Vertrouwensmodel

Van: **Nictiz**
Aan: **Ministerie VWS**
Datum: **18 april 2008**
Status: **definitief**

Inhoudsopgave

Inleiding

Om te kunnen komen tot een landelijk EPD is gewerkt aan een samenhangend stelsel van standaarden die in de volle breedte van de zorg vereist zijn om te borgen dat de voor de zorg noodzakelijke informatievoorziening uitsluitend toegankelijk is voor bevoegde zorgverleners en de betrokken patiënt. Met de inzet van ICT moet de kwaliteit, maar ook de doelmatigheid en fraudebestrijding in de zorg verbeterd worden.

Adequate informatiebeveiliging en een zorgvuldige omgang met persoonsgegevens (conform WBP en WGBO) is absolute voorwaarde voor betrouwbare gegevensverwerking, al wordt dat in de huidige decentrale en regionale praktijken niet altijd in praktijk gebracht. De introductie van een uniek identificerend nummer voor patiënten – als een van de onderdelen van het identificerende stelsel - is een andere belangrijke randvoorwaarde, die binnenkort doorgevoerd zal worden.

Deze notitie kent de volgende opbouw. Om de positionering van het landelijk EPD in de zorg te kunnen weergeven zal eerst (§ 1) kort worden ingegaan op de uitgangspunten zoals die gehanteerd worden. De huidige situatie met de algemene maatregelen zoals in eerder stadium met partijen overeengekomen, is weergegeven in § 2.

Nieuw ten opzichte van de huidige situatie is een aantal maatregelen die specifiek ingaan op de bezwaarprocedure en de controle van de behandelrelatie. De functionele implicaties van deze maatregelen worden in de twee volgende paragrafen besproken.

In § 3.1 wordt de nieuwe maatregel met betrekking tot een 6 weken bedenktermijn beschreven. Daaraan is toegevoegd een niet eerder in deze vorm beschreven overzicht van de andere mogelijkheden inzake bezwaar. De diverse maatregelen op dit punt (bestaand en gepland) dienen immers in de onderlinge relatie tot elkaar afgewogen te worden.

In § 4.1 wordt ingegaan op de nieuwe maatregel om een behandelrelatie te registreren ten behoeve van de controle hierop bij toegang tot het EPD (§ 4.2) Omdat de behandelrelatie er een is tussen zorgverlener en patiënt is de controle van de geregistreerde behandelrelaties door de patiënt het sluitstuk (§ 4.3).

In paragraaf § 5 wordt aangegeven op welke wijze de functionele uitwerking past binnen de uitgangspunten zoals door het CBP verwoord.

In de laatste paragraaf (§ 6) wordt de effectuering van de diverse waarborgen en maatregelen in de tijd gezet.

§1. Het landelijke elektronisch patiënten dossier (EPD)

Registratie en communicatie van medische gegevens in de zorg is niet nieuw. Op decentraal niveau wordt al sinds de jaren 80 van de vorige eeuw het elektronisch voeren van een dossier in de praktijk gebracht. De eerste beroepsstandaard voor registratie van medische gegevens door huisartsen dateert uit 1990.[1] Ook standaardisatie van de communicatie werd bij deze groep zorgaanbieders voortvarend ter hand genomen. Hoewel deze standaarden inmiddels verouderd zijn, worden ze nog volop gebruikt. De beveiliging van de gegevens en de beveiliging van de communicatie is, voorzover die al aangebracht werd, nooit op peil gebracht. Communicatie kenmerkte zich door een elektronische variant van de brievenpost: de verzender kende de ontvanger en omgekeerd. De brief werd vervangen door een bericht en verder bekommerde men zich niet om de privacy aspecten.

Op regionaal niveau is er rond 2000 in de eerstelijns gezondheidszorg een ander type communicatie ontstaan: niet meer 1:1 uitwisseling tussen zorgverleners die elkaar kennen, maar het koppelen op regionale schaal van alle zorgaanbieders via netwerken. In de meeste gevallen zijn de sectorale netwerken het meest succesvol: regionale waarneming tussen huisartsen onderling en regionale waarneming tussen apothekers onderling. De beveiliging van de privacy hierin is niet gestandaardiseerd, laat staan overal adequaat ingebouwd. Systemen worden er niet op getoetst. De beveiliging van de communicatie is in het begin wel gespecificeerd maar nergens ingebouwd (de netwerken zijn afgeschermd, maar de verbindingen zijn in de praktijk niet versleuteld). De afgelopen jaren zijn er diverse regionale platformen ontstaan. Vanuit de intentie om de gezamenlijk verleende zorg te verbeteren werden allerlei transmurale projecten gestart waarbij ook ziekenhuis gegevens beschikbaar kwamen voor de zorgverleners die op het regionale netwerk aangesloten zijn. In de meeste gevallen wordt weliswaar een minimale identificatie/authenticatie toegepast (gebruikersnaam en wachtwoord), maar meestal ontbreekt de controle op functie, op behandelrelatie en op beperking van de uitgewisselde informatie (de opvragende zorgverlener is slechts bevoegd datgene op te vragen wat nodig is voor de behandeling van de betreffende patiënt).

De introductie van een landelijk EPD is daarom, naast de noodzaak om de informatievoorziening in het kader van een behandeling te continueren, ook noodzakelijk om de bescherming van de privacy en daaruit voortvloeiend de toegangscontrole tot medische gegevens serieus ter hand te nemen. De enorme groei aan technische mogelijkheden tot elektronische communicatie mag niet leiden tot een evenzo makkelijke toegang voor onbevoegden. Zonder adequate maatregelen gebeurt dit echter wel. Met adequate maatregelen is er de uitdaging om het voor alle zorgverleners te regelen, voor alle systemen die gebruikt worden, voor alle leveranciers van die systemen, en voor alle netwerken. Landelijke standaarden met betrekking tot informatiebeveiliging, met betrekking tot toegangscontrole op de uitwisseling en met betrekking tot de gegevensset die verstrekt wordt is cruciaal en noodzakelijk, maar niet voldoende. Het borgen van deze zaken in de praktijk van alledag is waar het uiteindelijk om gaat. Het is immers de praktijk van de zorgverleners waar een concrete hulpvraag zich voordoet en waar vertrouwelijke informatie ontstaat. Het regelmatig kwalificeren van zorgaanbieders, van hun systemen en netwerken is een daarom minstens zo belangrijk.

