voorbeelden hiervan. Het nadeel van een dergelijke aanpak is echter ondermeer dat lang niet alle doelen kunnen worden bereikt met het bouwen van tools op een HIS. Zo kan benchmarking tussen HISsen en kunnen analyses van geïntegreerde zorgverlening niet worden gemaakt op basis van een louter HIS gebaseerd model.

Het gevolg daarvan is dat zorgverleners vanuit de eigen HIS informatie zullen moeten gaan aanleveren voor verschillende doelen in onderscheiden formats en met eigen validatieprocedures. Binnen een door zorgverleners gecontroleerd informatiesysteem zoals ontwikkeld voor het EIC kan informatieverwerking voor verschillende doelstellingen dynamisch (voor aanpassing door tijd) plaatsvinden zonder dat zorgverleners hiervoor steeds weer nieuwe aanleveringsprocedures moeten invoeren [31].

Daarnaast moet geconstateerd worden dat in de praktijk aansluiting van tools op een HIS technisch vaak lastig is terwijl de controle en sturing van professionals op de ontwikkeling HIS tools erg laag. HIS leveranciers hebben als eerste prioriteit het onderhoud van hun eigen software en aanpassingen voor de dynamische ontwikkelingen in het leveren van zorg.

c. In het EIC heeft de hulpverlener op twee manieren zeggenschap. Hij heeft invloed als opdrachtgever voor beheer van data via een ASP bewerkersovereenkomst en toezicht op NEN certificatie voor de server en software en via lidmaatschap van de vereniging die de database-server beheert en ontwikkeling van nieuwe software coördineert. Daarnaast heeft hij zelf toegang tot de database, rapportfunctionaliteiten en heeft hij de mogelijkheid zelf analyses (te laten) uitvoeren op zijn eigen database. Bij de technische uitwerking zal de zorgverlener altijd via een *push model* beslissen wat er met data gebeurt en als deze worden doorgeleverd aan derden zal hij hiertoe expliciet opdracht kunnen en moeten geven.

d. Privacy maatregelen moeten voor het EIC goed worden uitgewerkt zodat sprake is van een robuust, legitiem, duurzaam en dynamisch informatiesysteem dat door de tijd heen kan worden aan gepast aan veranderende doelstellingen en randvoorwaarden. Het EIC-model zoals uitgewerkt in deze notitie is een eerste beslissende stap om dit te realiseren, het is echter de bedoeling om in 2013 te komen tot NEN certificering.

e. Dit aspect is uitgewerkt in 2.5.

f. Ja, de databewerking is in het belang van de kwaliteit van de zorg, transparantie en efficiëntie van de zorgleverantie.

g. De verwerking van gegevens zal worden vastgesteld via bewerkersovereenkomsten voor het beheer van data en aanmaken van standaard rapporten. In geval van maatwerkopdrachten en opdrachten voor analyses moeten waarborgen worden ingebouwd voor beperkte en specifieke toegang tot data door bewerker. Dit zal verder worden uitgewerkt in het technische model.

[31] De Vos (2010) *Vertrouwelijkheid een noodzakelijk instrument in de Geestelijke Gezondheidszorg, KDVP/Voswiz*, suggereerde eerder voor de GGZ een dergelijke opzet om een alternatief te bieden voor de grote risicovolle database, DIS. Dit document is tevens achtergrondsdocument bij de nog lopende CBB-zaak waarin de hoogste bestuursrechter nu al doorlevering van DBC gegevens aan zorgverzekeraars heeft verboden.

3.4 Relatie zorgverlener met derden

Zoals hiervoor al is gesteld zullen zorgverleners behandelgegevens in enige vorm moeten dan wel willen doorleveren aan derden voor de verbetering van transparantie in de zorgverlening, voor verantwoording en kwaliteitsborging of ter ondersteuning van wetenschappelijk onderzoek. De ontvangende partijen kunnen zorggroepen zijn, overheidorganisaties, zorgverzekeraars of wetenschappelijk instituten.

Op landelijk niveau speelt echter op dit moment de vraag of op dit moment huisartsen wel in staat zijn kwaliteitsinformatie te leveren[32]. Op basis van een praktijk experiment en analyse van de huidige mogelijkheden voor aanlevering van gegevens van huisartsen stelt het NIVEL dat het produceren van indicatoren voor huisartsen een zeer lastige taak is. Hoewel NIVEL niet uitsluit dat huisartsen zelf via een systeem van lokale gegevensverwerking indicatoren kunnen gaan leveren[33] pleit het document in de conclusies over het juridisch organisatorisch model[34] voor gecentraliseerde aanlevering van data via een TTP constructie aan een derde partij.

Een van de oplossingen die wordt voorgesteld door het Platform Regionale Datacentra is een netwerk van deze Regionale Datacentra die data voor zorgverleners gaan bewerken en doorleveren. In dit model wordt het datacentrum een centrale speler tussen zorgverlener zorggroep en externe afnemers*. "In het algemeen zijn er vijf partijen te identificeren die een rol spelen bij de verwerking van behandelgegevens tot indicatoren of stuurinformatie: zorgaanbieders, zorggroepen, externe afnemers, datacentra en TTP's. In de praktijk hoeven niet alle partijen daadwerkelijk betrokken te zijn, dit hangt af van de lokale situatie. Zo schakelen niet alle zorggroepen een datacentrum in en doen de dataverzameling en verwerking zelf. Ook wordt niet altijd een TTP ingeschakeld. In deze paragraaf wordt de rol van deze vijf partijen in het dataverwerkingsproces besproken inclusief hun onderlinge relaties[35]."*

De opzet van het systeem (zie figuur) roept een aantal vragen op over de zeggenschap over data (wie heeft de uiteindelijke controle) en de bewerkersgrond voor bewerking van data door datacentra. De regionale datacentra zoeken daarom legitimering in de ruimte die de WBP biedt om wetenschappelijk onderzoek te doen met dossiers, mits de data gespeudonimiseerd zijn. Gevolg van dit voorstel is dat noodzakelijkerwijs een technisch model moet worden ingericht waarbij een TTP een rol speelt, hetgeen de kosten opjaagt[36]. Een ander alternatief dat wordt voorgesteld is een bewerking in opdracht van een zorggroep (al dan niet met een TTP) die als "verantwoordelijke" voor de data optreed. Zoals al hierboven besproken kleven er verregaande bezwaren aan het aanwijzen van een zorggroep als verantwoordelijke, omdat deze niet als direct betrokkene van de zorgrelatie kan worden aangemerkt (2.3 e.v.).

