Toezichtkader EPD

in opdracht van
Ministerie van VWS

door
Mw. mr. J.A.L. Krabben

13 december 2010
versie 1.1

Versiebeheer

1.0	21 september 2010.....	definitieve eerste versie
1.1	13 december 2010.....	kleine tekstuele aanpassing in 4.2 n.a.v. de formele gezamenlijke reactie van CBP en IGZ

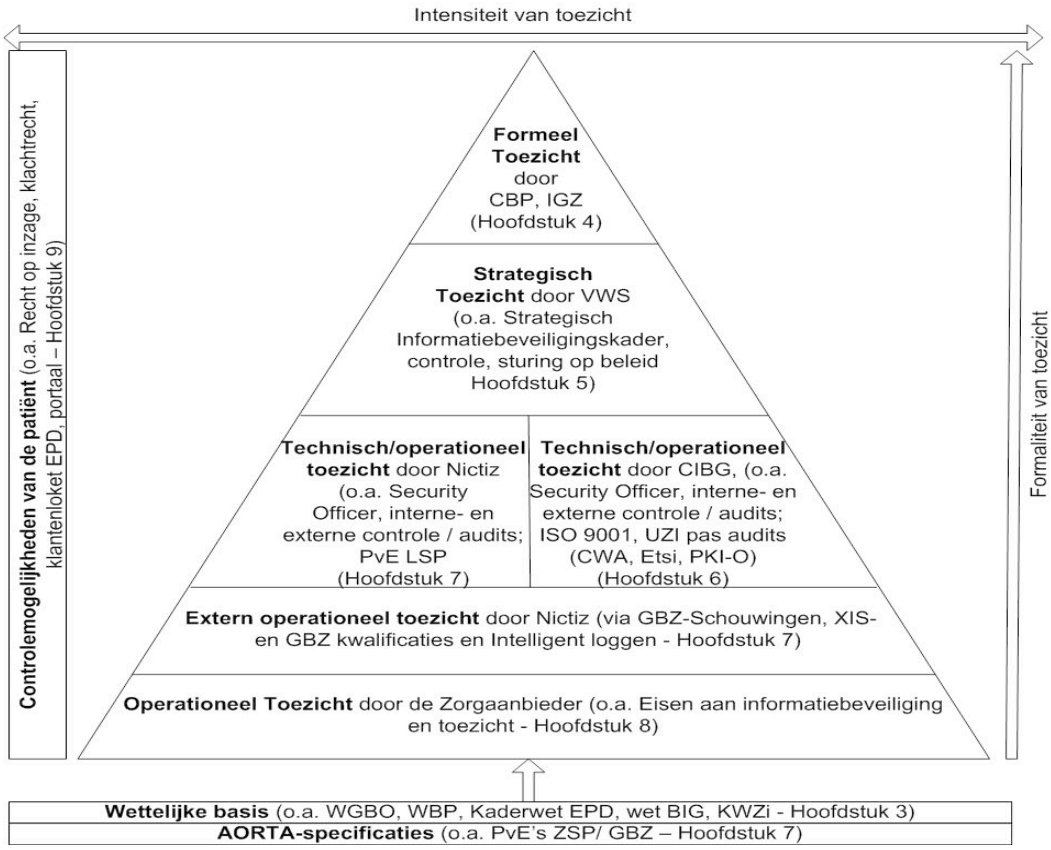
Inhoudsopgave

Managementsamenvatting

Inleiding
Voor een succesvolle invoering van het landelijk EPD is het noodzakelijk dat alle bij het EPD betrokken partijen vertrouwen kunnen hebben in een veilige en betrouwbare uitwisseling van patiëntgegevens. Bij de opzet en uitvoering van het landelijk EPD is daarom voorzien in technische, organisatorische en juridische waarborgen. Een belangrijk onderdeel van deze waarborgen is het toezicht op het EPD. Het toezicht op het EPD dient adequaat georganiseerd te zijn om het zorgvuldige, rechtmatige en veilige gebruik van het EPD te kunnen garanderen. Het doel van dit toezichtkader is een zo volledig mogelijk overzicht te geven van alle controle- en toezichtmaatregelen door alle betrokken partijen die tezamen het toezicht op het landelijk EPD vormgeven.

Toezichtmaatregelen
Rondom het landelijk EPD zijn vele maatregelen en mechanismen in werking die onderdeel zijn van het totale toezicht op het landelijk EPD. In dit kader wordt op elk niveau van het landelijk EPD besproken welke controle- en toezichtactiviteiten er plaatsvinden. Daarnaast wordt in een apart document ingegaan op enkele aanvullende maatregelen die het toezicht op het EPD kunnen completeren. Dit gebeurt in de vorm van aanbevelingen, welke zijn opgenomen in het document Aanbevelingen bij Toezichtkader EPD.

In dit toezichtkader worden de controle- en toezichtactiviteiten en mogelijkheden van alle bij het EPD betrokken partijen beschreven. Achtereenvolgens worden de controle- en toezichtactiviteiten van het ministerie van VWS, CIBG, NICTIZ en zorgaanbieders beschreven. Daarnaast wordt de toezichtbevoegdheid van het CBP en IGZ beschreven. Ook komen de controlemogelijkheden van de patiënt aan de orde.
Onderstaande figuur geeft de opzet van het document weer.



De toezicht- en controlemaatregelen steunen op procedure's en normen die zijn vastgesteld ten behoeve van de goede en rechtmatige uitvoering van het landelijk EPD, die op hun beurt in overeenstemming met het geldende wettelijke kader zijn. De eisen die gesteld worden aan het landelijk EPD zijn vervat in onder andere architectuurbeschrijvingen, Programma's van Eisen voor alle verschillende onderdelen en informatiebeveiligingsplannen en -procedures. Op de uitvoering conform eisen en procedures, normen en regelgeving wordt middels interne en onafhankelijke externe audits doorlopend getoetst. Ook de afspraken en procedures die gelden tussen Nictiz en CIBG en de door hen ingeschakelde dienstverleners, de operationele partners, worden door de dienstverleners zelf en door Nictiz en CIBG getoetst.

Formele toezichthouders
Het toezichtkader EPD beschrijft de rol van de formele toezichthouders CBP en IGZ. IGZ ziet toe op het leveren van verantwoorde zorg door zorgverleners, en houdt vanuit die invalshoek toezicht op het gebruik van het landelijk EPD. Het CBP houdt toezicht vanuit de invalshoek van de bescherming van persoonsgegevens en ziet derhalve toe op het rechtmatige verwerken van persoonsgegevens in het EPD en het voorkomen van misbruik van de gegevens. De toezichthouders hebben een onafhankelijke positie en hebben een zelfstandige bevoegdheid het toezicht naar eigen inzicht in te vullen en uit te oefenen. Het uitoefenen van toezicht op het EPD is onderdeel van de totale toezichtactiviteit van genoemde toezichthouders.

Uitgangspunt voor horizontaal toezicht
De maatregelen van controle en toezicht zoals die in dit document beschreven zijn dienen als goed uitgangspunt voor de inzet van horizontaal toezicht door de formele toezichthouders. Horizontaal toezicht kenmerkt zich door samenwerking tussen de toezichthouder en de onder toezicht staande partijen, waarbij deze partijen zoveel mogelijk zelf controleren en aantonen in overeenstemming met de (toezicht)regelgeving te handelen en te doen handelen. Aangevuld met de aanbevolen maatregelen in het document Aanbevelingen bij Toezichtkader EPD, zijn de omstandigheden voor horizontaal toezicht zeer goed. De toezichthouder kan op deze manier handelen op basis van rapportages over zelftoezicht, verklaringen van onafhankelijke auditors daarover en de resultaten van door externen uitgevoerde audits.

H1. Toezichtkader EPD

1.1 Inleiding

Dit Toezichtkader EPD gaat over toezicht op het zorgvuldige, rechtmatige en veilige gebruik van het landelijk Elektronisch Patiëntendossier (EPD). Het landelijke EPD is een virtueel dossier voor de zorg. Via een beveiligde infrastructuur, ook aangeduid als 'AORTA', zijn zorginformatie-systemen in Nederland met elkaar verbonden en kan relevante informatie over een patiënt elektronisch worden uitgewisseld. AORTA is een netwerk dat zorginformatiesystemen in Nederland met elkaar verbindt door middel van een verwijsindex in het Landelijk Schakelpunt (LSP). Alle patiëntgegevens zijn lokaal opgeslagen bij de verantwoordelijke zorgaanbieders. Het schakelpunt maakt slechts de uitwisseling van de gegevens mogelijk.

Voor een succesvolle invoering van het landelijk EPD is het noodzakelijk dat alle bij het EPD betrokken partijen vertrouwen kunnen hebben in een veilige en betrouwbare uitwisseling van patiëntgegevens. Bij de opzet en uitvoering van het landelijk EPD is voorzien in technische, organisatorische en juridische waarborgen.[1] Deze waarborgen worden onder andere beschreven in het 'Vertrouwensmodel landelijk EPD'[2] dat is opgesteld door Nictiz. Een belangrijk onderdeel van deze waarborgen is het toezicht op het EPD. Het toezicht op het EPD dient adequaat georganiseerd te zijn om het zorgvuldige, rechtmatige en veilige gebruik van het EPD te kunnen realiseren. In dit toezichtkader wordt een zo volledig mogelijk overzicht gegeven van alle controle- en toezichtmaatregelen door alle betrokken partijen die tezamen het toezicht op het landelijk EPD vormgeven.

Het Toezichtkader EPD is opgesteld op basis van informatie en documentatie van het ministerie van VWS, Nictiz, CIBG en andere bij het landelijk EPD betrokken partijen.[3]

1.2 Doelstelling en afbakening toezichtkader

Het doel van het toezichtkader EPD is om inzicht in en overzicht te geven van het totaalpakket van maatregelen dat alles tezamen het toezicht op het landelijk EPD omvat. Dit overzicht is van belang om aan alle betrokkenen bij het EPD het vertrouwen te bieden dat het toezicht op het EPD op een adequate en voldoende manier kan plaatshebben. Toezicht omvat alle handelen en alle instrumenten om naleving van regelgeving te onderzoeken, controleren, vast te stellen, te bevorderen en af te dwingen. Onder het toezicht dat in dit document wordt beschreven worden alle controle- en toezichtactiviteiten begrepen die zien op het juiste en rechtmatige gebruik van het landelijk EPD (en de gegevens die daarin beschikbaar komen) en die zien op voorkoming van misbruik of oneigenlijk gebruik van de toepassingen van het EPD. Daarbij gaat het zowel om controle en (zelf)toezicht op de eigen activiteiten door partijen, controle en toezicht door betrokken partijen op andere partijen in de EPD-keten, als om toezicht uitgevoerd door formele toezichthouders.

---

1 In dit verband is van belang dat juridische waarborgen mede zijn opgenomen in het wetsvoorstel van de Kaderwet elektronische zorginformatieuitwisseling, dat bij de Eerste Kamer ligt ter behandeling.
2 Vertrouwensmodel landelijk EPD, beschikbaar op www.nictiz.nl.
3 Waar relevant worden in de tekst de betreffende documenten genoemd.