Het landelijk EPD faciliteert niet alleen de noodzakelijke gegevensuitwisseling in de zorg, maar dwingt ook de bijbehorende maatregelen af om de informatiebeveiliging en de bescherming van de privacy te waarborgen. Om ook de zwakste schakels in een bepaalde dienstverlening op niveau te brengen, dient de hele keten van samenwerkende zorgverleners in kaart gebracht te worden. De consistentie in het samenhangend stelsel dient geborgd te zijn. De weg van wet

[1] WCIA referentiemodel voor Huisarts Informatiesystemen van het Nederlands Huisartsen Genootschap

naar zorgpraktijk is hierin weerspiegeld. Onder de naam Aorta ontwerpt en onderhoudt Nictiz een samenhangende architectuur voor zowel een landelijk beveiligde infrastructuur voor de zorg waar de beveiliging van uitwisseling en de toegangscontrole geregeld en bewaakt worden, als ook landelijke standaarden voor de afbakening van de gegevens die uitgewisseld mogen worden. In deze architectuur worden wet- en regelgevende kaders als uitgangspunt genomen en deze worden voor afzonderlijke zorgprocessen toegepast waarbij per zorgtoepassing een afbakening plaatsvindt van de informatiebehoefte. Het geheel mondt uit in programma's van eisen voor de afzonderlijke schakels in de keten. Een gedeelte wordt in de decentrale zorgsystemen ingebouwd en een ander gedeelte wordt in het LSP ingebouwd. Over de keten heen wordt al het noodzakelijke ingebouwd en gekwalificeerd.

§ 2. Algemene waarborgen inzake privacy en bevoegde toegang tot EPD

In de eerste plaats wordt opgemerkt dat deze notitie zich primair richt op betrouwbare gegevensverwerking in de zorg zoals dat binnen het landelijk EPD gespecificeerd wordt. Hierbij gaat het over zaken als toegang tot patiëntendossiers, informatie-uitwisseling in relatie tot de WGBO en de WBP. Zoals opgemerkt in de inleiding gaan we in deze notitie uit van vigerende wet- en regelgeving in het kader van de persoonsgegevens en maatregelen die getroffen zijn in verband met de bescherming van persoonsgegevens. Het gaat dan vooral om identificatie, authenticatie en autorisatie.

De noodzaak van een brede en effectieve toepassing van ICT in de zorg wordt alom onderkend. De noodzakelijke kwaliteit en effectiviteit van de gezondheidszorg en het voorkomen van onnodige fouten kan in de toekomst niet worden gegarandeerd indien hierin geen doorbraak wordt bereikt. De noodzakelijke verbreding van de beschikbaarheid van cliëntgegevens in de zorg dient echter gepaard te gaan met (veel) betere waarborgen voor vertrouwelijke verwerking van gegevens. Vanuit het oogpunt van continuïteit van de informatievoorziening tussen samenwerkende zorgverleners (met name van verschillende zorginstellingen) is de beschikbaarheid van gegevens voor bevoegde behandelaars cruciaal. Vanuit het oogpunt van de gegevensbescherming is het voorkomen van toegang tot deze gegevens voor onbevoegden cruciaal. Onder de onbevoegden zitten ook zorgverleners. De juiste afbakening tussen de twee cruciale vereisten spitst zich daarmee toe op de vraag: *welke zorgverleners en welke medewerkers van een zorginstelling zijn bevoegd en welke zijn het niet en op welke wijze kan de grens technisch worden afgedwongen.*

De beoogde landelijke infrastructuur[2] vereist wat betreft de opslag van gegevens dat iedere aangesloten zorgpartij een 'Goed Beheerd Zorgsysteem' heeft. Dit begrip wordt in § 2.1 toegelicht. Wat betreft het transport en de toegang tot gegevens geldt de vertrouwensketen als uitgangspunt bestaande uit drie stappen: identificatie, authenticatie en autorisatie. Dat betekent dat in alle processen van gegevensuitwisseling deze drie stappen moeten worden doorlopen. Dat geldt voor het bevragen van het BSN-gegevens op operationeel niveau, maar ook voor het bevragen van zorggegevens door zorgaanbieders of het uitwisselen van persoonsgegevens met zorgverzekeraars.
Identificatie en authenticatie worden in § 2.2 beschreven en autorisatie in § 2.3.

2.1. Goed Beheerde Zorgsystemen

De basisinfrastructuur voor de zorg is ontworpen om een veelheid aan applicaties in de zorg te ondersteunen. Deze applicaties draaien op zorginformatiesystemen. Zorginformatiesystemen

[2] Zie voor meer informatie de architectuur en de specificaties van Aorta, die te vinden zijn via: www.nictiz.nl.