32 NIVEL (2011)
33 NIVEL (2011) Bijvoorbeeld Hoofdstuk 8.4
34 Idem: Hoofdstuk 8.7
35 Van Es & Ekker (2011) Kwaliteitscriteria voor dataverwerking ten behoeve van indicatoren en stuurinformatie. Platform van Regionale Datacentra/ Jan van Es/ NICTIZ. Concept november 2011; Versie 6:p5
36 NIVEL (2011); p96 E. van Es (2011) Kwaliteitsindicatoren voor dataverwerking ten behoeve van indicatoren, NICTIZ/RDC platform. Concept september 2011.

Figuur 3.2 – Betrokken partijen bij dataverwerking en hun onderlinge relatie (copie uit : van Es, 2011;v6;p5)

Met het model van het EIC is het goed mogelijk dat huisartsen (en andere behandelaars) zelf indicatoren gaan leveren en openbaar maken. Binnen het EIC kunnen naast doelen verbonden met de verbetering van zorgverlening (informatie die direct van belang is bij het zorgproces) dus ook goed (de wettelijke) doelen van kwaliteit en transparantie worden gediend. Dit EIC systeem kan eenvoudiger worden opgezet en er is geen grote verplaatsing van data naar derden nodig. Hiermee wordt verder het 'dure' TTP-model overbodig. Voorts signaleert het NIVEL dat "maatschappelijke weerstand niet onwaarschijnlijk lijkt" dat tegen een TTP model van verzameling van data door derden grote weerstand kan ontstaan.

Het EIC levert een oplossing voor dit legitimiteitsprobleem door opslag, uitwisseling, gebruik en analyse van behandelinformatie te doen plaatsvinden onder het beheer van huisartsen. Bijgevolg kan worden volstaan met een systeemmodel dat veel eenvoudiger is dan de een aantal van de nu voorliggende modellen met trajecten voor informatieverwerking via TTPs, overheden dan wel het NIVEL. Privacy wetgeving schrijft voor dat systemen die de minste inbreuk vormen op privacy rechten van patiënten en het medisch beroepsgeheim de voorkeur verdienden (toepassing van in wet en EVRM vastgelegde beginselen van subsidiariteit en proportionaliteit).

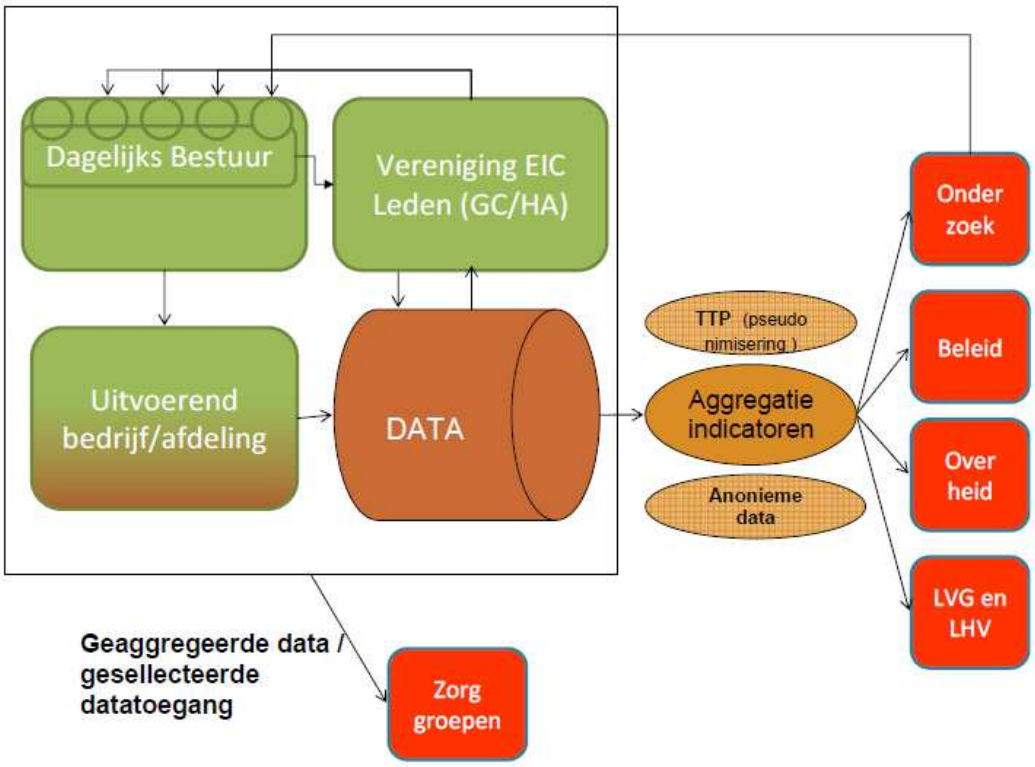
Hierboven is aangegeven hoe EIC (vergelijkbaar met een ASP HIS) de rol van "datacentrum" op zich kan nemen, zonder dat het beheer over het dossier uit handen komt van de zorgverlener. In dit model zal altijd de zorgverlener zijn die data doorlevert aan de Zorggroep, overheid en/of andere partijen. Het EIC is zoals eerder betoogd noch verantwoordelijke noch zelfstandige bewerker, maar fungeert slechts als opdrachtnemer van individuele leden.

Het Dagelijks Bestuur dan wel een Raad van Toezicht kan een belangrijke adviserende rol vervullen ten opzichte van de leden waar het gaat over deelname aan onderzoek en gebruik van data door derden. Het Bestuur heeft hierbij een voorlichtende rol zodat zorgverleners/leden een afgewogen geïnformeerde eigen beslissing kunnen maken aangaande doorlevering van data aan derden. Om belangenverstrengeling te voorkomen tussen Dagelijks Bestuur en derden die (al dan niet tegen betaling) om datadoorlevering vragen is het een optie om hiervoor een toetsingsprocedures op te stellen die wordt uitgevoerd door een zelfstandige commissie van huisartsen. Het SFK model en het IPSI model kunnen tot inspiratie dienen. In het SFK model houdt een Raad van Toezicht toezicht op: 1) privacy

regels, 2) datadoorlevering aan derden[37]. In het IPSI model wordt dit toezicht ook uitgeoefend door een Raad van Toezicht waarin deelnemende huisartsen een meerderheid hebben De taken zijn toezicht op privacyregels, gebruik van data voor onderzoek en door derden en toestemming op publicatie van resultaten[38].

Het nadeel van deze twee modellen is dat er een gedelegeerde toestemming wordt gegeven over datadoorlevering. Door huisartsen de uiteindelijke rol te geven in het geven van toestemming over het gebruik van hun data kunnen de voordelen van deze constructie (advies door een groep die zich verdiept in de materie) worden gecombineerd met een push model, waarbij binnen het EIC uiteindelijk de huisartsen verantwoordelijk blijven voor het delen van data voor onderzoek door middel van expliciete toestemming.