1.3 Opzet

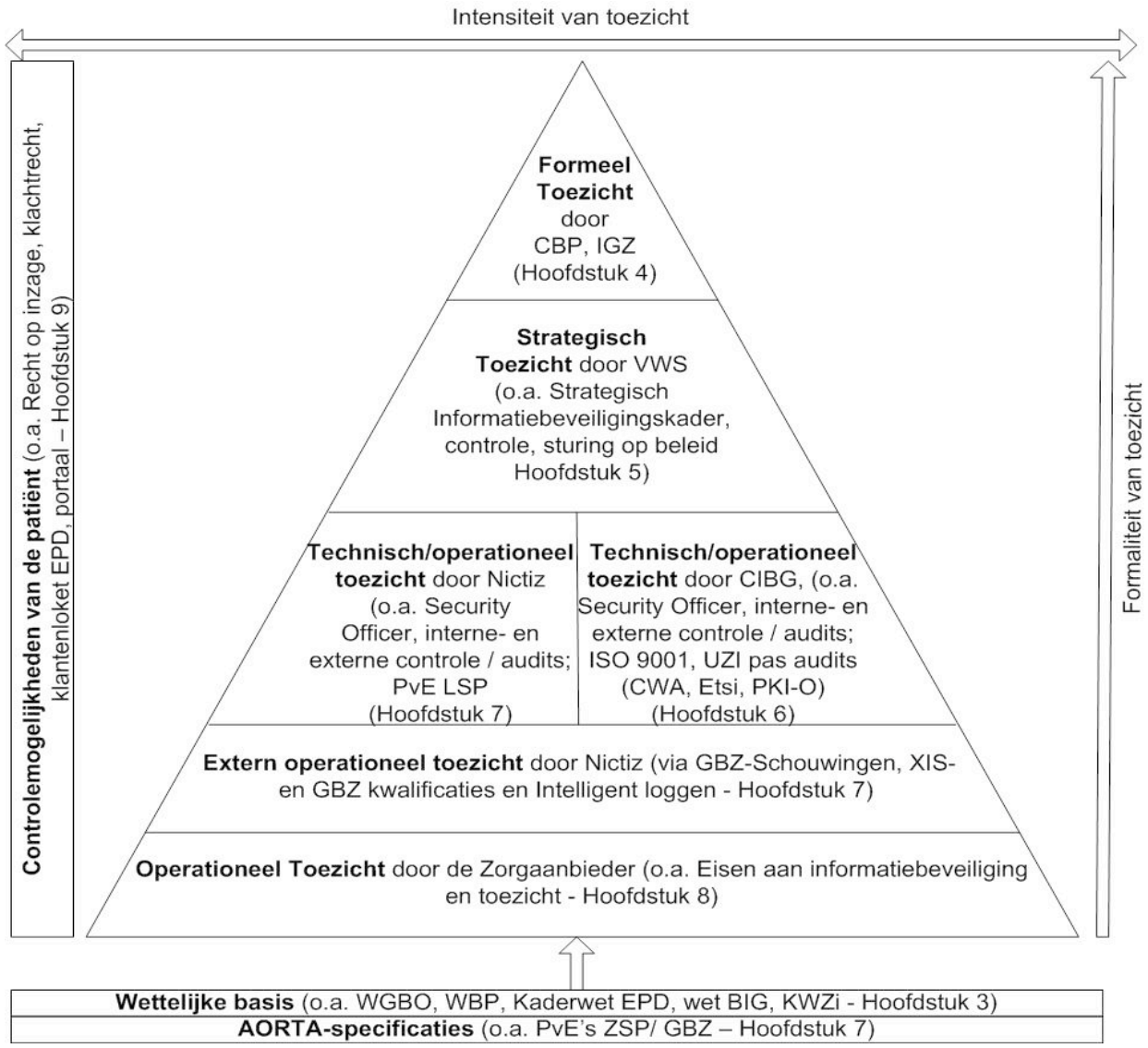
Bij het landelijk EPD zijn vele partijen betrokken. Dat geldt voor zorgaanbieders en patiënten zowel als voor partijen betrokken bij de opzet, de aansturing en uitvoering van het landelijk EPD. Rondom het landelijk EPD zijn vele maatregelen en mechanismen in werking die onderdeel zijn van het totale toezicht op het landelijk EPD. In dit kader wordt op elk niveau van het landelijk EPD besproken welke controle- en toezichtactiviteiten er plaatsvinden. Daarnaast wordt in een apart document ingegaan op enkele aanvullende maatregelen die het toezicht op het EPD kunnen completeren. Dit gebeurt in de vorm van aanbevelingen, welke zijn opgenomen in het document Aanbevelingen bij Toezichtkader EPD.

In dit document worden de verschillende niveaus van toezicht van elkaar onderscheiden door op elk niveau van betrokkenheid bij het EPD de controle- en toezichtactiviteiten te bespreken. Betrokkenen bij het EPD zijn in de eerste plaats de patiënten van wie de gegevens worden uitgewisseld in het EPD. Daarnaast zijn individuele zorgverleners betrokken bij het EPD, maar ook zorgaanbieders zoals groepspraktijken en zorginstellingen.

Het Ministerie van VWS is opdrachtgever voor het landelijk EPD zoals dat is opgezet en vanuit die hoedanigheid betrokken. Het Nationaal ICT instituut in de Zorg (Nictiz) is verantwoordelijk voor het beheer en de uitvoering van het LSP en een aantal uitvoerings- en ontwikkelingstaken met betrekking tot het landelijk EPD. Het CIBG is in de ontwikkeling en uitvoering van het EPD betrokken, onder andere als verantwoordelijke voor de uitgifte en registratie van UZI-passen. Nictiz en CIBG zetten derde partijen in bij uitvoering van een aantal taken.

De Inspectie voor de gezondheidszorg (IGZ) en het College bescherming persoonsgegevens (CBP) zijn de formele toezichthouders op het EPD. Ook het tuchtrecht en de rechter kan in het geval van een aangebracht geschil betrokken worden bij toezicht op het landelijk EPD.

Achtereenvolgens worden in dit toezichtkader de controle- en toezichtactiviteiten en mogelijkheden van alle bij het EPD betrokken partijen beschreven. Onderstaande figuur geeft de opzet van het document weer.



Figuur Toezichtpiramide landelijk EPD

H.2 Het landelijk EPD

2.1 Kenmerken van het landelijk EPD

In andere documenten wordt ingegaan op de inhoud en werking van het landelijke EPD. Voor een kort en leesbaar overzicht wordt verwezen naar het document 'Vertrouwensmodel landelijk EPD'[4]. In dit toezichtkader wordt volstaan met een korte aanduiding van de kenmerken voor een goed begrip van het toezichtkader. Bij het bespreken van het toezicht op verschillende niveaus wordt nader ingegaan op deze kenmerken waar relevant.

Het landelijke EPD is een virtueel dossier voor de zorg. Via een beveiligde infrastructuur, ook aangeduid als 'AORTA', zijn zorginformatie-systemen in Nederland met elkaar verbonden en kan relevante informatie over een patiënt elektronisch worden uitgewisseld.

Het landelijk EPD kenmerkt zich door een aantal principes. Zo is er sprake van decentrale opslag van patiëntgegevens in het bronsysteem van de zorgaanbieder, waarvoor deze verantwoordelijk is en blijft onder het EPD. AORTA bevat dus geen centrale database met patiëntgegevens. Om gegevens uit te kunnen wisselen dienen de betrokken systemen onderdeel te zijn van AORTA. Dit houdt in dat zij moeten zijn aangesloten op het Landelijk Schakelpunt (LSP), dat voor de uitwisseling van gegevens uit de bronsystemen wordt gebruikt. Het LSP omvat een verwijsindex die gezochte informatie vind en toegankelijk maakt en die er voor zorgt dat informatie naar de juiste zorgaanbieders toegezonden kan worden.

Om aan te mogen sluiten op het LSP dienen de zorgaanbieders te beschikken over een Goed Beheerd Zorgsysteem (GBZ), dat wil zeggen dat hun bronsysteem aan specifieke eisen moet voldoen ten aanzien van beveiliging en beheer om te kwalificeren. Die eisen zijn geformuleerd in het programma van eisen GBZ. Daarnaast verloopt de communicatie tussen een GBZ en het LSP altijd via een *Zorg Service Provider* (ZSP). Dat is een dienstverlener die de (besloten) infrastructuur voor de communicatie biedt tussen LSP en GBZ. De ZSP dient middels kwalificatie te voldoen aan een programma van eisen voor de ZSP.

AORTA kent verschillende zorgtoepassingen. Welke zorgaanbieders ervan gebruik kunnen maken verschilt per toepassing. Zo vindt bijvoorbeeld de uitwisseling in het kader van het Elektronisch Medicatiedossier alleen plaats tussen informatiesystemen van huisartsen, apothekers en medisch specialisten. Om het EPD te kunnen raadplegen, dienen zorgaanbieders in te loggen met hun UZI-pas welke wordt uitgegeven door het UZI-register. Een zorgaanbieder kan pas toegang krijgen tot de verwijsindex als hij verschillende stappen voor toegang tot het EPD succesvol heeft doorlopen. Die stappen houden identificatie, authenticatie en autorisatie van de (individuele) zorgaanbieder in, door middel van de UZI-pas (en het UZI-servercertificaat).

Voor het vaststellen van de identiteit van de patiënt in het EPD wordt het burgerservicenummer (BSN) van de patiënt gebruikt. De Sectorale Berichten Voorziening in de Zorg (SBV-Z) faciliteert deze toepassing.

[4] Dit document is beschikbaar op www.nictiz.nl.

Ten behoeve van het landelijk EPD heeft de Tweede Kamer ingestemd met de Kaderwet elektronische zorginformatieuitwisseling (kortweg Kaderwet EPD). Het wetsvoorstel ligt op dit moment bij de Eerste Kamer ter behandeling. Op grond van de Kaderwet EPD zal voor zorgaanbieders een wettelijke verplichting ontstaan om aan te sluiten op AORTA. Welke categorieën zorgaanbieders het betreft wordt nader geregeld in lagere regelgeving. Tot de Kaderwet EPD van kracht wordt, geschiedt aansluiting op vrijwillige basis.

Het LSP, het UZI-register en de SBV-Z worden gezamenlijk ook wel aangeduid als de 'centrale voorzieningen' van het EPD, het CIBG en Nictiz daarmee als 'centrale voorzieningen partijen'.

2.2 Opdrachtgever VWS

Het ministerie van VWS is opdrachtgever van het landelijk EPD zoals dat nu ontwikkeld is. Omdat het nut van betrouwbare zorginformatie voor landelijke toepassing wordt gekend en daarnaast het belang van veilige en betrouwbare uitwisseling wordt onderschreven is gekozen voor inrichting van een landelijk systeem conform uniforme, kenbare en op die aspecten gerichte vereisten.

Teneinde een aantal zaken ook juridisch te garanderen zijn verschillende voorwaarden van het EPD vastgelegd in het voorstel voor de Kaderwet elektronische zorginformatieuitwisseling en bijbehorende lagere regelgeving, welke ten tijde op opstellen van dit document ter goedkeuring bij de Eerste Kamer liggen. De kaderwet wordt besproken in hoofdstuk 3.

Als opdrachtgever voor opzet van het landelijk EPD voert het ministerie toezicht uit op de uitvoering van diverse taken door de centrale voorzieningen partijen.