mogen alleen op de basisinfrastructuur van de zorg worden aangesloten indien wordt voldaan aan een aantal eisen. Een Goed Beheerd Zorgsysteem (GBZ) is de organisatie van beveiliging en beheer die een zorgaanbieder realiseert met betrekking tot de uitwisseling van gegevens die in het kader van de dossiervoeringsplicht zijn geregistreerd. GBZ-eisen met betrekking tot beveiliging van de gegevens zijn gebaseerd op bestaande normen zoals de Code voor informatiebeveiliging (ISO IEC 17799), de norm voor informatiebeveiliging in de zorg (NEN 7510) en het beveiligingsadvies van het CBP. DE GBZ-eisen worden onderverdeeld in eisen die betrekking hebben op de zorgapplicatie (ICT-voorziening), op de implementatie en op de exploitatie. De eisen met betrekking tot de zorgapplicatie worden apart gekwalificeerd bij de leverancier van de betreffende applicatie. Voor de implementatie van de ICT voorziening zal de zorgverlener vaak een professioneel bedrijf ingezet hebben. Dit is in toenemende mate een Applicatie Service Provider (ASP), waarbij het fysieke beheer van de applicatie en van de database bij een daartoe gespecialiseerde onderneming is ondergebracht. De exploitatie-eisen hebben betrekking op de organisatorische en procedurele maatregelen die nodig zijn om de informatiebeveiliging te borgen. De mens is immers een belangrijke schakel in de keten, en meestal niet de sterkste als het gaat om de informatiebeveiliging. De eisen met betrekking tot componenten van de keten worden niet op het niveau van een wet geregeld, maar vanuit lagere regelgeving wordt ernaar verwezen. Normering van de overkoepelende architectuur wordt momenteel met het NEN besproken.

2.2. Identificatie en authenticatie

Identificatie behelst een tweetal zaken:

- identificatie van de communicerende partijen te weten zorgverleners en zorginstellingen en de medewerkers van een zorginstelling die namens een zorgverlener mag handelen (hulpmiddel hierbij zijn de door het UZI-register uitgegeven passen en certificaten) en
- de identificatie van de cliënt. Dit geschiedt met behulp van een BSN en indien noodzakelijk (zoals o.a. bij eerste contact) aan de hand van een WID document.

Identificatienummers zijn weliswaar betrouwbaarder bij gegevensverwerking dan NAW-gegevens, maar bij elektronische communicatie is het vervolgens van groot belang dat iemand daadwerkelijk degene is die hij zegt te zijn. Vast kunnen stellen dat iemand daadwerkelijk degene is die hij zegt te zijn wordt authenticatie genoemd. De authenticiteit van iemand vaststellen kan door het gebruik van digitale certificaten op basis van de zogenaamde Public Key Infrastructure (PKI). PKI is een internationaal erkend stelsel (op een hoog betrouwbaarheidsniveau) van organisatorische en technische regels waar authenticatie een belangrijk onderdeel van uitmaakt, aangevuld met de mogelijkheid om gegevens te versleutelen (waarborgt de vertrouwelijkheid) en de mogelijkheid om een elektronische handtekening te plaatsen (waarborgt de onweerlegbaarheid en de integriteit van verzonden informatie). Per inwerkingtreden van de wet op het gebruik van BSN in de zorg zullen zorgaanbieders die met BSN gaan werken zich voor hun elektronische communicatie identificeren en authenticeren met behulp van een PKI certificaat. Minimaal noodzakelijk is het systeemcertificaat dat de zorginstelling authenticeert, maar in de praktijk zullen ook de betreffende medewerkers een UZI-pas hiervoor krijgen. Hieronder wordt UZI nader toegelicht.

Unieke Zorgverlener Identificatie (UZI)

Voor de unieke identificatie en authenticatie van zorgaanbieders heeft het CIBG het Unieke Zorgverlener Identificatie register (UZI-register) ingericht. De UZI-pas kan verschillende functies vervullen in de elektronische communicatie. Zo kunnen zorgaanbieders zich met de UZI-pas identificeren en **authenticeren**, dat wil zeggen dat zij hun identiteit kunnen bewijzen. Wanneer een huisarts toegang zoekt tot een informatiesysteem of webapplicatie van bijvoorbeeld een ziekenhuis dan moet het ziekenhuis er zeker van kunnen zijn dat het daadwerkelijk de betrokken huisarts is die toegang zoekt. Andersom wil de huisarts met zekerheid kunnen vaststellen dat het informatiesysteem waartoe hij toegang zoekt daadwerkelijk tot het ziekenhuis behoort. Met

behulp van UZI-passen voor de zorgverlener en het systeem in de zorginstelling kan de benodigde zekerheid met betrekking tot authenticatie worden verkregen. Naast authenticatie vervult de UZI-pas een rol bij het zeker stellen van de **vertrouwelijkheid** van de communicatie omdat ook de functie of beroepsgroep van de zorgaanbieder op de pas is opgenomen. Wanneer zorginhoudelijke gegevens van een zorgconsument worden uitgewisseld tussen de huisarts en het ziekenhuis, is er zekerheid gewenst dat alleen de huisarts zelf en niemand anders de gegevens kan lezen die het ziekenhuis toestuurt. Door gebruik van de UZI-passen kan bovendien de zekerheid worden verkregen dat niemand de gegevens tijdens verzending van het ziekenhuis naar de huisarts kan lezen of wijzigen: het borgen van de **integriteit** van de communicatie. Ten slotte kan de UZI-pas worden gebruikt om **onweerlegbaarheid** te garanderen. Dat wil zeggen dat de huisarts bijvoorbeeld een recept, verwijzing of contract kan voorzien van een elektronische handtekening. De elektronische handtekening die de huisarts met een UZI-pas kan zetten, heeft in principe juridisch dezelfde waarde als een handtekening die de huisarts op papier zet. De mogelijkheid van een rechtsgeldige elektronische handtekening geldt alleen voor de UZI-passen die op naam door het register van zorgaanbieders zijn uitgegeven.

2.3. Autorisatie en logging

Autorisatie gaat over de vraag wie, onder welke voorwaarde, toegang mag krijgen tot de beschikbare cliëntengegevens. Ook gaat het om de vraag tot welke gegevens men toegang mag krijgen. De implementatie van autorisatie in de basisinfrastructuur, in eerste instantie beperkt tot autorisatie aangaande het landelijk elektronisch medicatiedossier en elektronische dienstwaarneming bij huisartsen, staat onder leiding van een autorisatiecommissie onder de stuurgroep ICT & Innovatie, met vertegenwoordigers van o.a. de NPCF, de KNMG, de KNMP en de NEN, onder voorzitterschap van de directeur van Nictiz.