Het EIC model van datadoorlevering ziet er vervolgens als volgt uit:



Figuur 3.3 Model EIC server, verantwoording en datastromen

In dit model is onderscheid gemaakt tussen datasets met medische persoonsgegevens voor onderzoek en geaggregeerde rapporten voor zorggroepen. Eventueel kan voor onderzoek een TTP worden ingeschakeld. De zorgverlener zelf kan via de EIC infrastructuur (geselecteerde) data doorzetten naar een TTP. Zorggroepen zullen met een EIC model geen gebruik hoeven maken van een TTP, omdat data analyse door de zorgverlener zelf mogelijk wordt en de zorggroep in praktijk niet met persoonsgegevens op individueel patiënt niveau aan de slag hoeven. Zorggroepen kunnen natuurlijk wel een belangrijke opdrachtgever worden voor analyses en standaard rapportage functionaliteit en onder voorwaarden toegang krijgen tot een eigen geaggregeerde database.

37 SFK (2005). Statuten SFK.
http://www.sfk.nl/informatieaanvragen/algemeen/statuten_en_privacy/statuten.html
38 Mi&eur (2011) Overeenkomst Mi&eur met Bijlage Raad van Toezicht. Intern document Mi&eur en aangesloten artsen.

4 Technologisch model

De juridische en organisatorische context hebben consequenties voor hoe het technologisch model wordt voorgesteld. EIC is zo opgezet dat leden van het EIC controle houden over hun eigen dossier als een verlengde van hun zorg systemen. Een dergelijk systeem is opgezet volgens een combinatie van een ASP-model vergelijkbaar met enkele HISsen en een SFK-achtig model. Daarnaast worden een aantal functies toegevoegd die benchmarking binnen groepen faciliteert en die delen van informatie met derden (zorggroepen en wetenschap/beleid) mogelijk maakt.

Het technologisch model voldoet aan de volgende criteria:

- Het is een ASP systeem dat in het verlengde van de zorgdossiers van de zorgverleners kan functioneren
- Het zorgt voor directe controle over de medische persoonsgegevens door zorgverleners
- Het bouwt eisen van de WBP en WGBO in het technologisch ontwerp in
- Het maakt het eenvoudig om eigen analyses te (laten) doen
- Het moet mogelijk zijn bewerkte (geaggregeerde) gegevens te delen
- Het moet mogelijk worden via een TTP gegevens voor onderzoek en beleid door te (laten) leveren.

Het ontwerp en de implementatie is expliciet gericht op "privacy by design", waarbij juridische en organisatorische eisen als het ware bewust worden "ingebakken" in de technologie[39].

Door uit te gaan van een model waarbij de database onder beheer is van zorgverleners en het systeem waar mogelijk met opensource software wordt gebouwd is een modulaire aanpak mogelijk van rapportages en toepassingen. Er is geen dure licentiesoftware nodig voor onderhoud van software.

De belangrijkste technologische onderdelen zijn:

- de Proigia server en desktop applicatie
- de rapportage functionaliteit en databeheer
- beveiliging
- benchmarken en delen van informatie met derden.

4.1 Proigia server en desktop applicatie

Het technologisch model bestaat uit een server en een lokale applicatie die zorgen voor het veilig kunnen inzien, bewerken en verzenden van data. In figuur 4.1 staat een schematische weergave hiervan. Uit het HIS wordt data gehaald en door de "desktoptool" in de server geladen. De data wordt opgeslagen in een praktijkspecifieke database die alleen toegankelijk is voor die specifieke praktijk. Door een strikte scheiding van opslag en veilige toegangsprotocollen (zie onder 4.3) is het onmogelijk dat derden de data van de eigen praktijk inzien.

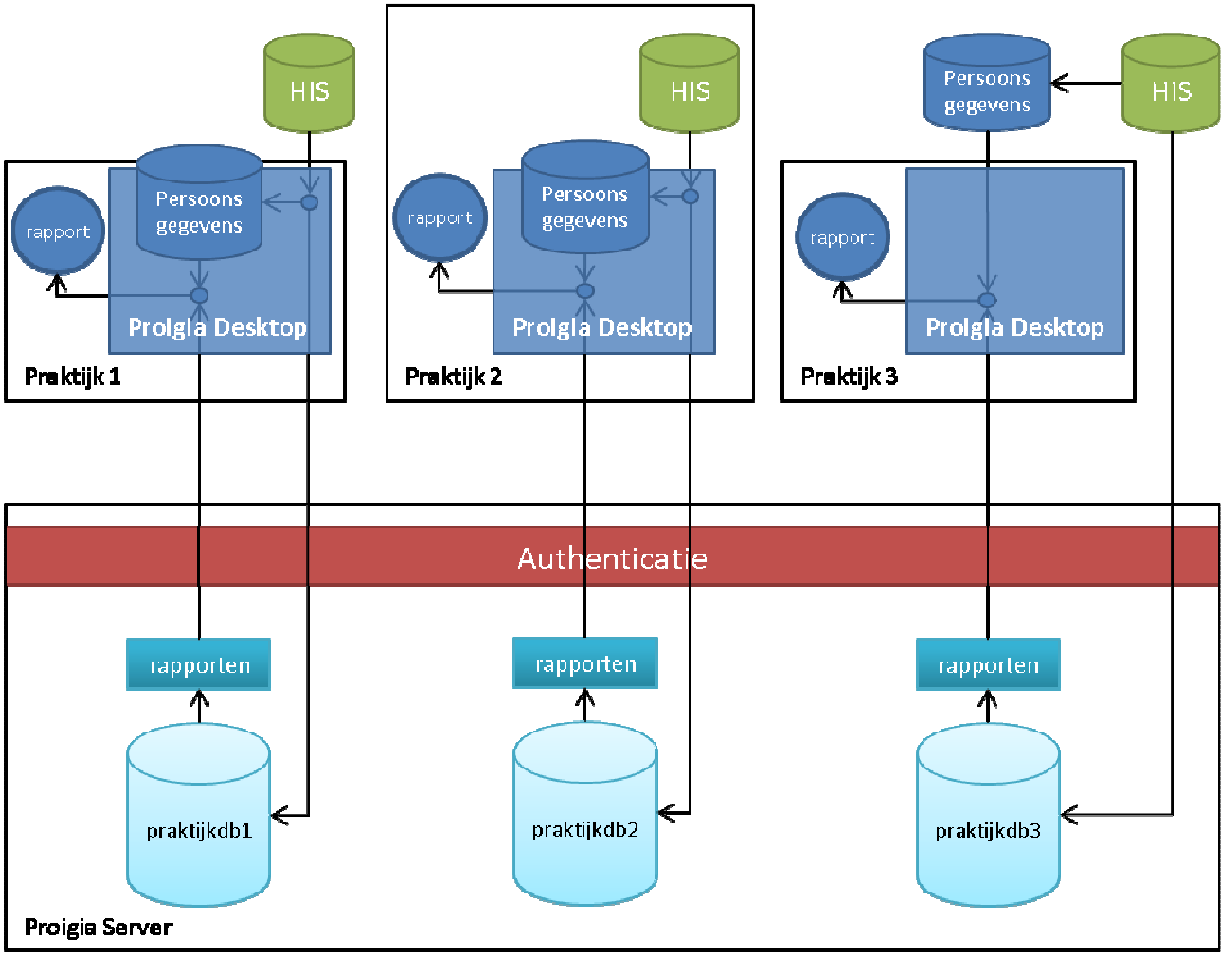
Alle acties door zorgverlener worden gedaan via de Proigia desktop applicatie. Dit is de interface voor alle inzage van data. De desktop applicatie heeft verschillende functies:

- Het zorgt voor het importeren van HIS data naar de server
- Het zorgt voor scheiding van NAW en medische gegevens. De NAW blijft bij de praktijk, terwijl de medische gegevens worden verzonden naar de server[40].