2.3 CIBG en Nictiz

De centrale partijen in de ontwikkeling, uitvoering, opzet en beheer van het landelijk EPD zijn het CIBG en Nictiz. Het CIBG voert als uitvoeringsorganisatie van het ministerie van VWS het UZI-register en is verantwoordelijk voor ontwikkeling, uitgifte en registratie van UZI-passen. UZI-passen worden voor individueel gebruik uitgegeven aan zorgverleners als uniek identificatiemiddel voor toegang tot het EPD. Daarnaast is CIBG verantwoordelijk voor de Sectorale Berichten Voorziening in de Zorg (SBV-Z). SBV-Z faciliteert het juiste gebruik van het BSN voor identificatie van de patiënt. Ook is het CIBG verantwoordelijk voor de ontwikkeling van een Patiëntenportaal waarmee de patiënt in de nabije toekomst toegang kan krijgen tot de informatie die over hem beschikbaar wordt gesteld in het EPD. Tevens kan de patiënt via het portaal de beschikbaarheid van zijn gegevens beheren en aanpassen en de inzage in zijn gegevens door zorgverleners monitoren.

Nictiz wordt krachtens de Kaderwet EPD aangewezen als beheerder van het LSP.[5] Nictiz is verantwoordelijk voor ontwerp en ontwikkeling van de architectuur van AORTA. Daarnaast is Nictiz verantwoordelijk voor alle activiteiten die zien op de inrichting, het beheer en onderhoud van het LSP, en vele activiteiten die direct verband houden met de goede uitvoering van het landelijk EPD en controle en toezicht

[5] Artikel 2b lid 1 Uitvoeringsbesluit Kaderwet elektronische zorginformatieuitwisseling. Het wetsvoorstel en het daarop rustende besluit moet nog worden aanvaard door de Eerste Kamer.

daarop. Zowel Nictiz als CIBG maken bij uitvoering van hun taken gebruik van de dienstverlening van derden, waarop verderop in dit document ingegaan zal worden.

H.3 Juridisch kader

3.1 Toezichtwetgeving

Voor het toezicht op het landelijk EPD zijn een aantal wetten en daarop gebaseerde regelingen van belang. De Inspectie voor de Gezondheidszorg (IGZ) houdt toezicht op de kwaliteit van de zorg, door te toetsen of 'verantwoorde zorg' wordt geleverd. De basis voor de toets van verantwoorde zorg ligt besloten in de Kwaliteitswet zorginstellingen (Kwzi). Maar ook de toepassing van andere zorgwetten of normering (zoals NEN normering) kan aan de orde zijn bij invulling van het begrip verantwoorde zorg waaraan de IGZ toetst. Het College bescherming persoonsgegevens (CBP) ziet toe op de naleving van de Wet bescherming persoonsgegevens (Wbp) en aanverwante wetgeving (zoals de WGBO). Het CBP ziet ook toe op de verwerking van persoonsgegevens in het landelijk EPD. Het CBP heeft uitgebreid geadviseerd over de opzet en ontwikkeling van het EPD aan betrokken partijen en de minister van VWS over mogelijke risico's voor de gegevensverwerking en enkele verbeterpunten om die risico's te kunnen ondervangen. Een en ander gebeurde mede in het kader van de wettelijk vereiste advisering door het CBP over het voorstel voor de Kaderwet EPD.

3.2 Kwaliteitswet zorginstellingen (Kwzi)

De Kwaliteitswet zorginstellingen (Kwzi) verplicht zorginstellingen hun eigen kwaliteit te bewaken, te beheersen en te verbeteren. De wet noemt vier kwaliteitseisen waaraan een instelling moet voldoen: verantwoorde zorg, op kwaliteit gericht beleid, het opzetten van een kwaliteitssysteem en het maken van een jaarverslag. Zorginstellingen en georganiseerde zorgaanbieders zijn mede op grond van deze wet verplicht verantwoorde zorg aan te bieden. Het beleid dat de instelling voert, moet daarom gericht zijn op het in stand houden en verbeteren van de kwaliteit van zorg.

De in de Kwaliteitswet zorginstellingen vastgelegde normen voor het verlenen van zorg kunnen ook in het kader van het landelijk EPD relevant zijn. De Minister van VWS en de Inspectie voor de Gezondheidszorg (IGZ) houden toezicht op de naleving van deze normen.

3.3 Wet bescherming persoonsgegevens (Wbp)

De Wbp formuleert algemene en specifieke normen en uitgangspunten die bij de verwerking van persoonsgegevens in acht moeten worden genomen. De Wbp is van toepassing op het verwerken van persoonsgegevens. Een persoonsgegeven is ‘elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon’. Het 'verwerken' omvat elke handeling met betrekking tot de persoonsgegevens, zoals het inzien, opslaan en delen van de gegevens.

Het verwerken van persoonsgegevens, zoals patiëntgegevens uit het EPD en gegevens uit de verwijsindex, valt onder de werking van de Wbp. Ook loggegevens van een raadpleging van het Landelijk Schakelpunt, die betrekking hebben op patiënten of individuele zorgverleners die aan de hand van hun BSN of uniek identificatiemiddel kunnen worden geïdentificeerd, vallen onder de werking van de Wbp.

De normen in de Wbp richten zich grotendeels tot de ‘verantwoordelijke’ voor de

gegevensverwerking in de zin van de Wbp. Dit is degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Nictiz is de verantwoordelijke voor de verwerking van persoonsgegevens in het LSP.[6] Voor de gegevensverwerking in de bronsystemen die zijn aangesloten op het landelijk EPD zijn de betreffende zorgverleners de verantwoordelijke.

De Wbp formuleert daarnaast verschillende rechten van 'betrokkenen' waarvan gegevens worden verwerkt. Deze rechten corresponderen met rechten van patiënten zoals die zijn geformuleerd in de Wet op de geneeskundige behandelingovereenkomst (WGBO, zie hierna). In de Kaderwet EPD zijn enkele rechten specifiek voor de situatie in het landelijk EPD nader uitgewerkt.

In artikel 51 lid 1 Wbp wordt het CBP aangewezen als toezichthouder op de Wbp en aanverwante wetgeving.

Uitgangspunten van belang voor het EPD
De Wbp formuleert een aantal regels met betrekking tot de toelaatbaarheid en de kwaliteit van gegevensverwerking. Gegevens van patiënten, zoals dossiergegevens, verwijsgegevens (of indexgegevens) en loggegevens mogen slechts worden verwerkt voorzover daarvoor een verwerkingsgrond aan te wijzen is. Daarnaast is voor het verwerken van gegevens betreffende de gezondheid, waartoe deze gegevens gerekend moeten worden, een ontheffing nodig uit de Wbp. Dat komt omdat de gegevens gelden als bijzondere gegevens waarvoor een hoger verwerkingsrisico geldt en de Wbp een strenger regime kent dan voor niet bijzondere gegevens.

Een ontheffing voor het verwerken van gegevens betreffende de gezondheid bestaat voor toepassing van de gegevens voor de zorgverlening en in de uitdrukkelijke toestemming van de betrokkene. Overigens mogen de gegevens slechts worden verwerkt voor zover en zolang dat noodzakelijk is voor het doel van de verwerking. Daarnaast geldt voor deze gegevens dat verwerking achterwege moet blijven wanneer een geheimhoudingsplicht aan het (verder) verwerken in de weg staat. Dit correspondeert met het medisch beroepsgeheim dat geregeld is in de WGBO en in de Wet BIG.

Een uitgangspunt is dat persoonsgegevens op behoorlijke en zorgvuldige wijze dienen te worden verwerkt. Dat betekent ook dat persoonsgegevens voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden dienen te worden verkregen, dat ze juist en niet bovenmatig dienen te zijn en niet langer worden bewaard dan noodzakelijk is.

Beveiliging
Op grond van artikel 13 Wbp dient de verantwoordelijke passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. 'Passend' betekent in dit verband dat de beveiliging in overeenstemming is met het risico van de gegevensverwerking (in verband met onder andere de aard van de gegevens en het gebruik) en de stand van de techniek.

Deze open norm kan in de zorg op passende wijze worden ingevuld, door te voldoen aan de bestaande (Nederlandse) normen voor informatiebeveiliging in de

[6] Mede afhankelijk van invoering van de Kaderwet elektronische zorginformatieuitwisseling en aanwijzing in artikel 2b van het daarop steunende Besluit gebruik burgerservicenummer in de zorg. Zie ook de brief van 21 juli 2005 van CBP aan Nictiz (z2005-0505) en de brief van 16 april 2009 van CBP aan het ministerie van VWS (z2009-00164), omtrent verantwoordelijkheid in de zin van de Wbp. Zie in dit verband ook de Aanbevelingen bij Toezichtkader EPD van 21 september 2010.

gezondheidszorg NEN7510/7511/7512. Dit blijkt uit toetsingskaders die door het CBP en de IGZ gehanteerd worden in onderzoek.

Uit de Wbp volgt ook dat het betrekken van een derde bij de gegevensverwerking een aantal verplichtingen opwerpt voor zowel de verantwoordelijke als de derde, wanneer deze optreedt als bewerker in de zin van de Wbp. Artikel 14 Wbp regelt de verhouding tussen de verplichtingen van beide partijen. De verantwoordelijke moet erop toezien dat hij door of ondanks het inschakelen van de bewerker de verplichtingen uit de Wbp die op hem rusten kan waarmaken. Zo zal de bewerker moeten voldoen aan de eisen voor gegevensbeveiliging zoals die ook op de verantwoordelijke rusten. Het is noodzakelijk dat partijen de afspraken met betrekking tot de gegevensverwerking schriftelijk vastleggen.

3.4 Wet op de geneeskundige behandelingsovereenkomst

De rechtsverhouding tussen hulpverlener en patiënt is geregeld in Wet op de geneeskundige behandelingsovereenkomst (WGBO). In de WGBO staan de rechten van de patiënt beschreven alsook de rechten en plichten van de hulpverlener.

Op grond van de WGBO (onderdeel van Boek 7 Burgerlijk Wetboek) heeft de hulpverlener een dossierplicht, die hem ertoe verplicht een dossier op voorgeschreven wijze bij te houden en conform de bewaartermijn te bewaren. De patiënt heeft op grond van de wet onder andere recht op inzage in het dossier en recht op correctie of aanvulling van het dossier. In beginsel is er ook recht op vernietiging van de gegevens. De hulpverlener heeft een geheimhoudingsplicht over het dossier ten opzichte van anderen dan de patiënt. Dit geldt behoudens de bij wet gemaakte uitzonderingen.

Uitgangspunt is dat alleen met toestemming van de patiënt inlichtingen over hem of gegevens uit het dossier aan anderen worden verstrekt. Verstrekking kan echter zonder toestemming plaatsvinden in het geval van een wettelijke verplichting. Toestemming van de patiënt is evenmin vereist voor verstrekking aan degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst. Een en ander geldt voorzover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden, en behoudens een door de patiënt geuit bezwaar tegen verstrekking van de gegevens. Op de hulpverlener, in de WGBO zowel de zorginstelling als de individuele zorgverlener, rust de verantwoordelijkheid en zorgplicht om de verplichtingen ten aanzien van het patiëntdossier te waarborgen. In de uitvoering van het EPD en het toezicht daarop is dat een belangrijk gegeven.

In het kader van het landelijk EPD komen al deze aspecten van het verwerken van de gegevens aan de orde. Verwerking in het EPD dient dan ook overeenkomstig de WGBO te geschieden.

Overigens is overtreding van het medisch beroepsgeheim ook in het Wetboek van Strafrecht strafbaar gesteld.

3.5 Wet op de beroepen in de individuele gezondheidszorg

Voor de positie van de individuele zorgverlener is voorts nog de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG) relevant in verband met het toezicht op het

EPD. Deze wet regelt de registratie van beroepsbeoefenaars en stelt normen met betrekking tot de kwaliteit van de beroepsuitoefening. Ook het medisch beroepsgeheim is verankerd in de Wet BIG. Daarnaast is van belang dat de Wet BIG het tuchtrecht voor beroepsbeoefenaars in het leven roept.