Genoemde autorisatiecommissie zorgt er, ten aanzien van het landelijk elektronisch medicatie-dossier en elektronische dienstwaarneming huisartsen voor dat op projectmatige basis eerder vastgestelde autorisatievoorwaarden[3] in de praktijk ingevoerd worden. De voorwaarden:

- Voor de cliënt moet het helder zijn hoe met diens gegevens wordt omgegaan en voldaan wordt aan de rechten van de cliënt overeenkomstig de WGBO en de WBP;
- *Toegang* tot opgeslagen cliëntengegevens (in casu het medicatiedossier of het waarneemdossier van de huisarts) heeft de zorgverlener alleen als dat noodzakelijk is voor de behandeling van de cliënt. Ook dient de zorgverlener daarbij de UZI-pas te gebruiken;
- Zo mogelijk vooraf en anders achteraf moet vastgesteld kunnen worden of de toegang tot de cliëntengegevens noodzakelijk is geweest voor de behandeling van de cliënt. Misbruik wordt gestraft. Dankzij de UZI-certificaten en geavanceerde logging, wordt het beter dan ooit te voren mogelijk oneigenlijke toegang tot gegevens op te sporen;
- De zorgaanbieder is verantwoordelijk voor autorisatie (inclusief logging) in zijn eigen organisatie. Landelijk worden daar uniforme standaarden en adviezen voor aangereikt. De NEN start op 22 april as met het normalisatietraject Logging.

Het in praktijk brengen van de autorisatievoorwaarden is uitgewerkt in de gekwalificeerde systemen voor de projecten 'dienstwaarneming huisartsen' en 'het elektronisch medicatiedossier'. Dit betreft de ICT van huisartsenposten en huisartsen, van apothekers en ziekenhuizen en van het LSP.

---

[3] Zie onder andere de modelrichtlijn van de taakgroep Toegang tot patiëntgegevens van het WGBO-implementatieprogramma, in het boekje 'Toegang tot patiëntgegevens' dat in opdracht van VWS en Nictiz tot stand is gekomen met medewerking van vele koepelorganisaties en externe deskundigen in de zorgsector. Zie www.nictiz.nl

§ 3. Specifieke waarborgen m.b.t. bezwaar van de burger

In deze paragraaf zullen de maatregelen en waarborgen met betrekking tot het geheel of gedeeltelijk bezwaar aantekenen door de burger tegen gegevensuitwisseling in het kader van het landelijk EPD aan de orde komen, inclusief de gevolgen die dat heeft.

3.1. Zes weken bedenktermijn bij landelijke introductie EPD

Voor het EPD zal het principe van informed consent gelden, naar analogie van het model zoals dat door de NHS in de UK is gebruikt. Dit betekent dat burgers, na collectief te zijn geïnformeerd over (de invoering van) het EPD, de gelegenheid krijgen om gedurende 6 weken op voorhand een eventueel bezwaar centraal kenbaar te maken bij het Informatiepunt BSN in de zorg en landelijk EPD (voorheen 'klantenloket'), naast de mogelijkheid dit op elk gewenst moment te doen (zie 3.2).

Het informeren van de zorgconsumenten over (de invoering van) het EPD zal bij de start van de landelijke invoering van het EPD plaatsvinden. De landelijke voorlichting zal bestaan uit de volgende activiteiten:

a. landelijke campagne door middel van advertenties in huis-aan-huisbladen, eventueel aangevuld met radiospotjes
b. een brief aan elk huisadres vanuit het ministerie van VWS

Advertenties (en eventueel radiospotjes) en brief bevatten algemene informatie over het EPD, met als belangrijke aandachtspunten:

- invoering EPD zal de komende twee jaar zijn beslag krijgen
- rechten van zorgconsumenten, waaronder recht op inzage en bezwaar maken (altijd mogelijk)
- de komende 6 weken kunnen gebruikt worden om op voorhand bezwaar te maken
- aankondiging van brief bij eerste aanmelding van gegevens bij het LSP (indien geen bezwaar is gemaakt)

Zorgaanbieders zullen twee weken voorafgaand aan de start van de landelijke invoering per brief geïnformeerd worden. In deze brief zal naast algemene informatie over de start van de landelijke invoering van het EPD worden uitgelegd dat zorgconsumenten collectief geïnformeerd zullen worden en 6 weken bedenktijd wordt gegeven. Ook zal uitgelegd worden dat de 6 weken bedenktijd zal betekenen dat aansluitingen van systemen op het LSP wel gewoon doorgaan, maar dat er gedurende die 6 weken geen gegevens aangemeld of uitgewisseld kunnen worden. Deze voorlichting vanuit het ministerie ontslaat zorgverleners niet van de plicht om de zorgconsumenten te informeren.

3.2. Structurele bezwaarprocedure bij uitwisseling EPD

Naast de 6 weken bezwaartermijn bij de start van de landelijke invoering van het EPD, is er altijd de mogelijkheid om bezwaar aan te tekenen. Dit is reeds operationeel via het Informatiepunt (voorheen 'Klantenloket') en zal na verwachting elektronisch gerealiseerd kunnen worden door de patiënt zelf indien een adequaat authenticatiemiddel beschikbaar is (eNik, wellicht DigID+).

VWS is voornemens om de burger met een persoonlijke brief hierover te informeren op het moment dat er voor het eerst gegevens van de betreffende burger worden aangemeld bij het LSP. Dat kan enkele maanden na de 6 weken termijn zijn, indien pas op dat moment de regio van de betreffende burger aansluit. Voor deze procedure zal het LSP het betreffende BSN moeten voorzien van adresgegevens om de bedoelde persoonlijke brief te kunnen versturen.

Zowel dit algehele bezwaar (3.2) als het bezwaar van de 6 weken termijn (3.1), betreffen een 'hoofdschakelaar': er wordt niets uitgewisseld: geen aanmeldingen, geen index, geen opvragingen en geen verzendingen. Consequentie is wel dat als een patiënt besluit dit bezwaar in te trekken alle zorgverleners pas zullen aanmelden als ze vernemen dat de patient het bezwaar heeft ingetrokken. Deze consequentie is er niet bij gedeeltelijk bezwaar (zie 3.3).