39 WRR (2011) De staat van informatie. Verkenningen 25.

- Rapporten die voor de praktijk beschikbaar zijn kunnen worden ingezien waarbij de lokale NAW gegevens transparant in het rapport terug gezet worden
- Rapporten kunnen eventueel worden gedownload (in Excel) voor verdere eigen analyse in de praktijk

Het verkrijgen van data uit de HISsen kan op verschillende manieren plaatsvinden. Op dit moment is optie 1 het meest gangbaar. Data wordt uit een ASP –achtige omgeving (Promedico ASP, Medicom, Scipio) van het HIS gehaald via extractie tools van het HIS dan wel via een directe koppeling. Optie 2 geldt voor HISsen die nog op locatie in de praktijk staan met dataserver en al. TetraHIS en Promedico VDF zijn voorbeelden hiervan[41]. Optie 3 geldt nu nog voor geen enkel HIS maar onderhandelingen zijn gaande met in eerste instantie een HIS voor deze manier van datalevering direct naar de centrale server (het SFK model). Uiteraard moet de zorgverlener/verantwoordelijke de opdracht expliciet geven en zal de opdracht volgens protocol worden vastgelegd.



Figuur 4.1 Overzicht Server, Desktop applicatie en datastromen.

40 Op dit moment wordt vanwege mogelijke automatische koppeling van HISsen ook een systeem ontworpen die deze pseudonimisatie mogelijk maakt bij ASP HIS-systemen. Verwacht wordt dat dit halverwege 2012 werkend is.
41 In het geval Medicom een CD levert voor data analyse geldt in feite de situatie uit optie 2.

Drie zaken zijn van belang voor privacywetgeving:
- de datatoegang is per praktijk strikt gescheiden geregeld
- de data wordt gescheiden opgeslagen in een praktijkspecifieke kluis
- door scheiden van NAW is het erg moeilijkvoor datamanagers tijdens ondersteuning van praktijken personen te herkennen.

Door de garanties van gescheiden dataopslag is het technisch eenvoudiger beveilingsmaatregelen te treffen, en er voor te zorgen dat data strikt onder beheer van de zorgverlener blijft. Mocht er per ongeluk toch een inbraak mogelijk zijn, dan blijft de schade "beperkt" tot alleen die ene database[42].

De despeudonimisatie heeft voordelen die direct zichtbaar zijn. In geval een zorgverlener voor maatwerk toestemming geeft voor het doen van analyses op zijn database is het voor de "bewerker" niet direct zichtbaar over welke personen de rapportage gaat. Dit voorkomt snuffelwerk, hoewel de data voor de wet nog steeds persoonsgegevens blijven vanwege de omvang va de database, de indirecte herleidbaarheid en de terug-herleidbaarheid via de desktop tool[43].

Hierom is naast een technische maatregel altijd een organisatorische inbedding nodig voor de "bewerkersopdracht". Op termijn zal een extra beveiliging worden ingebouwd waarmee de zorgverlener uitsluitend voor een bepaalde opdracht en een bepaalde tijdsperiode expliciete toestemming geeft voor toegang tot de 'datakluis' voor "opdracht x en tijdsperiode y" (de toestemmingsmodule). Via een logging systeem kan worden nagezien dat deze bewerking wordt nageleefd volgens protocol (zie 4.3). De ontwikkeling van het regelen van de "toestemmingsmodule" staat op het programma voor halverwege 2012. Een "ruwe" versie van logging zal in januari 2012 worden geïmplementeerd.

De desktop applicatie geeft ook toegang tot de rapporten van de desbetreffende praktijken. Hierin kunnen zorgverleners hun eigen rapporten opzoeken en inzien en eventueel downloaden in Excel. In geval er patiëntenlijsten in de rapporten zit zorgt de desktop applicatie voor het toevoegen van NAW aan deze lijsten (zowel bij inzage in de server rapporten als in de Excel sheets: zie verder 4.3).

4.2 Rapportage functionaliteit en databeheer

Rapporten worden als voorgedefinieerde rapporten klaargezet in de server door de ondersteunende technische organisatie van het EIC, voor iedere praktijk die "recht" heeft dit rapport in te zien[44]. De ondersteunende technische organisatie heeft daarbij geen toegang tot de data van de praktijken nodig. De meeste rapporten die nu beschikbaar zijn bevatten twee soorten gegevens: indicatoren en patiëntenbladen met patiënten die aan bepaalde kenmerken voldoen. Via de desktop applicatie kunnen rapporten worden ingezien en gedownload in Excel.

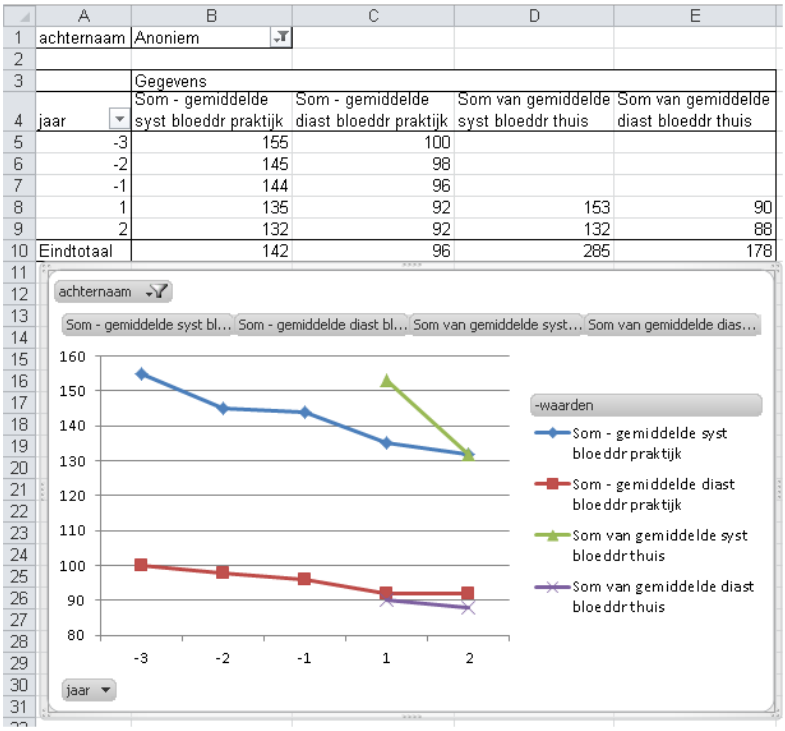
De beschikbare rapporten zijn:
- NHG accreditatie indicatoren (DM, COPD, astma, HVZ, preventie, medicatie)
- NHG standaard CVRM
- AGIS en Achmea GEZ prestatie indicatoren met module wijkgerichte opdeling en module verwijzingen naar de tweede lijn.
- Nierfalen
- Osteoperose
- Hypertensiezelfmanagement