De Wet BIG heeft als doelstelling de kwaliteit van de beroepsuitoefening te bevorderen en te bewaken en de patiënt te beschermen tegen ondeskundig en onzorgvuldig handelen door beroepsbeoefenaren. De IGZ kan naleving van de Wet BIG toetsen in zijn toezicht. Regels omtrent het omgaan met persoonsgegevens, zoals het in artikel 88 Wet BIG vastgelegde medisch beroepsgeheim, worden ook door het CBP getoetst.

UZI-passen
De BIG registratie is voor het EPD en het toezicht daarop van belang omdat alleen BIG-geregistreerde zorgverleners een UZI-pas kunnen aanvragen waarmee, onder voorwaarden, toegang gekregen kan worden tot het landelijk EPD. Gemandateerde medewerkers kunnen met een UZI-pas op naam, onder omstandigheden, ook bevoegd zijn voor toegang tot het EPD.

Tuchtrecht
Voor de bij wet geregelde beroepen voorziet de Wet BIG in tuchtrechtspraak. In het kader van het toezicht op het EPD neemt ook het tuchtrecht een betekenisvolle plaats in. Het tuchtrecht dient immers het bewaken van de zorgvuldige beroepsuitoefening. De Wet BIG kent twee tuchtnormen. De eerste heeft betrekking op de te betrachten zorgvuldigheid bij het verlenen van zorg aan de patiënt. De tweede geldt ten aanzien van andere gedragingen die strijdig zijn met het belang van een goede uitoefening van de individuele gezondheidszorg, waaronder mede enig handelen of nalaten in strijd met de artikelen 13h en 13hb van de voorgestelde Kaderwet EPD.[7] De tuchtrechter behandelt klachten over overtreding van tuchtrechtnormen en legt bij een gegrondverklaring een maatregel op.

De Wet BIG kent naast tuchtrechtelijke maatregelen ook strafbepalingen.

3.6 Kaderwet elektronische zorginformatieuitwisseling

Zoals hierboven al beschreven ligt het voorstel voor de Kaderwet elektronische zorginformatieuitwisseling (Kaderwet EPD)[8] op dit moment ter goedkeuring voor aan de Eerste Kamer. In dit wetsvoorstel zijn de inrichting van en de aansluiting op het Landelijk Schakelpunt (LSP) geregeld. Daarnaast legt de Kaderwet EPD de zorgaanbieder en de beheerder van het LSP een aantal verplichtingen op en wordt een aantal rechten voor de patiënt beschreven. Het toezicht op het EPD ziet mede op de naleving van deze verplichtingen en rechten.

De Kaderwet EPD betreft een wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg (Wbsn-z). Deze wijzigingswet voegt onder andere een hoofdstuk ('Hoofdstuk 2A Elektronisch patiëntendossier') toe aan de al bestaande Wet gebruik burgerservicenummer in de zorg. Deze wet wordt met de wijziging hernoemd tot Kaderwet elektronische zorginformatieuitwisseling.

---

[7] Het voorstel voor de Kaderwet EPD ligt ter behandeling bij de Eerste Kamer.
[8] Kamerstukken I 2008-2009, 31 466, A.

Landelijk Schakelpunt en Nictiz
Krachtens de Kaderwet EPD wordt Nictiz aangewezen als beheerder en daarmee verantwoordelijk voor het beheer en de inrichting van het LSP. De voorgenomen kaderwet bepaalt dat het LSP een elektronische landelijke verwijsindex dient te bevatten. Ook dient te zijn voorzien in logging van raadplegingen en in een toepassing waarmee de patiënt zijn gegevens en de hem betreffende logging elektronisch kan opvragen en afschermen voor (specifieke) raadpleging. Daarnaast dient Nictiz via het Klantenloket EPD de uitoefening van bepaalde patiëntenrechten mogelijk te maken. Zo heeft de patiënt onder andere recht op inzage en verwijdering van zijn indexgegevens in het LSP.

Zorgaanbieders
Voor zorgaanbieders regelt de kaderwet welke soort gegevens van patiënten zij dienen vast leggen in het bronsysteem teneinde de kwaliteit en uniformiteit van de beschikbare gegevens te reguleren.

Een groot deel van de voorschriften in de Kaderwet EPD is gericht aan zorgaanbieders. Bij overtreding van deze voorschriften kan de minister van VWS een zorgaanbieder in het kader van het toezicht een bestuurlijke boete opleggen.

Geen toegang
BIG-geregistreerden die werkzaamheden verrichten als bedrijfsarts, verzekeringsarts of keuringsarts, zullen geen toegang krijgen tot de voorzieningen van het LSP of het landelijk EPD. Welke beroepsbeoefenaars, onder voorwaarden, wel toegang kunnen krijgen tot het EPD is afhankelijk van welke zorgtoepassing het betreft.

Strafrechtelijke bepaling
Hoewel sanctionering van misbruik van het EPD langs andere weg reeds mogelijk is, acht de minister het van belang dat de strafrechter de mogelijkheid krijgt om bij misbruik van het EPD, een beroepsbeoefenaar van het recht te ontzetten zijn beroep uit te oefenen. De minister is daarom voornemens een strafrechtelijke bepaling op te nemen in de kaderwet. Onder huidig recht kan misbruik van het EPD strafrechtelijk worden vervolgd op grond van overtreding van het artikel inzake computervredebreuk (art. 138a Wetboek van Strafrecht) of in verband met een schending van de geheimhoudingsplicht (art. 272 Wetboek van Strafrecht).

3.7 NEN 7510

De NEN 7510 norm is de Nederlandse norm voor informatiebeveiliging in de zorg. Deze is gebaseerd op de Code voor Informatiebeveiliging (NEN-ISO/IEC 27002), de algemene norm voor informatiebeveiliging. De NEN 7510 en subnormen NEN 7511 en NEN 7512 worden beschouwd als een goede uitwerking van beveiligingsvereisten in de zorg. In rapportage van onderzoek bij ziekenhuizen in Nederland naar de stand van informatiebeveiliging door het CBP en de IGZ gezamenlijk, is door de toezichthouders vastgesteld dat het voldoen aan de NEN 7510 in de gezondheidszorg kan worden beschouwd als het voldoen aan de beveiligingseisen die worden gesteld in artikel 13 Wbp.

Sinds de invoering van het burgerservicenummer in de zorg en de verplichte verwerking daarvan bij persoonsgegevensverwerking van cliënten in de zorg, dient de gegevensverwerking in de zorg ook wettelijk te voldoen aan de NEN 7510. Dit volgt

uit artikel 2 van de Regeling gebruik burgerservicenummer in de zorg.

Gesteld kan worden dat daarmee ook de informatiebeveiliging van het LSP dient te voldoen aan de NEN 7510. Ook een GBZ dient, als zorgsysteem van een zorgaanbieder, te voldoen aan de eisen van de NEN 7510. Een ZSP die als bewerker voor een GBZ optreedt dient derhalve in overeenstemming met de NEN 7510 te handelen.

De NEN 7510 geeft algemene richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die een organisatie in de gezondheidszorg moet treffen ter beveiliging van de informatievoorziening. De NEN 7512 is specifiek gericht op de elektronische gegevensuitwisseling in de zorg.

Informatiebeveiliging omvat volgens de NEN 7510 "maatregelen om verstoringen in de zorgvuldige en doelmatige informatievoorziening te voorkomen en eventuele schade als gevolg van desondanks optredende verstoringen te beperken". De NEN 7510 noemt onder andere de volgende aspecten:

- *vertrouwelijkheid:* het beschermen van gegevens tegen onbevoegde kennisname;
- *integriteit:* het waarborgen dat gegevens niet ongecontroleerd worden gewijzigd of verloren gaan;
- *beschikbaarheid:* het zekerstellen dat gegevens en informatiediensten op de gewenste momenten beschikbaar zijn voor gebruikers;
- *onweerlegbaarheid:* het waarborgen dat het vastleggen van gegevens of het verzenden van een bericht niet kan worden ontkend.

H.4 Formeel toezicht

4.1 De onafhankelijke toezichthouders

De formele toezichthouders op het landelijk EPD zijn de Inspectie voor de Gezondheidszorg (IGZ) en het College bescherming persoonsgegevens (CBP). Zoals in het juridisch kader al even aan de orde is geweest is IGZ toezichthouder op het leveren van verantwoorde zorg door zorgverleners. Vanuit die invalshoek houdt IGZ toezicht op het gebruik van het landelijk EPD. Het CBP houdt toezicht op het landelijk EPD vanuit de invalshoek van de bescherming van persoonsgegevens. Het CBP ziet derhalve toe op het rechtmatige verwerken van persoonsgegevens in het EPD en het voorkomen van misbruik van de gegevens. De toezichthouders hebben een onafhankelijke positie en hebben een zelfstandige bevoegdheid het toezicht naar eigen inzicht in te vullen en uit te oefenen. Het toezicht op het EPD is onderdeel van de totale toezichtactiviteit van genoemde toezichthouders.

Omdat de wijze van omgang met persoonsgegevens onderdeel is van toezicht op de kwaliteit van zorgverlening waarop door IGZ wordt toegezien, kunnen de aan IGZ en CBP opgedragen taken of de uitoefening van de aan IGZ en het CBP toegekende bevoegdheden elkaar raken of overlappen. Om die reden hebben de IGZ en het CBP een samenwerkingsconvenant met elkaar gesloten. In het convenant hebben zij afspraken gemaakt over het uitoefenen van toezicht op de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer binnen de gezondheidszorg in geval van samenlopende bevoegdheden[9]

4.2 IGZ

De Inspectie voor de Gezondheidszorg is belast met het onafhankelijk staatstoezicht op de volksgezondheid en ziet toe op de naleving van diverse zorgwetten, waaronder de Wet BIG, de Kwaliteitswet zorginstellingen en de Wet klachtrecht cliënten zorgsector. Op 13 april 2010 heeft de Eerste kamer ingestemd met het wetsvoorstel '*Uitbreiding van de bestuurlijke handhavingsinstrumenten in de wetgeving op het gebied van de volksgezondheid*'[10]. Dit wetsvoorstel breidt in een aantal wetten op het gebied van de volksgezondheid de handhavingsmogelijkheden van de minister van Volksgezondheid, Welzijn en Sport uit met de bevoegdheid tot het opleggen van bestuurlijke boetes. Hierdoor mag de IGZ boetes opleggen aan zorginstellingen die in de zorg te kort schieten, in bij wet geregelde gevallen. IGZ is ingevolge de Kwzi uitsluitend bevoegd ten aanzien van 'zorgverleners' als gedefinieerd in die wet.

Tevens heeft de IGZ in het kader van het toezicht de bevoegdheid gekregen om zonder toestemming van de patiënt het dossier in te zien, indien dat voor de goede uitoefening van haar taken noodzakelijk is. Dat betekent dat de Inspectie in voorkomende gevallen ook inzage kan krijgen in gegevens die worden uitgewisseld in het kader van het landelijk EPD, iets dat voor het toezicht op het EPD van belang is. IGZ heeft aangegeven, indien aan de orde, meldingen en rapportages over onrechtmatig gebruik van (gegevens in) het landelijk EPD te willen ontvangen van andere partijen betrokken bij controle en toezicht op het EPD, zoals bijvoorbeeld Nictiz en CIBG. Het gaat daarbij in de eerste plaats om situaties die de kwaliteit van de zorg

[9] www.cbpweb.nl/downloads_samenwerking/samenw_prot_cbp_igz.pdf
[10] Eerste Kamer, vergaderjaar 2007–2008, 31 122, A

kunnen betreffen.