3.3. Gedeeltelijke afscherming van inzage door burger

Als zorgconsument heeft de burger de mogelijkheid om bepaalde gegevens af te schermen voor anderen. Daarvoor zijn twee mogelijkheden: 1. aan de kant van de decentrale gegevensbron kunnen gegevens niet beschikbaar worden gesteld en 2. aan de kant van de opvrager kan inzage centraal worden geblokkeerd.
Bij het niet beschikbaar stellen van gegevens worden bepaalde gegevens uit het dossier afgeschermd voor anderen dan de betreffende arts aan wie de gegevens in vertrouwen worden gemeld. In algemene zin kan in overleg met de behandelaar worden vastgesteld wat er geregistreerd wordt in het dossier en wat er vanuit het dossier gecommuniceerd mag worden. In de praktijk zal het zo zijn dat de behandelaar de beroepsnormen volgt (al dan niet op schrift gesteld via richtlijnen) als het gaat om het voeren van een dossier: wat is nodig voor de behandeling en wat is nodig om zich te verantwoorden. Indien de patiënt bepaalde gegevens wil afschermen voor anderen, heeft hij hiertoe het recht. De betreffende zorgverlener is dan verplicht te wijzen op de impact die dit mogelijk heeft op vervolgbehandelingen door anderen. Afhankelijk van de mate waarin het systeem van de zorgverlener dit ondersteund, kunnen een heel dossier worden afgeschermd, een episode, een contact of bijvoorbeeld één uitslag (bv. een HIV bepaling). In de autorisatierichtlijnen die horen bij een landelijke zorgtoepassing kan het niveau hiervan worden vereist aan de systemen van de zorgaanbieders. Het decentraal kunnen afschermen van gegevens op verschillende nivo's is daarmee verplicht.

Bij het blokkeren van opvragende zorgverleners wordt op centraal niveau (in het LSP) door de patiënt aangegeven welke zorgverleners uitgesloten worden van inzage. Om de patiënten maximaal te faciliteren worden verschillende mogelijkheden uitgewerkt. Het aantal mogelijkheden zal echter niet oneindig zijn, want dan wordt het zo complex dat de patiënt denkt iets geregeld te hebben maar het dan net iets anders wordt vertaald. In het programma Autorisatie op Maat wordt een balans gezocht tussen de wensen van de patiënt enerzijds en de uniformiteit van enkele basale mechanismen anderzijds. Een eerste vooronderzoek is onlangs besproken met de autorisatiecommissie onder de Stuurgroep ICT&Innovatie. Daarin is onderzocht om aan patiënten die dat willen de mogelijkheid te geven autorisatie op maat zelf te definiëren. Dat houdt in dat een patiënt die vertrouwen heeft in de algemene beschermende maatregelen (uzi-pas, beroepsfilter, behandelrelatie) en de toegevoegde waarde ziet van beschikbaarstellen van gegevens, toch gedifferentieerd personen moet kunnen uitsluiten van inzage van die gegevens. Daarbij kan gedacht worden aan beroepsgroepen (alle apothekers), individuele zorgverleners (huisarts Jansen) en zorginstellingen (ziekenhuis). Realisatie van bepaalde vormen van autorisatie op maat vereisen een goede authenticatie van de patiënt. De eNik is hiervoor geschikt, andere vormen zoals DigID+ kunnen worden onderzocht.

Daarmee worden drie belangrijke wensen ondervangen: 1) patiënten die niets uitgewisseld willen hebben, kunnen de hoofdschakelaar uitzetten. Er wordt dan niets aangemeld en niets uitgewisseld. 2) patiënten die nu nog even niet mee willen doen, maar op termijn wellicht hun bezwaar opheffen, kunnen alle zorgverleners uitsluiten van inzage. De index zal in dit geval wel worden opgebouwd, zodat men bij het intrekken van het bezwaar niet langs alle zorgverleners hoeft. 3) patiënten die zelf op detailniveau willen bepalen wie ze uitgesloten moet worden, krijgen de mogelijkheid om per persoon, per instelling of per beroepsgroep dit te doen.

In al deze drie gevallen worden gegevens die bij de bron afgeschermd zijn nooit opgeleverd. Zonder aanmelding wordt immers niets opgeleverd. Indien er wel wordt aangemeld bij het LSP, dan betekent dit nog niet dat de gegevens beschikbaar worden gesteld; ze worden beschikbaar

gemaakt, dat wil zeggen het is mogelijk geworden om ze beschikbaar te stellen. Als bijvoorbeeld een huisarts meldt dat hij een dossier van een patiënt in beheer heeft, worden er geen medische gegevens uitgewisseld. Pas als een andere behandelaar een samenvatting van deze gegevens opvraagt wordt het LSP gebruikt om de vraag door te zetten naar de betreffende huisarts. Als er tussen de aanmelding en de opvraging een laboratoriumbepaling is afgeschermd, dan gaat deze niet mee in de oplevering van de gegevens waar om gevraagd wordt.

§ 4. Specifieke waarborgen m.b.t. behandelrelatie

In het kader van een behandelrelatie kan uitwisseling van de noodzakelijke medische gegevens fouten voorkomen en de behandeling optimaliseren. Omgekeerd is het niet toegestaan gegevens op te vragen indien men geen behandelrelatie met de patiënt heeft. Zo is ook de toegang tot het landelijk EPD niet toegestaan indien zorgverleners en de door hen gemandateerde medewerkers geen behandelrelatie hebben met de betreffende patiënt van wie gegevens worden opgevraagd.