42 Mits de beveiliging afdoende is geregeld is het hierdoor het veel interessanter voor een crimineel om in te breken in een HIS dan in het EIC systeem.
43 Veen, E.B.van (2011) Patient data for health research A discussion paper on anonymisation procedures for the use of patient data for health research. October 2011. Medlaw consult.
44 Gedacht kan worden aan "recht" vanwege rapporten in het standaard abonnement, als de praktijk specifieke rapporten heeft aangeschaft of laten ontwikkelen als maatwerk.

- Registratie correctierapporten met modules : algemeen overzicht registratie, DM, CVRM, COPD/astma
- NHG Jaarverslag (met maatwerk; zonder maatwerk beschikbaar halverwege 2012)

De server heeft verder standaard ingebouwde functionaliteit voor benchmarking. Als praktijken aangeven dat ze mee willen doen aan het delen van hun geaggregeerde data (bv praktijkgemiddelden) met een bepaalde groep praktijken (zorggroep, hele EIC populatie, andere samenwerkingsverbanden) worden de uitgerekende gegevens op praktijk niveau automatisch naar een aparte benchmark database doorgezet voor deze groep praktijken/deelnemers.In opdracht kan deze database, inclusief daarop gebaseerde rapporten, toegankelijk worden gemaakt voor bijvoorbeeld de zorggroep. Tot slot is deze benchmark database interessant voor doorlevering van intern afgesproken "gemiddelden data" aan derden (zie 4.4).

Voor een aantal rapporten is via Excel functionaliteit een aantal grafieken en samenvattende tabellen toegevoegd. Op dit moment kunnen deze verrijkte rapporten worden gedownload, maar nog niet worden weergegeven in de webinterface[45]. In figuur 4.2 staat twee voorbeelden van dit soort Excel functionaliteit, waarbij hypertensie patiënten kunnen worden gevolgd ten opzichte van de start van een project (horizontale as) en waarbij draaitabellen kunnen worden voor gedefinieerd (hier gemiddelde bloeddrukwaarde).



Figuur 4.2 Excel grafieken en draaitabellen in de Proigia server

Wat in eerste instantie van belang is bij het opzetten van een database voor analyse van de praktijkpopulatie, geleverde zorg en organisatie van zorg is dat de data beschikbaar is, vindbaar is en kwalitatief in orde is. Hoewel een praktijk uitstekende zorg verleend is het mogelijk dat de registratie van de zorg niet voldoende op orde is of zelfs onvindbaar.

45 Dit is in ontwikkeling voor eind 2012. Tevens zal dan eenvoudige selectie en zoekfunctionaliteit in de server worden ingebouwd.

Om registratieverbetering te vergemakkelijken is daarom een set correctierapporten ontwikkeld. Het is aan te bevelen deze als standaard op te nemen als basis voor aansluiting bij EIC. Dit correctierapport is nu ontwikkeld voor een HIS en in ver gevorderd stadium voor de overige HISsen. Met behulp van deze rapporten kan de registratie worden verbeterd eventueel ondersteund door EIC.

> Voor de accreditering bij de NPA zijn de NHG indicatoren nodig, volgens een strikte registratie volgens ADEPD-richtlijnen. Deze richtlijn schrijft voor waar bepaalde zaken geregistreerd moeten worden in het HIS. Het opzoeken en meenemen van indicatoren uit andere velden dan de daarvoor voorgeschreven velden door ADEPD is voor deze accreditering niet toegestaan (). De cijfers van de accreditering zeggen dus niet direct alles over geleverde zorg, maar aanvankelijk ook veel over de registratie gewoontes van de praktijk. Praktijken dienen hier rekening mee te houden voordat ze aan de accreditering beginnen.

Met de huidige infrastructuur is het mogelijk steeds flexibel rapporten aan te laten passen voor specifieke deelvragen en wensen van de praktijk of kunnen praktijken (met of zonder ondersteuning) via de uitgebreide Excelsheets zelf aan de slag.

Voor meer complexe aantrekkelijke visualisatie is het op verschillende manieren mogelijk presentatie software te koppelen aan de Proigiaserver. In het model van EIC is het denkbaar dat verschillende leveranciers rapportage functionaliteit koppelen aan de data. EIC of groepen professionals kunnen op termijn eigen maatwerk tools (laten) bouwen en op de database laten aansluiten, mits aan een aantal technische regels en voorwaarden wordt voldaan. De aansturing en coördinatie van het koppelen van derden software staat onder verantwoordelijkheid van het dagelijks bestuur van EIC, geadviseerd door de leiding van de technische staf.

Een voorbeeld van koppeling van de EIC server met andere software is een dashboard zoals aangeboden door Vinzi. De Vinzi dashboards zijn gebaseerd op koppeling van de praktijkdata aan een Business Intelligence software pakket, waarin voorgedefinieerde zoekfunctionaliteit wordt gebouwd. Hiermee kan de praktijk interactief de eigen data analyseren. Nu is een dashboard beschikbaar voor CVRM. Een dashboard voor analyse van bedrijfsresultaten is in ontwikkeling. Door de structuur van de server set-up blijven ook de data van het dashboard per praktijk gescheiden en worden alleen geaggregeerde rapporten gedeeld voor benchmark achtige toepassingen.

4.3 Beveiliging

Het EIC heeft beveiliging hoog in het vaandel staan. Daarbij is de opzet van techniek en de organisatorische context van groot belang. De verantwoordelijke over het patiëntendossier zal een aantal veiligheidsmaatregelen moeten nemen zodat de privacy en vertrouwelijkheid van de gegevens blijven gegarandeerd.