4.3 CBP

Op grond van artikel 51 lid 1 Wbp is het College Bescherming Persoonsgegevens aangewezen als toezichthouder op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de Wet bescherming persoonsgegevens bepaalde. In het kader van het EPD zijn naast de Wbp, de WGBO en de Kaderwet EPD relevant voor het toezicht door het CBP.

Het College kan op eigen initiatief of op verzoek van een belanghebbende, een onderzoek instellen naar de wijze waarop persoonsgegevens worden verwerkt. De verantwoordelijke is daarbij verplicht om inzage te verschaffen in de noodzakelijke gegevens en systemen. Hij kan zich daarbij tegenover het CBP niet beroepen op een geheimhoudingsplicht. In het kader van toezicht op het landelijk EPD is het CBP derhalve bevoegd om op elke locatie van het landelijk EPD, zowel bij de zorgaanbieder, bij het LSP als bij een ICT dienstverlener inzage te verlangen in de gegevensverwerking.

Het CBP kan ten behoeve van naleving en handhaving een bestuurlijke boete opleggen of bestuursdwang toepassen.

Het CBP heeft het ministerie van VWS en andere betrokkenen aangegeven dat het vindt dat de verwerking van gegevens in het landelijk EPD een continue en specifiek gericht toezicht behoeft. Iets dat in de huidige situatie, gelet op de capaciteit van de toezichthouder en de overige toezichtactiviteit waarvoor de toezichthouder verantwoordelijk is, niet in de eerste plaats door de toezichthouder zelf, noch uitsluitend door hem, kan worden uitgeoefend. De controle- en toezichtactiviteiten die door andere partijen op het landelijk EPD worden uitgevoerd zullen derhalve gestalte moeten geven aan het specifieke toezicht dat nodig is en zal zodanig moeten zijn ingericht dat de toezichthouder het totale toezicht, dat wil zeggen gecombineerd met zijn eigen activiteiten, voldoende acht.

4.4 De rechtspraak

Het sluitstuk van toezicht is rechtspraak. De rechter is de hoogste instantie die uitsluitsel geeft over correcte toepassing en naleving van de wet. Patiënten kunnen naast de toezichthouder ook de rechter inschakelen wanneer zij misbruik van het EPD aanhangig zouden willen maken. De toezichthouders kunnen op hun beurt bijvoorbeeld het Openbaar Ministerie inschakelen als zij menen dat het strafrecht van toepassing is op een bepaalde situatie. Daarnaast kan de rechter ook het oordeel van de toezichthouder toetsen in een aangebracht geschil.

Patiënten, zorgverleners en de IGZ kunnen bovendien de tuchtrechter inschakelen. Deze behandelt klachten over zorgverleners op wie de Wet BIG van toepassing is en die in strijd met de Wet BIG zouden hebben gehandeld of nagelaten. De tuchtrechter legt bij gegrondheid van de klacht een tuchtmaatregel op overeenkomstig de Wet BIG.

H.5 Toezicht door VWS

5.1 Opdrachtgever VWS

Het ministerie van VWS (VWS) werkt samen met Nictiz, CIBG en betrokken partijen en organisaties aan de invoering en ontwikkeling van het landelijk EPD. Als opdrachtgever is het ministerie eindverantwoordelijk voor het beleid ten aanzien van de invoering van het EPD. VWS ontwikkelt het beleid en ontwerp de wetgeving ten behoeve van het EPD. Daarnaast ondersteunt VWS de ontwikkeling van onderdelen van het EPD en uitvoering van het beleid in programma's en projecten. VWS controleert en stuurt aan op de opvolging en uitvoering van het beleid.

Op verschillende manieren dragen de activiteiten van VWS bij
aan het toezicht op het landelijk EPD. Zo ziet het ministerie toe op de uitvoering en ontwikkeling van de EPD-dienstverlening volgens vastgestelde kaders, terwijl de kaders op hun beurt steeds worden getoetst op het voldoen aan wet- en regelgeving, vastgelegde afspraken over de opzet, werking en voorwaarden van het EPD, alsmede de kwaliteitseisen die zijn gesteld aan beveiliging, integriteit en vertrouwelijkheid van het landelijk EPD.

VWS ontwikkelt het beleid ten aanzien van de informatiebeveiliging van het landelijk EPD. Informatiebeveiliging en beveiligingsbeleid is van groot belang voor het toezicht op het EPD omdat de informatiebeveiliging van het landelijke EPD, naast goed beheer en correct gebruik van het landelijk EPD, het voornaamste onderwerp van het toezicht is (de toezichthouders IGZ en CBP zien vanuit hun eigen invalshoek beide toe op adequate informatiebeveiliging als voorwaarde voor verantwoorde zorg en de zorgvuldige verwerking en bescherming van persoonsgegevens) én adequate informatiebeveiliging in zichzelf ook controle en toezicht borgt.

5.2 Informatiebeveiligingsbeleid

Het beleid ten aanzien van de informatiebeveiliging van het landelijk EPD dient ertoe zowel de beschikbaarheid, integriteit en vertrouwelijkheid van de EPD-en BSN-dienstverlening, als de controleerbaarheid te waarborgen, door middel van een stelsel van toezicht en controle.

Genoemde aspecten worden als kwaliteitsaspecten beschouwd en als volgt gedefinieerd:

- *Beschikbaarheid:* het zekerstellen dat de gegevensverwerking door de Centrale Voorzieningen Partijen (CVP) Nictiz en CIBG en de gegevensuitwisseling ten behoeve van de EPD- en BSN-dienstverlening op de noodzakelijke tijdstippen bestand is tegen negatieve beïnvloeding.
- *Integriteit:* het voorkomen van ongecontroleerde wijzigingen of verlies van gegevens binnen de gegevensverwerking door de CVP en de gegevensuitwisseling ten behoeve van de EPD- en BSN-dienstverlening, zodat de juistheid, tijdigheid en volledigheid hiervan wordt geborgd en het gebruik van het systeem of de gegevens niet kan worden ontkend (onweerlegbaarheid).
- *Vertrouwelijkheid:* het beschermen van de gegevensverwerking door de CVP en de gegevensuitwisseling ten behoeve van de EPD- en BSN-dienstverlening tegen onbevoegde inzage en gebruik (dus niet zonder de combinatie van de bevoegdheid

als zorgverlener en een behandelrelatie tussen zorgverlener en patiënt) door middel van identificatie-, authenticatie- en autorisatie-mechanismen.
- *Controleerbaarheid:* het zekerstellen dat de naleving van de relevante wet- en regelgeving ten aanzien van 'Informatiebeveiliging' kan worden aangetoond (compliance).

Andere doeleinden van het informatiebeveiligingsbeleid zijn het borgen van een 'managementproces' voor informatiebeveiliging en het tijdig onderkennen en opvolgen van eventuele informatiebeveiligingsincidenten of vermeend misbruik van het EPD.

Om na te kunnen gaan of ongeautoriseerde toegang tot of bewerking van informatie heeft plaatsgevonden vindt vastlegging, analyse en opvolging van deze gebeurtenissen plaats. Logging en monitoring zijn derhalve een noodzakelijk onderdeel van het informatiebeveiligingsbeleid.

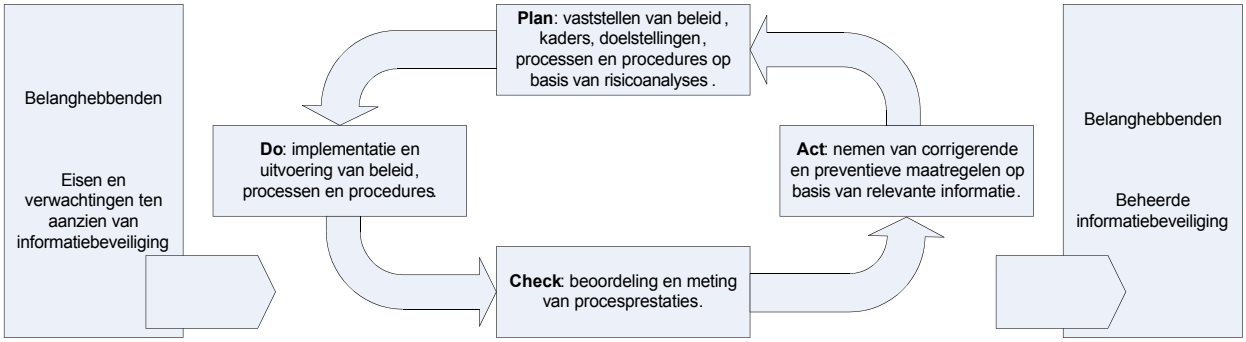
Ten behoeve van dit beleid heeft VWS de Strategische Beleidskaders voor Informatiebeveiliging van het landelijk EPD opgesteld, welke op dit moment nog moeten worden bekrachtigd. Een jaarlijkse herziening van de beleidskaders zal gebeuren op basis van een jaarlijkse risicoanalyse. Nadere uitwerking van de kaders naar concrete informatiebeveiligingsmaatregelen is de verantwoordelijkheid van de Centrale Voorzieningen Partijen Nictiz en CIBG. Zij voeren het 'operationele beheer'.

Het ministerie van VWS voert de regie over de ontwikkeling en het beheer van de EPD- en BSN-dienstverlening. Binnen VWS wordt ook een stuk 'Tactisch Beheer' uitgevoerd, dat de goede uitvoering van het informatiebeveiligingsbeleid en het operationele beheer conform de beleidskaders door de CVP aanstuurt en controleert. Overkoepelende afspraken zoals vastgelegd in de Service Level Agreements (SLA's) en Dossier Afspraken en Procedures (DAP) tussen de CVP en het ministerie spelen daarbij ook een rol. De Security Officers binnen de CVP zijn het eerste aanspreekpunt voor Tactisch Beheer bij VWS. Zij zijn binnen de eigen organisaties verantwoordelijk voor de inrichting van de informatiebeveiliging (voorzover die betrekking heeft op het landelijk EPD) en het toezicht op de implementatie en correcte werking van de operationele maatregelen die hieruit voortvloeien. Op hun rol en verantwoordelijkheid wordt in de hoofdstukken 6 en 7 nader ingegaan.

Tactisch Beheer faciliteert de afstemming van informatiebeveiligingsrisico's en maatregelen in een regulier ketenoverstijgend Informatiebeveiligingsoverleg (IBO) waarin alle relevante partijen deelnemen.

5.3 Controle en sturing op beleid

Om de Informatiebeveiliging binnen het landelijk EPD zodanig te structureren dat voldaan wordt aan de doelstellingen van de Strategische Beleidskaders is een managementproces voor Informatiebeveiliging noodzakelijk. Dit is door VWS opgezet volgens het Plan-Do-Check-Act (PDCA)-model zoals hieronder grafisch weergegeven.