Vanuit het oogpunt van zowel de privacy-bescherming als de algemene informatiebeveiliging is het wenselijk om deze toegangscontrole met ICT te ondersteunen. Onder het motto 'vertrouwen is goed, controleren is beter' kunnen technische filters helpen om het blokkeren van de toegang voor onbevoegden hard in te bouwen. Dit veronderstelt wel een eenduidige afbakening van bevoegden en onbevoegden. In een eerdere rapportage zijn de technische mogelijkheden onderzocht om de toegang tot het landelijk EPD via een controle op de behandelrelatie te reguleren.[4] In deze paragraaf zullen de nieuwe maatregelen en waarborgen met betrekking tot de behandelrelatie aan de orde komen.

4.1. Registratie van de behandelrelatie

4.1.1. registratie van de inschrijving per instelling

In aansluiting op de 4e conclusie zoals bovenvermeld, zal de eis van inschrijving technisch worden afgedwongen als men aansluit op het LSP. Dat betekent dat op het moment dat een zorgaanbieder toegang vraagt tot het landelijk EPD voor een bepaalde patiënt, het betreffende systeem van die zorgaanbieder eerst controleert of de patiënt is ingeschreven bij die zorgaanbieder. Met deze maatregel, die inmiddels van kracht is, kunnen bijvoorbeeld ziekenhuizen of apotheken waar een patiënt nooit geweest is, geen enkele opvraging doen van medische gegevens van die patiënt. Functioneel is hiermee de controle op behandelrelatie per zorginstelling geregeld. Ieder patiënt die met een hulpvraag bij een zorginstelling binnenkomt, zal eerst worden ingeschreven alvorens toegang verleend wordt. Zowel op de huisartsenpraktijk als op de huisartsenpost, in de apotheek als in het ziekenhuis is dit nu geregeld voor de gekwalificeerde systemen. In de komende kwalificaties is het structureel als eis en toets toegevoegd aan een GBZ.

4.1.2. Registratie van de behandelrelatie per zorgverlener

De behandelrelatie op het niveau van een zorgverlener is hiermee nog niet geregeld. Dat is voor solo-praktijken niet erg, want daar valt de instelling samen met de ene behandelaar. Voor grotere instellingen zijn aanvullende maatregelen nodig om onderscheid te maken tussen zorgverleners die betrokken zijn bij de behandeling van een patiënt en zorgverleners die dat niet zijn.

De eerste maatregel om de behandelrelatie te registeren op het niveau van de zorgverlener is een combinatie van inschrijving in de instelling en aanmelding door een zorgverlener. Bijkomend voordeel van de instellingsregistratie is dat aanmeldingen beschouwd kunnen worden als start van de behandelrelatie. Immers, aanmeldingen worden gedaan door of namens een zorgverlener die gegevens van de patiënt beheert en die de patiënt dus behandeld heeft in een instelling waar

[4] Haalbaarheidsonderzoek controle op behandelrelatie van Nictiz, sep2007

de patiënt ingeschreven is. Aanmeldingen kunnen daarom functioneel beschouwd worden als de start van een behandelrelatie tussen de patiënt van wie gegevens worden aangemeld en de zorgverlener die (of namens wie) de gegevens worden aangemeld, waarbij gegarandeerd is dat de betreffende patiënt ook ingeschreven is in de instelling vanwaaruit de aanmelding plaatsvindt.

De tweede maatregel om de behandelrelatie te registreren op het niveau van de zorgverlener is een combinatie van inschrijving in de instelling, opvraging van gegevens en een expliciete vraag of er sprake is van een behandelrelatie. Als een patiënt voor de eerste keer bij een zorgverlener komt, zijn er nog geen gegevens aangemeld. Voordat de zorgverlener toegang krijgt tot het landelijk EPD zal de patiënt ingeschreven moeten zijn bij de betreffende instelling. Indien er nog geen behandelrelatie met de betreffende zorgverlener is geregistreerd, wordt er expliciet gevraagd om een bevestiging van de behandelrelatie.

De derde maatregel om de registratie van de behandelrelatie mogelijk te maken is de beëindiging ervan. Hier zullen de beroepsgroepen richtlijnen voor kunnen uitgeven. Ten behoeve van het landelijke EPD zal het gefaciliteerd moeten worden. Voor het beëindigen van een behandelrelatie zullen deze zowel in de instelling als op het LSP in een aparte tabel opgenomen moeten zijn (apart van de aanmeldingen). Immers, een behandelrelatie kan worden beëindigd, terwijl de gegevens van de behandeling nog steeds bij de bron opvraagbaar moet kunnen blijven. Het beëindigen van een behandelrelatie vergt aparte berichten om deze op centraal en decentraal niveau actueel te houden.

De registratie van de behandelrelatie zal altijd decentraal ontstaan en geregistreerd worden. Het centraal beschikbaar hebben van deze registraties biedt de patiënt het voordeel dat er centraal inzage gegeven kan worden welke zorgverleners hebben aangegeven hebben dat zij een behandelrelatie hebben en welke de status die relatie heeft. Op welke wijze de centrale registratie georganiseerd wordt (bijvoorbeeld via berichten) wordt momenteel nader uitgewerkt.

4.2. Controle van de behandelrelatie door patiënt

Een degelijke registratie van de behandelrelatie kan niet voorkomen dat zorgverleners ten onrechte claimen een behandelrelatie te hebben. Met de eis tot inschrijving wordt dit risico beperkt tot die zorginstellingen waar de patiënt wel behandeld is. Sancties op misbruik vormen een onderdeel van de maatregelen voor handhaving en toezicht.

De maatregelen die waarborgen dat de patiënt de registratie van de behandelrelatie kan controleren, omvatten enerzijds het toevoegen van de status van de behandelrelaties aan de inzage in de logging en anderzijds de procedure om aan te geven dat er volgende de patiënt sprake is van ten onrechte verleende toegang.