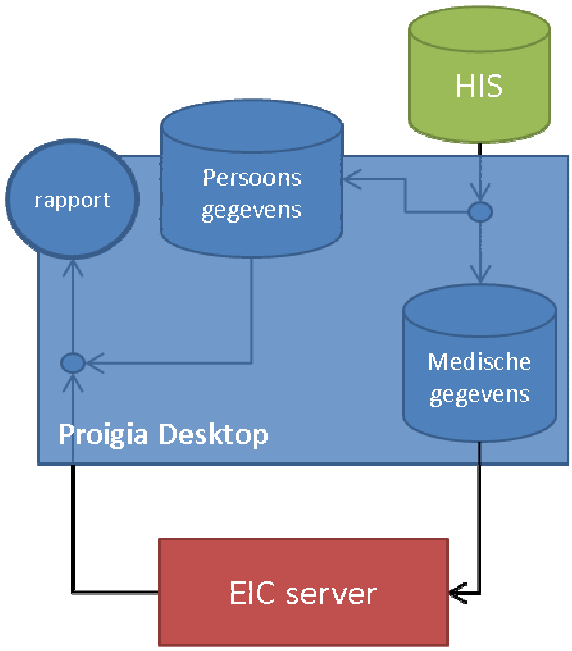
Beveiliging omvat een aantal organisatorische en technische maatregelen. Hierboven zijn we in gegaan hoe het organisatiemodel veiligheid en zorgvuldigheid van omgang met data kan bevorderen. In dit hoofdstuk zal de technische uitwerking worden beschreven.

De fysieke veiligheid van de data wordt gegarandeerd door het neerzetten van de server bij een ISO 27001 gecertificeerd datacentrum. EIC werkt momenteel met een server provider Site4U (bijlage 2). Site4U huurt meerdere server racks bij

BIT. , een kwalitatief hoogwaardige en betrouwbare leverancier van datacenterdiensten. Dit datacenter voldoet aan de internationale standaard voor informatiebeveiliging (ISO27001 gecertificeerd) en is bouwkundig en elektronisch beveiligd conform BORG klasse 4, de hoogste klasse voor een normaal bedrijfspand. Fysieke toegang tot servers is biometrisch beveiligd en contractueel is vastgelegd welk personeel toegang heeft tot de servers. Data wordt ge-encrypt opgeslagen zodat vervreemding of frauduleus kopiëren nutteloos is zonder de bijbehorende sleutels. De toegangskeys tot decryptie worden elders apart veilig opgeslagen. Met Site4U is afgesproken dat het samen met EIC / Proigia (en Vinzi) samen in 2012 het NEN 7510 traject zullen doorlopen.

Zoals hierboven (4.1) al uitgelegd worden de data voordat ze naar de EIC server worden gezonden eerst gepseudonimiseerd in de praktijk. In de praktijk worden de NAW gegevens opgeslagen en wordt een pseudoniem meegestuurd met de medische gegevens. De EIC server bestaat dus uit strikt gescheiden ge-encrypte databases met medische gegevens gekoppeld aan een pseudoniem.

In de praktijk blijft een kleine database achter met NAW gegevens. Toegang tot deze NAW database is alleen mogelijk met een toegangscertificaat. Op het moment dat rapporten worden ingezien of gedownload door een geautoriseerde persoon worden de NAW automatisch gekoppeld aan de rapporten. Hieronder staat het proces van pseudonimisatie uitgelegd in figuur 4.3.

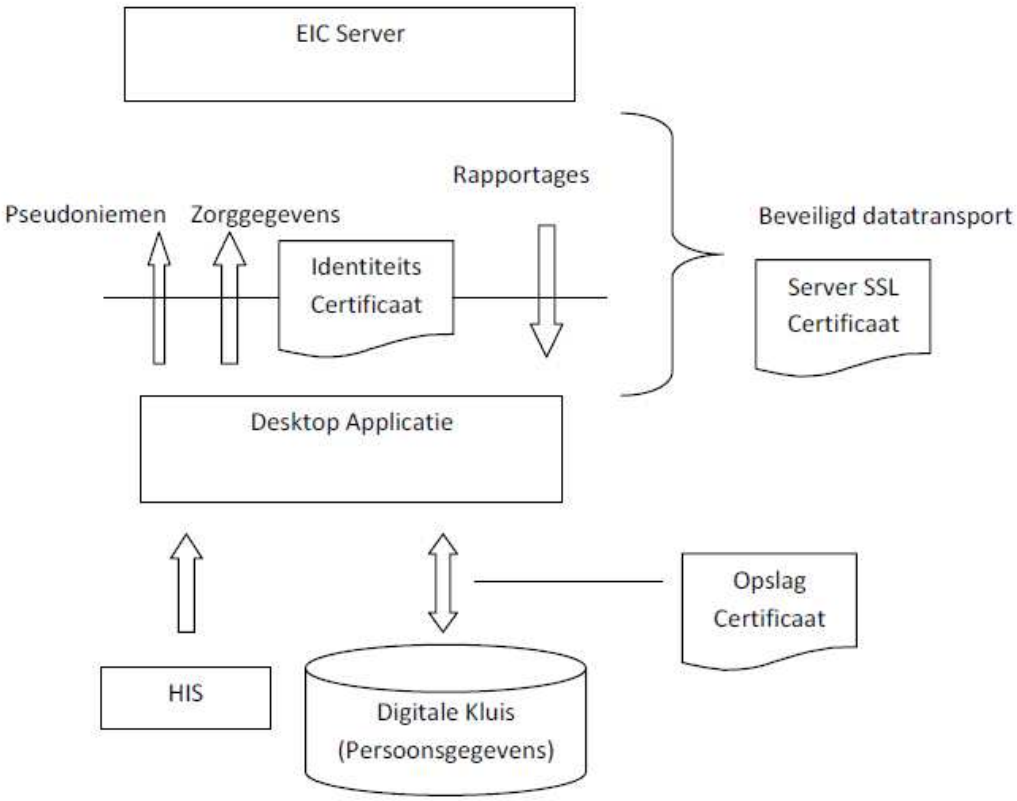


Figuur 4.3 Scheiding van direct herkenbare NAW van medische gegevens in de Proigia desktop applicatie

Toegang tot de praktijk databases via de desktopapplicatie wordt geregeld bij de installatie van de desktop applicatie en door protocollen voor datatoegang tijdens gebruik van de software die door EIC wordt aangeboden.

Voor elke gebruiker wordt een identiteit certificaat aangemaakt dat tijdens de installatie van de Proigia Desktop applicatie geïmporteerd wordt. Het certificaat is beveiligd met een apart wachtwoord waardoor alleen iemand die over beide beschikt het certificaat kan importeren. De gebruiker wordt met dit certificaat

individueel identificeerbaar[46]. In de server wordt vervolgens de autorisatie geregeld voor de verschillende gebruikers tot bepaalde praktijken (en hun databases) Toegang is dus alleen mogelijk als een gebruiker lokaal beschikt over het eigen identiteit certificaat, en in de server geautoriseerd is voor een praktijk. Toegang tot de NAW is alleen mogelijk vanuit de praktijk en met een tweede opslag certificaat dat alleen in de praktijk bekend is en tijdens het installeren van de Proigia Desktop applicatie aangemaakt wordt. Dit opslag certificaat, dat ook gebruikt wordt voor het encrypten van de NAW gegevens, kan eventueel met meerdere gebruikers gedeeld worden.