Plan-Do-Check-Act model

Een managementcyclus voor informatiebeveiliging waarborgt de continue verbetering van informatiebeveiliging van het landelijk EPD door middel van de volgende stappen:

- **Plan:** De Strategische Beleidskaders voor Informatiebeveiliging bevatten de definities, uitgangspunten en beheersdoelstellingen voor de Informatiebeveiliging van het landelijk EPD. Dit document dient aan te sluiten bij de algemene doelstellingen en uitgangspunten voor het landelijk EPD en de bestaande informatiebeveiligingsrisico's die door middel van een risicoanalyse in kaart zijn gebracht. Op basis van deze analyse wordt jaarlijks een informatiebeveiligingsplan opgesteld om de risico's ten aanzien van Informatiebeveiliging te adresseren.
- **Do:** De strategische uitgangspunten worden in lijn met het informatiebeveiligingsplan verder vertaald naar operationele maatregelen, processen en procedures binnen Tactisch Beheer en het operationele beheer door Nictiz en CIBG. De Strategische Beleidskaders voor Informatiebeveiliging vormen de basis voor de verdere uitwerking van kwaliteit- en performancemanagement voor de EPD- en BSN-dienstverlening door Tactisch Beheer. De beveiligingsplannen van Nictiz en CIBG sluiten aan op het strategisch beleidskader. Op basis daarvan worden processen en procedures ingericht.
- **Check:** Door Tactisch Beheer wordt in samenwerking met het operationele beheer bij Nictiz en CIBG in kaart gebracht en gemonitord of de operationele procesprestaties in lijn zijn met de doelstellingen voor Informatiebeveiliging van het landelijk EPD die zijn beschreven in de Strategische Beleidskaders voor Informatiebeveiliging.
- **Act:** Op basis van de resultaten uit de Check-fase worden door het operationele beheer binnen Nictiz en CIBG in samenwerking met Tactisch Beheer corrigerende en preventieve maatregelen bepaald. Deze worden vervolgens door het operationele beheer geïmplementeerd. Daarnaast worden de Strategische Beleidskaders voor de Informatiebeveiliging van het landelijk EPD jaarlijks geëvalueerd en bijgewerkt.

De uitgebreide maatregelen die de toepassing en uitwerking van de managementcyclus vormen worden besproken in de hoofdstukken 6 en 7 over Nictiz en CIBG.

Grootschalige ketenbrede indringerstest (GKI)
Aanvullend daarop is het ministerie van VWS opdrachtgever tot de Grootschalige ketenbrede indringerstest (GKI).

Om de beveiliging van de gegevensuitwisseling binnen de gehele landelijke ICT-infrastructuur voor de zorg (AORTA-keten) te testen, heeft de minister aan de Tweede Kamer toegezegd dat het systeem aan een grootschalige indringerstest zal worden

onderworpen voorafgaand aan het verplichte aansluiten op het landelijk EPD.

De test biedt een integraal beeld van de veilige werking van de AORTA-keten en bestaat uit een samenstel van de volgende afzonderlijke indringerstesten op onderdelen en koppelvlakken van de AORTA-keten:

- Indringerstest SBV-Z, uitgevoerd in opdracht van CIBG;
- Indringerstest UZI-Register, uitgevoerd in opdracht van CIBG;
- Indringerstest LSP, uitgevoerd in opdracht van Nictiz;
- GBZ schouwingen bij een representatieve steekproef van aangesloten Goed Beheerde Zorgsystemen (GBZen), uitgevoerd in opdracht van Nictiz;
- Epd-keten Indringertesten op de Schakelconnecties (EIS) op connecties en connectiepunten tussen de GBZen en het LSP, uitgevoerd door/in opdracht van Nictiz.

Met de uitvoering van EIS wordt getest of de informatiebeveiliging van de connecties tussen de GBZ-en, de Application Service Providers (ASPs) en de Zorgserviceproviders (ZSPs) zijn ingericht conform de eisen beschreven in het PvE GBZ en PvE ZSP.

Instellen van de GKI, dat feitelijk een overkoepelend begrip is voor een samenstel van testen, biedt de garantie dat de testen die er deel van uit maken periodiek zullen worden uitgevoerd. De indringerstesten bij SBV-Z, UZI en LSP worden eens per jaar uitgevoerd. Jaarlijks wordt een representatieve steekproef van de deelnemende GBZ-en gecontroleerd in schouwingen. Wat betreft de in ontwikkeling zijnde indringerstest op de schakels van de keten (EIS) is voorgenomen dat iedere drie jaar alle schakels zijn getoetst en in tussen liggende jaren de nieuwe en de risicovolle schakels worden getoetst.[11]

Calamiteitenplan landelijk EPD
Ook is er vanuit het ministerie een uitgebreid Calamiteitenplan[12] voor het landelijke EPD opgezet. Dit plan omvat een algemene calamiteitenprocedure voor het gehele landelijke EPD. Het calamiteitenplan bevat een overzicht van de gehele calamiteitenorganisatie en een protocol voor elke soort van calamiteiten. Tactisch Beheer van VWS is verantwoordelijk voor de opvolging en het (doen) uitvoeren van het Calamiteitenplan, in geval van calamiteiten binnen de EPD- en BSN-dienstverlening. Het plan is onderwerp van toetsing, evaluatie en onderhoud. Het is opgesteld aan de hand van een risicoanalyse van de huidige landelijke voorzieningen voor het EPD. In 2010 zal een update van de risicoanalyse plaatsvinden.

Doorlopend toezicht
Gelet op het bovenstaande voert het ministerie van VWS vanuit Tactisch Beheer doorlopend en op gestructureerde wijze controle uit en houdt toezicht op de naleving en uitvoering van de verplichtingen en afspraken omtrent het landelijk EPD door betrokken partijen in de EPD-keten, die op hun beurt verantwoordelijk zijn voor naleving en uitvoering van de afspraken en verplichtingen binnen de eigen organisaties.

[11] Brief ministerie van VWS, Voortgangsrapportage elektronisch patiëntendossier II, 20 juli 2009, Bijlage 2.
[12] Ministerie van VWS, Calamiteitenplan landelijk EPD, oktober 2009.

H.6 Toezicht door CIBG

6.1 Taken van CIBG

Het CIBG voert als uitvoeringsorganisatie van het ministerie van VWS het UZI-register en is verantwoordelijk voor ontwikkeling, uitgifte en registratie van UZI-passen en servercertificaten. UZI-passen worden voor individueel gebruik uitgegeven aan zorgverleners als uniek identificatiemiddel voor toegang tot het EPD. Met de servercertificaten worden de GBZ-applicaties geïdentificeerd. Daarnaast is CIBG verantwoordelijk voor de Sectorale Berichten Voorziening in de Zorg (SBV-Z). SBV-Z faciliteert het juiste gebruik van het BSN voor identificatie van de patiënt. Ook is het CIBG verantwoordelijk voor de ontwikkeling van een Patiëntenportaal waarmee de patiënt in de nabije toekomst toegang kan krijgen tot de informatie die over hem beschikbaar wordt gesteld in het EPD. Daarnaast kan de patiënt via het portaal de beschikbaarheid van zijn gegevens beheren en aanpassen en de inzage in zijn gegevens door zorgverleners monitoren.

6.2 UZI-register

Voor het inrichten van een rechtmatig gebruik van het EPD is essentieel dat zorgaanbieders op een betrouwbare manier kunnen worden geïdentificeerd. Dit gebeurd met gebruik van de persoonlijke UZI-pas. Het UZI-register is verantwoordelijk voor het proces van aanvraag, productie en uitgifte van de UZI-pas. Het UZI-register beoordeelt de pasaanvragen. De zorgverlenerpas is bestemd voor beroepsbeoefenaars als bedoeld in de artikelen 3 en 34 van de Wet BIG. De UZI-pas is een soort elektronisch paspoort waarmee de zorgverlener zich kan identificeren en waarmee authenticatie mogelijk is voor toegang tot het EPD. Hoewel een voorwaarde om aan te kunnen melden voor het systeem, is de UZI -pas uiteraard niet de enige voorwaarde voor toegang. In de autorisatieprocedure worden immers de aanvullende voorwaarden getoetst.

Zorgaanbieders (instellingen of individuele beroepsbeoefenaars niet werkzaam in een instelling) die zijn geregistreerd in het UZI-register krijgen een UZI-abonneenummer. Als een zorgverlener meer dan één beroepstitel of specialisme heeft kan per beroepstitel of specialisme een pas worden aangevraagd. Als een zorgverlener of medewerker voor verschillende zorginstellingen werkt krijgt hij voor iedere zorginstelling een afzonderlijke UZI-pas. Als een zorgverlener meerdere passen heeft zullen deze altijd hetzelfde persoonsgebonden UZI-nummer hebben.

Goed beheerde zorgsystemen van waaruit toegang tot het landelijk EPD gemaakt wordt, dienen daarnaast tevens te zijn voorzien van een UZI-servercertificaat als functionele voorwaarde. De zorgaanbieder wordt geregistreerd als abonnee. Alle registratieactiviteiten worden door het UZI-register zelf uitgevoerd. De beveiligde uitgifte van de pas en het vaststellen van de identiteit van een pashouder of houder van een servercertificaat gebeurt met inzet van TNT Post Retail.

Certificaten
De UZI-pas bevat verschillende certificaten waarin identificerende gegevens van de pashouder (zoals naam en UZI-abonneenummer) en de gegevens van de zorgaanbieder (naam en UZI-abonneenummer) zijn opgenomen. Deze certificaten zijn

voorzien van de elektronische handtekening van het UZI-register. Hiermee kan worden vastgesteld dat een certificaat op een UZI-pas ook daadwerkelijk is uitgegeven door het UZI-register. Op de UZI-pas van zorgverleners staat ook de 'rolcode' die correspondeert met de geregistreerde professionele rol van de zorgverlener, op basis waarvan de pas is uitgegeven. Deze code is onder andere benodigd voor de autorisatie van de zorgverlener.

Smartcard
De lokale infrastructuur bij de zorgverlener omvat kaartlezers voor gebruik van de UZI-pas. Het gebruik van een smartcard biedt de volgende garanties:

- Als de UZI-pas niet fysiek aanwezig is in een kaartlezer, is het onmogelijk om transacties uit te voeren met een UZI-pas;
- Op basis van de huidige technische kennis is het maken van kopieën van de private sleutels niet mogelijk;
- De private sleutels zijn 'draagbaar' en kunnen eenvoudig meegenomen worden, zonder dat er kopieën achterblijven in het werkgeheugen of op de harde schijf van de PC. Wanneer een pashouder de pas bij zich draagt is misbruik onmogelijk.
- Er zijn altijd twee zaken vereist voor het gebruik van de private sleutels: bezit van de UZI-pas en kennis van de PIN-code.

Functie voor informatiebeveiliging
De UZI-pas vervult hierdoor een belangrijke rol in de informatiebeveiliging binnen de AORTA infrastructuur. Het gaat daarbij om de aspecten vertrouwelijkheid, integriteit en onweerlegbaarheid. Met behulp van de UZI-pas vindt authenticatie plaats van de zorgverlener die gebruik maakt van het EPD. De UZI pas maakt het mogelijk de toegang tot bepaalde gegevens te autoriseren voor een specifieke rol. Door gebruik te maken van UZI-passen voor toegang wordt bewerkstelligd dat gegevens tijdens verzending niet worden gelezen of gewijzigd, waarmee de integriteit van de communicatie is gewaarborgd. Door de elektronische handtekening waarin de UZI-pas voorziet, wordt onweerlegbaarheid gegarandeerd.

Soorten passen
Het UZI-register levert vier producten. Naast de zorgverlenerspas en servercertificaten zijn er 'medewerkerspassen op naam' en 'passen niet op naam'. Medewerkerspassen op naam kunnen door de geregistreerde zorgaanbieders (UZI-abonnees) worden aangevraagd voor niet BIG-geregistreerde medewerkers welke onder het mandaat van de zorgverlener werken en voor hun taak toegang nodig kunnen hebben tot bepaalde (geautoriseerde delen van) informatie.