Het mogelijkheid om in de logging van het LSP onderscheid te maken tussen opvragingen van zorgverleners die reeds aangemeld hebben enerzijds en opvragingen van zorgverleners die nog niets hebben aangemeld anderzijds is reeds aanwezig. Deze centrale log wordt 15 jaar bewaard, dus tot 15 jaar na dato kan reactief toezicht plaatsvinden op basis van de log bij het LSP. Het tonen van de aparte log (opvragingen door zorgverleners die geen dossier van de patiënt voeren) aan de patiënt is nog niet ingebouwd.

4.3. Toegangscontrole op basis van behandelrelatie

Hoewel bewust misbruik er niet helemaal mee voorkomen kan worden, is het technisch mogelijk om de registratie van de behandelrelatie te gebruiken als hard filter voor de toegang tot het landelijk EPD. De procedure is als volgt:

- Patiënten worden na een (doorgezette) hulpvraag ingeschreven in de systemen van de zorginstelling. Het BSN wordt op basis van de identificerende kenmerken opgevraagd of geverifieerd bij het SBV-Z.
- Behandelrelaties worden per patiënt geregistreerd in de systemen van de zorgaanbieder.
- Systemen zullen hierop worden getoetst in het kader van de kwalificatie.

- Bij invoering van de maatregel worden bestaande behandelrelaties van dossierbeheerders geregistreerd op het moment van aanmelding van dit dossier. Aanmelding veronderstelt inschrijving.
- Als gegevens worden opgevraagd door een zorgverlener wordt gecontroleerd of er een behandelrelatie is geregistreerd. Als dit het geval is, worden de opgevraagde gegevens getoond.
- Als dit niet het geval is, wordt nagegaan of de patiënt ingeschreven is bij de instelling. Is dat niet het geval dan kan er niets worden opgevraagd.
- Is de patiënt wel ingeschreven in de instelling, maar is er nog geen dosiser van de patiënt aangemeld, dan wordt er een pop-up scherm getoond. De zorgverlener moet de vraag beantwoorden of er een behandelrelatie bestaat met de betreffende patient. Indien met "ja" wordt geantwoord, wordt de behanderelatie geregistreerd en worden de opgevraagde gegevens getoond. Indien met "nee" wordt geantwoord, wordt er geen behandelrelatie geregistreerd en kunnen er geen gegevens worden opgevraagd.

Deze procedure zal in de eerstkomende release verplicht worden voor alle toepassingen van het landelijk EPD.

§ 5. Uitwerking van de terzake uitgangspunten van het CBP

(Uitgangspunten zoals weergegeven in de brief van het CBP d.d. 24 september 2004 aan de werkgroep inzake waarborgen rond de invoering van een BSN in de zorg en in het 'Advies wijziging Wet gebruik BSN in de zorg' van het CBP d.d. 14 juni 2007 aan ministerie van VWS)

1. *Het EPD heeft als doel patiëntgegevens, die berusten bij de behandelend arts, op elektronische wijze ter beschikking te stellen aan andere zorgverleners. Daarmee wordt de medische informatievoorziening op een hoger plan gebracht ten opzichte van de traditionele vormen van medische documentatie: er komt potentieel meer en betere informatie over de patiënt beschikbaar, waardoor de kwaliteit van de behandeling kan verbeteren. (...)Toegang tot de gegevens in een EPD moet in overeenstemming zijn met het hoofddoel van het EPD, namelijk een succesvolle medische behandeling door betere informatievoorziening.*

Uitwerking van dit advies:
Toegang tot het landelijk EPD is met de nieuwe maatregelen zo ingericht dat enerzijds recht gedaan wordt aan toegang tot behandelaars ten behoeve van een betere behandeling en anderzijds recht gedaan wordt aan de bescherming van de gegevens die in het kader van een (andere) behandelrelatie ontstaan zijn.

2. *Er is gekozen voor decentrale opslag, dat wil zeggen dat het EPD is vormgegeven als een systeem dat toegang biedt tot de medische dossiers die berusten bij de zorgverlener. Deze opzet sluit goed aan bij het medisch beroepsgeheim en bevordert het vertrouwen dat de patiënten in het systeem stellen: de zorgverlener blijft immers verantwoordelijk voor de gegevens en de vrees voor centrale opslag van gevoelige persoonsgegevens wordt bij voorbaat weggenomen.*

Uitwerking van dit advies:
Er is in Nederland niet gekozen voor een centrale opslag van medische gegevens. Zelfs de centrale index kan met een 'hoofdschakelaar' van bezwaar door de patiënt leeg gehouden worden. Afscherming van de gegevens vindt plaats in het kader van de behandelrelatie met de zorgverlener waar de gegevens ook ontstaan zijn. De controle op de behandelrelatie is eveneens decentraal, terwijl het gemak van de centrale inkijk in deze gegevens gerealiseerd wordt.

3. *Gezien het feit dat een zorgverlener in het algemeen zonder meer in staat is de declaratie van een behandeling naar de patiënt of diens verzekeraar te sturen en gezien de algemeen bestaande praktijk dat bij een eerste contact tussen zorgverlener en patiënt de laatste wordt opgenomen in de administratie van de zorgverlener, is het aannemelijk dat deze relatie wel degelijk kan worden gelegd in het systeem.*

Uitwerking van dit advies:
Door de inschrijving van een patiënt bij een zorginstelling te verplichten en onderdeel te maken van de toegangscontrole wordt een technische controle op de behandelrelatie per instelling gerealiseerd.