Figuur 4.4 Certificering en identificering in het Proigia model

Transport van data vindt plaats via een beveiligde SSL verbinding. Daarnaast zijn de NAW gegevens al uit de data gehaald.

Naast de fysieke en technische beveiliging zal het logging systeem worden uitgebreid. Het doel hiervan is: "…om verdachte, onrechtmatige toegang tot patiëntendossiers structureel te detecteren" In het rapport Beveiliging van persoonsgegevens stelt het CBP als eis aan persoonsgegevens die vallen onder risicoklasse II (en hoger): "*Elke poging (geslaagd of niet) om toegang te krijgen tot een informatiesysteem met persoonsgegevens wordt vastgelegd in een logbestand. Dit logbestand heeft een voldoende lange bewaartijd, zodat een analyse van bijzonderheden kan worden gemaakt en hierover kan worden gerapporteerd.*"[47].

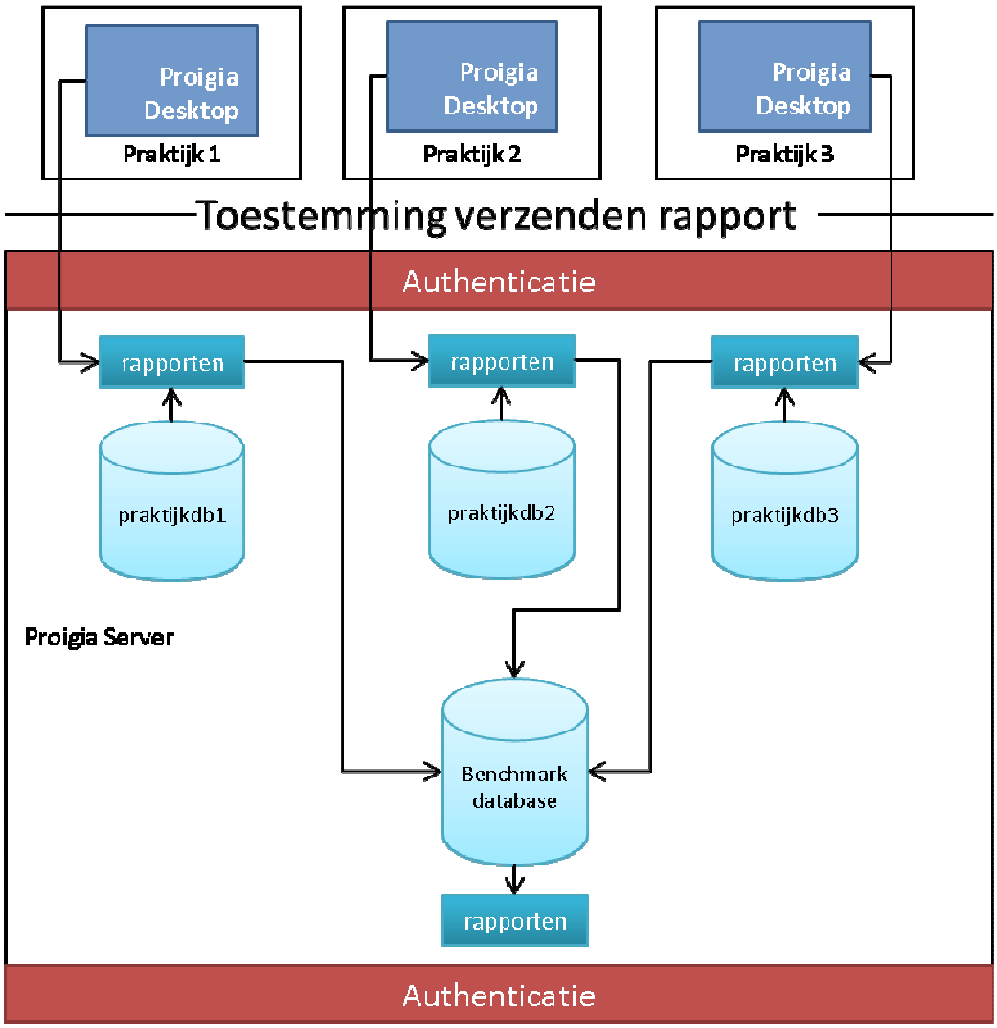
46 De veiligheid en zekerheid van de identificatie hangt wel af van het systeembeheer op de praktijklocatie omdat de certificaten worden gekoppeld aan een identiteit binnen het praktijksysteem. We gaan ervan uit dat binnen een praktijk identificatie goed is geregeld door inlognaam en password of andere aanvullende middelen.
47 KNMG, 2010 Privacy bij regionale uitwisseling van patiëntgegevens: Handreiking naar aanleiding van bevindingen van het CBP bij twee regionale situaties. P10

Om vast te kunnen stellen welke acties hebben plaatsgevonden op een patiëntendossier moeten volgens de NEN normen ten minste de volgende gegevens worden bijgehouden (gelogd)[48]:
- welke actie heeft plaatsgevonden;
- het tijdstip van de actie;
- [pseudo] identiteit van de patiënten dan wel groepen patiënten
- identiteit van de actor;
- identiteit van de verantwoordelijke voor de actie.

Het uitbreiden van het logging systeem om volledig aan deze eisen te voldoen zal starten in januari 2012 en zal getest en afgerond worden aan het einde van het jaar.

4.4 Benchmarken en delen van informatie

Het delen van informatie is gebonden aan strikte organisatorische en privacy regels. Technisch heeft het EIC het volgende model uitgewerkt voor geaggregeerde rapporten (figuur 4.5).



Figuur 4.5 Datastromen (na toestemming) in een benchmark database.

48 Idem.

Als een praktijk toestemming geeft data te delen in een benchmark worden samenvattende indicatoren uit de praktijkdatabse overgezet naar een 'benchmarkdatabase'. Ook wordt in het rapport van de praktijk een gemiddelde van een "voorgedefinieerde" groep praktijken toegevoegd aan de praktijkrapportage. De rapporten van groepen praktijken met gemiddelden van indicatoren per praktijk kan bijvoorbeeld gebruikt worden voor benchmarking in zorggroepen of als samenvattende gegevens voor kwaliteitsrapportages. In het geval van doorlevering naar buiten zal de praktijk hier ook op enig moment toestemming voor moeten geven.