Niet op naam gestelde passen worden onder voorwaarden uitgegeven aan geregistreerde zorgaanbieders ten behoeve van de beveiliging en controleerbaarheid van de werkzaamheden van bijvoorbeeld baliemedewerkers. Deze passen geven geen toegangsmogelijkheid tot het landelijk EPD, maar kunnen worden gebruikt om bijvoorbeeld het BSN te verifiëren. Van belang is dat de instelling die de pas heeft aangevraagd, deze uitgeeft en registreert voor gebruik door een individuele medewerker, hetgeen in de gebruiksvoorschriften is vastgelegd.

6.3 Sectorale Berichtenvoorziening in de Zorg (SBV-Z)

Voor het vaststellen van de identiteit van de patiënt in het EPD wordt het burgerservicenummer (BSN) van de patiënt gebruikt. Met behulp van het BSN kan op betrouwbare manier informatie tussen zorgaanbieders worden uitgewisseld en wordt

verwisseling van personen en gegevens voorkomen. De Sectorale Berichten Voorziening in de Zorg (SBV-Z) binnen CIBG faciliteert de veilige toepassing.

Bij de eerste aanmelding of opvraging van patiëntgegevens dient de zorgaanbieder op basis van een wettelijk identificatiemiddel het BSN van de patiënt te verifiëren bij de SBV-Z. Dit is wettelijk voorgeschreven. Bij de SBV-Z kan tevens worden nagegaan of een identiteitsdocument geldig is. Op deze manier is de zorgaanbieder ervan verzekerd dat hij de gegevens van de juiste patiënt opvraagt.

Op deze wijze wordt in de juistheid en het rechtmatige en zorgvuldige gebruik van persoonsgegevens voorzien. Inzage is mogelijk in het gebruik van het BSN. SBV-Z informeert de patiënt op zijn verzoek over welke zorgaanbieders zijn BSN hebben opgevraagd of geverifieerd.

6.4 Klantenloket EPD

Een andere taak van CIBG is het uitvoeren van het Klantenloket EPD. Deze taak is bij wet beschreven en aan de minister toegewezen. Deze heeft het beheer en uitvoeren van het Klantenloket EPD bij het CIBG belegd[13]. De functie van het klantenloket in het kader van het toezicht en de controle op het juiste en rechtmatige gebruik van het EPD wordt besproken in hoofdstuk 9 Controlemogelijkheden van de patiënt.

Het Klantenloket EPD zal het centrale aanspreekpunt voor de burger zijn inzake het landelijke EPD. Het klantenloket ondersteunt de patiënt indien gewenst bij de uitoefening van zijn rechten. De inrichting van het klantenloket gebeurt overeenkomstig het Programma van Eisen voor het Goed Beheerd Klantenloket (PvE GBK). Het klantenloket dient via een kwalificatieprocedure te kwalificeren als GBK. De kwalificatie wordt uitgevoerd door Nictiz. Het klantenloket zal ook het *Patiëntenportaal* beheren waarin de burger direct toegang heeft tot zijn gegevens.

Ook zorgt het klantenloket voor de afhandeling van verzoeken vanuit het LSP. Deze kunnen betrekking hebben op de kennisgeving aan de burger van een eerste aanmelding van zijn gegevens bij het LSP door een zorgaanbieder. Maar ook is het mogelijk dat een zorgaanbieder geïnformeerd moet worden over het bezwaar van een burger waarvan gegevens worden bewaard.

Het klantenloket heeft een belangrijke informatie- en voorlichtingsfunctie. De patiënt kan algemene vragen over het EPD aan het klantenloket voorleggen, maar ook vragen over het indienen van bezwaar, inzage of over lopende verzoeken. Het Klantenloket EPD is daarnaast ook het aanspreekpunt voor vermeende gevallen van misbruik van het EPD. Deze procedure wordt beschreven in hoofdstuk 9 Controlemogelijkheden van de patiënt.

ICT-Beheer
Het Klantenloket EPD is onderdeel van de digitale infrastructuur AORTA. Om de taken ten aanzien van de afhandeling van verzoeken van patiënten mogelijk te maken, wordt een informatiesysteem ingericht en beheerd. Het Patiëntenrechten Informatiesysteem Klantenloket EPD (PRIK) is het systeem dat wordt gebruikt voor de registratie, beoordeling, afhandeling en terugkoppeling van verzoeken aan het klantenloket. Het beheer van dit systeem is een taak van het klantenloket.

[13] De taken en werking van het Klantenloket EPD zijn vastgelegd in de Procesbeschrijving (AO) Klantenloket EPD van het CIBG.

Voor uitvoering van de taken van het Klantenloket EPD maakt CIBG gebruik van andere dienstverleners die het proces ondersteunen. De dienstverlening van deze derden heeft betrekking op het leveren en afnemen van informatie. Zo levert het LSP bijvoorbeeld index- en log-informatie en SBV-Z log-informatie op verzoek van de patiënt. De website infoEPD.nl levert de verzoeken van burgers die via die site binnenkomen aan het klantenloket aan ter afhandeling. Verder maakt het CIBG ten behoeve van het klantenloket gebruik van derden die optreden als bewerker in de zin van de Wbp, voor het verwerken van inkomende en uitgaande post.

6.5 Controle en toezichtmaatregelen CIBG

Aanvullend op de hierboven besproken maatregelen die de veiligheid en vertrouwelijkheid van de EPD-infrastructuur ten dienst staan, zijn er vele maatregelen getroffen door CIBG die specifiek de controle en het toezicht op het rechtmatige en juiste gebruik van het landelijk EPD omvatten.

Toezicht door Security Officer
De Security Officer van CIBG ziet intern toe op de beveiliging. De Security Officer bewaakt de naleving van de Wbp en het specifieke normatieve kader en voert risicoanalyses in dit kader uit. Bij afwijkingen en incidenten beoordeelt de Security Officer gemaakte analyses en maatregelen. Dit resulteert in het vroegtijdig kunnen onderkennen van risico's en het voorbereiden en nemen van passende maatregelen. De verantwoordelijkheden en bevoegdheden van de Security Officer zijn vastgelegd in het beveiligingplan van CIBG.

Bij calamiteiten en beveiligingsincidenten is de Security Officer verantwoordelijk voor de afhandeling daarvan binnen CIBG, de rapportage en het contact met externe partijen. De Security Officer koppelt regulier en indien nodig incidenteel terug aan VWS over de implementatie en de werking van het informatiebeveiligingsbeleid.

Organisatorische en procesmatige maatregelen
De processen en systemen van het UZI-register zijn ingericht op basis van een afhankelijkheidsanalyse, dreigingenanalyse en een kwetsbaarheidsanalyse, waarbij de relevante regelgeving uitgangspunt is. Er is een levend informatiebeveiligingsbeleid en alle maatregelen zijn vastgelegd in een beveiligingsplan. Dit plan wordt tenminste eenmaal per vier maanden, conform de Planning & Control cyclus van CIBG, gecontroleerd op actualiteit.

In het kader van beveiliging voert het UZI-register een restrictief beleid op het gebied van toegang tot systemen en gegevens. Toegang wordt alleen verleend op basis van noodzakelijkheid. Tenminste eenmaal per maand worden alle geldende autorisaties gecontroleerd. Loggings worden geanalyseerd. Eventuele beveiligingsincidenten worden geregistreerd en geanalyseerd en omgezet in correctieve en preventieve acties. Risicoanalyse en controle van de maatregelen vindt tenminste eenmaal per maand plaats.

Het beleid van het UZI-register is vastgelegd in een Certification Practice Statement. Dit document beschrijft de processen, procedures en beheersingsmaatregelen voor het aanvragen, produceren, verstrekken, beheren en intrekken van de certificaten. Met het Certification Practice Statement kunnen betrokkenen hun vertrouwen in de door het UZI-register geleverde diensten bepalen. De inhoud van het Certification

Practice Statement wordt jaarlijks getoetst door een geaccrediteerde externe auditor.

Wijzigingen in de systemen of processen van het UZI-register worden pas doorgevoerd nadat een impact analyse is uitgevoerd. Waar nodig wordt deze vooraf afgestemd met EPD ketenpartners. Een risicoanalyse maakt standaard deel uit van de impact analyse. Na realisatie van de wijziging worden de systemen of processen aan een volledige testcyclus onderworpen (moduletesten, systeemtesten, acceptatietesten). Voor deze testen wordt gebruik gemaakt van vooraf opgestelde (standaard) testplannen en testscripts. Wijzigingen worden gebundeld tot releases om het risico op verstoringen zo veel mogelijk te beperken.

De inrichting van zowel registratieprocessen als beheerprocessen is zodanig, dat is geborgd dat het voor één medewerker onmogelijk is om een product (zoals een UZI-pas) te laten produceren. Dit wordt afgedwongen door de systeemarchitectuur. Belangrijkste maatregelen zijn dat toegang tot het systeem sterke authenticatie vereist (door gebruik van een PKI-pas die is gekoppeld aan een persoonsgebonden useraccount). De applicatie dwingt verder een 'vier ogen principe' af in het registratieproces. Alle transacties worden gelogd en zijn tot op de persoon herleidbaar. Beheerprocessen zijn hieraan ondersteunend ingericht.

Leveranciersmanagement
Met alle leveranciers die diensten leveren in het primair proces worden maandelijks overleggen gevoerd over operationele en zo nodig tactische en strategische aangelegenheden. Leveranciers leggen daarin verantwoording af over de kwaliteit van de geleverde diensten. Zodoende wordt de afgesproken kwaliteit en kwantiteit van dienstverlening bewaakt. Daarnaast voert het UZI-register zelf actieve monitoring van het beheer op de infrastructuur uit. Hiermee wordt de rapportage over de dienstverlening getoetst.

De leveranciers van diensten in het primair proces van het UZI-register voldoen aan het voorgeschreven normenkader. Ook zij worden tenminste eenmaal per jaar door een geaccrediteerde partij geaudit. Daarnaast zijn zij verplicht om interne audits en selfassessments uit te voeren.

Interne toetsing en toezicht
Door CIBG worden daarnaast diverse maatregelen van controle en toezicht uitgevoerd. Dat geldt ook voor de bewerker TNT Post Retail. De door CIBG en TNT Post Retail uitgevoerde maatregelen om een continue toezicht op verschillende onderdelen en processen te waarborgen betreffen onder ander de volgende.

- *Selfassessments door de autorisator*
  Dit houdt de controle van de validatie van een aanvraag in door een autorisator. De autorisator is een ervaren registratiemedewerker die niet eerder bij de afhandeling van het betreffende dossier betrokken is. Het selfassessment gebeurt tijdens het registratieproces. Het doel hiervan is het voorkomen van producten met afwijkingen. De frequentie is doorlopend.
- *Kwaliteitstoets van het UZI-register*
  Dit is een kwaliteitscontrole achteraf door een stafmedewerker. De controle vindt steekproefsgewijs plaats waarbij steekproeven worden genomen per procesdeel, per team of per medewerker. Resultaten worden geanalyseerd en intern verwerkt. Doel van dit assessment is het vaststellen van de kwaliteit van de werkzaamheden en het identificeren van proceszwaktes en opleidingsbehoeften. Met dit inzicht

kunnen gericht voorstellen worden gedaan om het proces en de kennis van medewerkers te verbeteren. De frequentie is doorlopend en rapportage vindt wekelijks plaats.