4. *Gewaarborgd dient te zijn dat slechts de personen die overeenkomstig de WGBO en andere wetgeving toegang mogen hebben tot medische gegevens, daar toegang toe hebben. De toegang moet dus per concreet geval, dat wil zeggen per hulpverlener en per behandelingsrelatie, geregeld worden, niet slechts per functie.*
5. *Vanuit het oogpunt van gegevensbescherming is het een essentieel vereiste dat de toegang voor onbevoegden wordt voorkomen. De beloofde voordelen van het EPD zijn echter alleen te realiseren indien het systeem voor bevoegde zorgverleners vrijwel onbeperkt beschikbaar is wanneer die zorgverleners de betrokken gegevens nodig hebben. Als wezenlijk beginsel moet derhalve gelden dat – naast de patiënt zelf – uitsluitend zorgverleners/bevoegde personeelsleden van een zorginstelling die op dat moment betrokken zijn bij de behandeling van de patiënt toegang mogen krijgen tot het EPD: tussen de patiënt en de zorgverlener die toegang wenst te krijgen tot diens EPD moet op dat moment een behandelrelatie bestaan (overeenkomstig art. 7: 457 BW).*

Uitwerking van deze adviezen:
Door de behandelrelatie vast te leggen als een relatie tussen een zorgverlener en een patiënt wordt het mogelijk om de toegang tot het landelijk EPD in concrete situaties te baseren op die behandelrelatie. Deze toegangscontrole gaat verder dan het huidige autorisatieprotocol dat gebaseerd is op het beroep van de zorgverlener en gaat verder dan de mandatering die niet gekoppeld hoeft te zijn aan de patiënt.

6. *Een geheel ander punt is of een geslaagde check op behandelrelatie in alle gevallen een voorwaarde moet zijn voor toegang tot iemands patiëntgegevens. In spoed- of noodgevallen waarin (nog) geen behandelrelatie bestaat of kan worden aangetoond, kan, ook naar het oordeel van het CBP, toegang worden verleend tot het individuele dossier. In zulke gevallen dient dan een specifieke log worden aangemaakt waardoor op zulke transacties achteraf gericht toezicht mogelijk wordt.*

Uitwerking van dit advies:
Onderscheid wordt gemaakt tussen opvragingen door zorgverleners die van de betreffende patiënt een dossier hebben ingericht en aangemeld enerzijds en opvragingen door zorgverleners die geen gegevens van de betreffende patiënt hebben, maar wel een behandelrelatie geregistreerd hebben. In de toepassing eSpoed geven zelfs de ambulancediensten aan dat de patient wordt ingeschreven en dat er sprake is van een behandelrelatie.

7. *Gezien het uitgangspunt dat niemand kan worden verplicht om aan het EPD deel te nemen, moet in het juridische kader worden voorzien in heldere procedures voor volledige en gedeeltelijke terugtrekking uit een EPD-systeem.*

Uitwerking van dit advies:
Volledige terugtrekking uit het landelijk EPD is reeds mogelijk via de 'hoofdschakelaar' met betrekking tot bezwaar. Deze kan via het Informatiepunt worden gerealiseerd en op termijn elektronisch via vormen van DigID (bv. eNik). Gedeeltelijke terugtrekking uit het landelijk EPD is mogelijk door bepaalde gegevens te onttrekken aan de uitwisseling. Afhankelijk van de wijze waarop dit in de decentrale systemen is ingebouwd, is het nu reeds mogelijk om contacten of dossierregels 'geheim' te verklaren. Gedeeltelijke bezwaar aantekenen is ook mogelijk door zorgverleners uit te kunnen sluiten van inzage.

§ 6. Bekrachtiging nieuwe waarborgen en maatregelen

In de volgende tabel wordt uiteengezet wanneer de in deze notitie besproken waarborgen en maatregelen van kracht kunnen zijn.

	Vanaf heden	Vanaf sep 2008	Vanaf medio 2009
Zes weken bedenktermijn voor bezwaar burgers		X	
Persoonlijke attentiebrief bij eerste aanmelding		X	X
Algeheel bezwaar tegen uitwisseling gegevens	X	X	X
Geheel/gedeeltelijk afschermen van gegevens	X	X	X
Gedifferentieerd blokkeren van inzage zorgverleners			X
Toegang EPD o.b.v. inschrijving patient bij instelling	X	X	X
Toegang EPD o.b.v. behandelrelatie	X	X	X
Toegang EPD o.b.v. geregistreerde behandelrelatie			X
Inzage geregistreerde behandelrelatie door patient			X
Controle opvragingen zonder aanmelding door toezicht	X	X	X

In het programma eSpoed wordt de uitwisseling van gegevens in spoed-situaties gerealiseerd en dat maakt het mogelijk voor patiënten om aan te geven dat de toegang tot het landelijk EPD uitsluitend voor spoed-situaties wordt toegestaan.

In het programma Autorisatie op Maat worden de mogelijkheden uitgewerkt om de patiënt vooraf in staat te stellen wie toegang krijgen tot het landelijk EPD en wie niet.

Op dit moment is het voor de koploper regio's die via het operationele LSP gegevens uitwisselen zodanig ingericht dat men centraal een algeheel bezwaar kan aangeven en decentraal gegevens geheel of gedeeltelijk kan blokkeren. Met betrekking tot de behandelrelatie is de borging hiervan op instellingsniveau via de verplichte inschrijving van de patiënt geregeld. Via aanvullende communicatie naar zorgaanbieders wordt benadrukt dat men alleen gegevens mag opvragen in het kader van een behandelrelatie met als doel het verbeteren van de behandeling. Mogelijkheden voor toezichthouder kunnen worden gerealiseerd via steekproefsgewijze controle in de praktijk of analyse van de centrale logging.

Per september van dit jaar zal hieraan worden toegevoegd de waarborgen rondom bezwaar via collectieve bedenktijd van 6 weken en via een persoonlijke brief bij eerste aanmelding waarin gewezen wordt op de mogelijkheden om bezwaar aan te tekenen.

In 2009 zal technisch gecontroleerd kunnen worden of men inderdaad alleen in het kader van een behandelrelatie het landelijk EPD bevraagt. Ook de controle door de patiënt zal dan gerealiseerd zijn. Verder zal het voor de patiënten mogelijk zijn om desgewenst zelf zorgverleners uit te sluiten van het opvragen c.q. inzien van hun landelijk EPD. De gegevensuitwisseling in spoed-situaties zal gestart zijn en uit de evaluatie moet blijken of hiermee aan de behoefte kan worden voldaan om gegevens uit te wisselen zonder geregistreerde behandelrelatie.