Data voor onderzoek, beleid en verantwoording kan bestaan uit geaggregeerde data zoals hierboven beschreven, maar kan ook bestaan uit een subset van geanonimiseerde data. Het is mogelijk snel een anonieme dataset te maken met voorgedefinieerde gegevens, na goedkeuring van de interne toetsingscommissie (zie 3.4) en goedkeuring door de verantwoordelijken over de praktijkdata.

In geval onderzoek vereist dat data uit het EIC gekoppeld moet worden aan andere externe gegevens is het mogelijk via een externe TTP data door te leveren. Het TTP zorgt in dat geval voor de koppeling. Technisch is het goed mogelijk een dergelijke koppeling te maken vanuit de EIC server[49]. Wel zullen aan een aantal organisatorische en juridische eisen moeten zijn voldaan (zie ook hoofdstuk 3).

Een goede analyse in een latere fase voor een keuze voor het meest gewenste TTP-model zal in overweging moeten nemen dat in het overgrote deel van de data-aanvragen voor wetenschappelijk onderzoek het *niet* noodzakelijk is een "twee-weg" pseudonimisering op te zetten hetgeen de kosten van de TTP behoorlijk kan drukken en privacytechnisch te verkiezen is boven twee-weg despeudonimisatie van *álle* data. Vaak is het mogelijk anonieme data te gebruiken. Als er uitsluitend een 1-weg pseudonimisatie nodig is zou wellicht kunnen worden volstaan met een anonimisatie-tool binnen het EIC. In specifieke gevallen waarin koppeling wel is vereist kan uiteraard alsnog de techniek van twee-weg koppeling alsnog worden ingezet, waarbij de zorgverlener opdracht geeft om data voor wetenschappelijk onderzoek in te zetten[50]. De rol van zorgverlener is mede vereist uit de technische opzet omdat hij de versleutelde data moet laten "ontsleutelen" via zijn sleutel op de praktijk alvorens data naar een TTP te zenden. Dit model moet nog verder worden uitgewerkt wanneer de noodzakelijkheid en de vraag zich voordoet.

49 In het meest elegante model zal hiervoor de huidige lokale praktijk pseudonimisatie iets anders moeten worden opgezet zodat koppeling en doorzending van NAW vanuit een centrale pseudoniemen server van het EIC geregeld kan worden. Bij de ontwikkeling van rechtstreekse doorlevering van gegevens vanuit HISsen is in de ontwerpfase hiermee al rekening gehouden. Mogelijk zal dit voor Promedico al worden opgezet in de eerste helft van 2012.
50 Te denken valt aan onderzoeken die op data analyse gebaseerde enquêtes willen versturen. Hierbij spelt dan wel weer de overweging een rol of een dergelijk onderzoek niet op eenvoudigere wijze kan worden georganiseerd (bijvoorbeeld gedeeltelijk uitgevoerd door het EIC zelf).

5 Aanbevelingen uitwerking technisch model

Op het moment van schrijven wordt een EIC server geïnstalleerd volgens bovenstaande beschrijving. Het model van het EIC in organisatorische en technische zin voldoet aan de huidige privacywetgeving. In de voorgaande hoofdstukken zijn een aantal noodzakelijk vervolgstappen genoemd die moeten worden gezet om tot een "af" systeem te komen, die zal zorgen dat het model ook daadwerkelijk zorgvuldig uitgewerkt in praktijk wordt geïmplementeerd.

5.1 afspraken en contracten

Er dienen duidelijke contracten en afspraken te worden gemaakt.
1) Tussen het EIC en haar leden.
EIC moet in haar afspraken en contracten met leden opstellen hoe de organisatorische opzet is geregeld en de leden moeten door ondertekening hiermee akkoord zijn. Duidelijk en expliciet moeten aandacht worden besteed aan de verantwoordelijkheid over data en databases, ontwikkel prioriteiten, financiering en toekomstig businessmodel.
2) Tussen EIC en de dienstverlener(s).
Tussen EIC en dienstverlener moeten contractuele afspraken worden gemaakt over de geleverde diensten, SLA etc. alsmede over de afspraken/diensten die het EIC bemiddeld "aanbiedt" aan haar leden.
3)Tussen dienstverlener(s) en EIC leden
Er moet een duidelijke bewerkersovereenkomst worden getekend. Hiertoe kan worden uitgegaan van de aanbevelingen conform de normen die gelden voor uitvoering van de WBP. Er moeten contracten/afspraken worden gemaakt over te leveren diensten in modulaire vorm en hoe nieuwe diensten kunnen worden geleverd direct via de dienstverlener dan wel via het EIC. De huidige SLA-s dienen te worden getoetst aan de NEN norm en er zullen eventuele aanvullende afspraken moeten worden gemaakt.

Bij het opstellen van statuten en overeenkomsten moet rekening worden gehouden met de juridische randvoorwaarden zoals geschetst in dit document.

5.2 Bewerkersovereenkomsten

Met urgentie dienen standaard bewerkersovereenkomsten te worden afgesloten tussen EIC leden en de dienstverlener en het EIC. Hierin kunnen eisen worden opgenomen over toegang tot data, protocollen voor data bewerking.

5.3 NEN certificering stappenplan

Het opstellen van een stappenplan voor NEN certificering dient te worden opgezet door een NEN-werkgroep. De werkgroep moet bestaan uit verantwoordelijken voor de databewerking, de databewerkers en verantwoordelijken voor human resources en/of organisatorische opzet van EIC. De certificering vereist onder andere: het expliciet opstellen van afspraken, organisatieaanpassingen, beleidsinvoering, beheer technische middelen en een technische toets van huidige middelen, beheer ervan en monitoring van incidenten, alsmede plan voor onderhoud van de veiligheid. Het is van belang dat vroeg in 2012 een eerste bijeenkomst wordt gepland die een werkgroep instelt.

5.4 Ontwikkel prioriteitenplan

Hierin zal op zijn minst met prioriteit een logging systeem moeten worden opgezet, die frauduleuze handelingen detecteert.

Verder is het van belang dat de extractietool voor alle HISsen zoveel mogelijk standaard wordt aangemaakt. Onderzocht moet worden of HISsen bereid zijn mee te werken aan het ontwikkelen van standaard automatische geautoriseerde toelevering van data aan het EIC.

Interessante hierbij is de winst die dit kan opleveren op het gebied van privacy en controle over data. Voordeel van directe geautomatiseerde uitspoelen is dat het eenvoudiger wordt aanvragen van derden zoals onderzoekers te beantwoorden omdat aan de bron een koppeltabel kan worden gemaakt die de patiënten anonimiseert dan wel depseudonimiseert. Het ontwerp hiervoor is al ontwikkeld maar de onderhandelingen met HISsen moet in sommige gevallen nog worden opgestart in andere worden afgerond.

Automatische toestemmingsapplicatie door opdrachtgever en toegangsprotocol tot data voor bewerkers opzetten (zie boven)