- *Interne audits bij CIBG*
  Deze procesaudits gebeuren door een auditor van een van de andere onderdelen van het CIBG. Interne audits kunnen gericht zijn op het normatief kader, op specifieke processen (bijvoorbeeld registratie van abonnees of het intrekken van passen) maar kunnen ook themagericht zijn (bijvoorbeeld op beveiliging en beveiligingsbewustzijn of verbetergerichtheid). Doel hiervan is toetsen of invulling wordt gegeven aan alle gestelde vereisten van het proces. De frequentie is twee maal per jaar.
- *Interne audits UZI-systemen/infrastructuur*
  Toetsen en testen van de systemen/infrastructuur waarop het UZI-register functioneert (zoals het registratiesysteem, het card managementsysteem maar ook validatiediensten). Doel is het bewaken van beschikbaarheid, exclusiviteit en integriteit. De frequentie is bij elke wijziging in de infrastructuur.
- *Uitwijktest UZI-register*
  Tenminste eenmaal per jaar voert het UZI-register een uitwijktest uit. Hierbij worden alle systemen in de uitwijkomgeving in de lucht gebracht. De volledige functionaliteit word in de uitwijkomgeving getest. De dienstverlening blijft daarbij operationeel. Het uitvoeren van de uitwijktest is een onderdeel van het Business Continuity Management Plan dat samen met de systeemleverancier is opgesteld. Dit plan wordt tijdens de uitwijktest getoetst en zo nodig bijgesteld.
- *Autorisatiecontrole*
  De functioneel beheerder en de applicatiebeheerder van het UZI-register stellen gezamenlijk vast of alle autorisaties correct en onderbouwd zijn. Resultaten leggen zij vast in een proces verbaal. Doel is controle van het beheer van autorisaties. Dit gebeurt maandelijks.
- *Logginganalyse*
  Analyse van de transactieloggings uit het registratiesysteem kan worden uitgevoerd als er een vermoeden van ongewenst handelen door een medewerker is. De frequentie hiervan is ad hoc.
- *Interne audits TNT Post Retail*
  De uitgifte van de UZI-pas wordt meegenomen in de interne audits die TNT uitvoert op alle filialen en bij agentschappen. Alle onderdelen van het bewaar, uitgifte en retourproces zijn onderwerp van controle.

Externe maatregelen van controle en toezicht

Ook is er sprake van diverse maatregelen van toezicht en controle door externe, onafhankelijke instanties. De extern uitgevoerde maatregelen betreffen de volgende:

- *Compliance audits*
  Jaarlijks wordt door een geaccrediteerde auditor audits uitgevoerd op de invulling en naleving van de normen waaraan het UZI-register moet voldoen. De belangrijkste normen zijn:
  - Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures;
  - ETSI 101 456 Policy requirements for certification authority issuing qualified certificates;
  - De Wet elektronische handtekening;
  - Programma van Eisen PKIoverheid. Hierin zijn aanvullende eisen en

verscherpingen ten opzichte van de ETSI-norm opgenomen.
Deze externe audits worden jaarlijks uitgevoerd, waarbij eenmaal per drie jaar sprake is van een volledige audit gevolgd door twee controle audits. De audit wordt ook uitgevoerd bij alle leveranciers waaraan diensten zijn uitbesteed zoals op dit moment TNT Post Retail, Getronics/Sagem en het rekencentrum VWS. Deze test vormt een onderdeel van de Grootschalige ketenbrede indringerstest (GKI) die in hoofdstuk 5 aan de orde kwam.

- *IT-audit* op invulling en naleving van de eisen zoals gesteld in CWA 14167-1 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements). Elke geplande wijziging van de systemen wordt getoetst tegen deze norm. Bij grotere wijzigingen wordt een nieuwe verklaring aangevraagd. Deze test is tevens onderdeel van de Grootschalige ketenbrede indringerstest (GKI).
- *ISO 9001: 2008*
  CIBG is jaarlijks onderwerp van een ISO9001 audit uitgevoerd door een onafhankelijke auditor.
- *EDP Audit Pool en Algemene Rekenkamer*
  Het beveiligingsplan van het UZI-register is samen met de overige beveiligingsplannen van het CIBG getoetst door de EDP Audit Pool van de Rijksoverheid. De oordeelsvorming door de EDP Audit Pool is opgevolgd door de Algemene Rekenkamer.
- *Stresstest internetdiensten door TNO*
  Om zekerheid te krijgen dat de internetdiensten van het UZI-register naar behoren functioneren bij grootschalig gebruik heeft TNO een stresstest op deze diensten uitgevoerd. Het gaat daarbij bijvoorbeeld ook om een webapplicatie waarmee indien noodzakelijk UZI-passen direct zijn in te trekken. Naast het vaststellen van de belastbaarheid is een onafhankelijke analyse van de systeemarchitectuur doel van deze test. Ook indringerstesten van specifieke webapplicaties zijn onderdeel van de test. In de test is vastgesteld dat de infrastructuur voldoet. De test wordt tweejaarlijks uitgevoerd, dan wel na relevante wijzigingen. Deze test vormt een onderdeel van de Grootschalige ketenbrede indringerstest (GKI) die in hoofdstuk 5 aan de orde kwam.
- *Functionele testen van de UZI-pas*
  Dit gebeurde in het kader van het in gebruik nemen van een nieuwe chip door een onafhankelijke auditor, een testlaboratorium met ervaring in het testen van PKIoverheid-toepassingen. De test omvat bruikbaarheid van de UZI-pas vanuit applicaties voor het uitvoeren van generieke beveiligingsfuncties (zoals authenticatie en elektronische handtekening) en specifieke beveiligingsfunctionaliteiten zoals bijvoorbeeld het blokkeren van de UZI-pas na invoeren van drie foute PIN codes. Bij wijzigingen wordt de test opnieuw uitgevoerd (dit is voorzien in 2010).
- *Certificering van het produkt van leveranciers van UZI*
  Certificering van het produkt, de pas met chip, dat voor de UZI-pas gebruikt wordt. Dit gebeurd in opdracht van de chip leveranciers door externe auditors op basis van de zogenaamde 'Common Criteria' voor certificering. Onderdeel van het normenkader van PKI overheid is dat de hardware en het operating systeem van de UZI-pas onafhankelijk getest en gecertificeerd moeten zijn. In de normen is vastgesteld waaraan zogenaamde ‘Signature Creation Devices’, zoals de UZI-pas waarmee de gebruiker een elektronische handtekening kan plaatsen, moeten voldoen. Testen vinden plaats in een geaccrediteerd Common Criteria laboratorium. De huidige chip inclusief card operating systeem is Evaluation Assurance Level 5+ gecertificeerd. De frequentie van dergelijke certificering is

eenmalig met updates na wijzigingen.

- *Code review applet*
  Op de UZI-pas staat een klein programmaatje (applet). Deze applet beheert een bestandstructuur op de chip van de UZI-pas voor opslag van certificaten en sleutels van de gebruikers en vormt de interface tussen de software op de PC van de gebruiker en de sleutels en PIN codes in de chip. Daarmee vervult de applet een centrale functie die de totale beveiliging van de UZI-pas kan beïnvloeden. Dit is de reden dat er door een gekwalificeerd certificeringsbureau een 'code review' is uitgevoerd op de volledige broncode van de applet. De frequentie van dergelijke code reviews is eenmalig en na substantiële wijzigingen.
- *Security Evaluatie UZI-pas*
  Deze test is complementair aan de functionele test. Waar de functionele test uitgaat van ‘use cases’ bij regulier gebruik gaat deze evaluatie vooral uit van ‘misuse’ cases die bijna alleen in een laboratorium situatie uitvoerbaar zijn. Denk daarbij o.a. aan het bewust verstoren van voedingsspanning en kloksignalen om de chip ‘in de war’ te maken en zodoende informatie over sleutelmateriaal te krijgen. De test wordt uitgevoerd door een onafhankelijk laboratorium dat gespecialiseerd is in smartcard beveiliging. De frequentie van deze test is tweejaarlijks om nieuwe ontwikkelingen op het gebied van smartcard aanvallen mee te nemen en tussentijds na substantiële wijzigingen.
- *SBV-Z Indringerstest*
  Dit betreft een 'blackbox test' op de produktie-omgeving en een 'crystalbox test' op de acceptatie-omgeving. Hierbij wordt zowel de beveiliging van de web applicatie als de servers getest. De test wordt per nieuwe release door een geaccrediteerde auditor uitgevoerd. Deze test is tevens onderdeel van de Grootschalige ketenbrede indringerstest (GKI) die in hoofdstuk 5 aan de orde kwam.

Doorlopend toezicht

Op de systemen waarmee de primaire processen worden uitgevoerd vindt zeven dagen per week 24 uur per dag monitoring plaats. Beheer van deze systemen is steeds belegd bij partijen die voldoen aan de Code voor informatiebeveiliging (NEN-ISO/IEC 27002) en hierop in externe audits worden getoetst. De inrichting van uitvoering en beheer is zodanig dat is gegarandeerd dat de leverancier of andere externe partijen geen toegang kunnen krijgen tot sleutelmateriaal van het UZI-register zelf of uitgegeven certificaten.

Bijzonder toezicht

OPTA

Omdat de UZI-pas gekwalificeerde certificaten bevat, houdt de OPTA toezicht op de verstrekking van de UZI-pas. Het UZI-register doet hiertoe jaarlijks aangifte bij de OPTA. De OPTA is bevoegd om controlerend op te treden, maar steunt veelal op de rapportages van de externe audits.

Policy Authority PKIoverheid

Omdat de certificaten van het UZI-register worden uitgegeven onder het stamcertificaat van de Staat der Nederlanden, houdt de Policy Authority (PA) namens de minister van BZK toezicht op het UZI-register. Jaarlijks worden bilaterale gesprekken gevoerd. Daarnaast neemt het UZI-register deel aan de overleggen die door de PA worden georganiseerd. De PA heeft het recht om zelfstandig controlerend op te treden, maar steunt over het algemeen op de rapportages van externe audits.

H.7 Toezicht door Nictiz

7.1 Nictiz

Het Nationaal ICT Instituut in de Zorg (Nictiz) is een stichting die in 2002 is opgericht om het gebruik van ICT in de zorg te stimuleren. Samen met het ministerie en andere betrokken partijen werkt Nictiz aan de realisatie en het onderhouden van het landelijk EPD. Inmiddels is Nictiz aangewezen als beheerder van het Landelijk Schakelpunt. De taken en activiteiten van Nictiz zijn daardoor toegespitst op het conform alle voorwaarden in stand houden van het landelijk EPD.

Nictiz verricht daartoe onder andere de volgende activiteiten:

- Ontwerpen en onderhouden van de basisinfrastructuur (AORTA) voor de landelijke gegevensuitwisseling via het EPD.
- Ontwerpen en onderhouden van de standaarden voor toepassingen van het EPD.
- Kwalificeren en certificeren van ICT-leveranciers en zorgaanbieders voor aansluiting op het LSP.
- Ondersteuning bieden bij de invoering van toepassingen van het EPD.
- Monitoren van (inter)nationale ontwikkelingen, best practices en mogelijkheden.

7.2 Security Officer

In de organisatie is de functie van Security Officer belegd. De Security Officer is onder meer verantwoordelijk voor de goede uitvoering van het informatiebeveiligingsbeleid met betrekking tot AORTA in de organisatie en het toezicht op het correcte gebruik van het LSP. De Security Officer zorgt voor het uitvoeren van risicoanalyses met betrekking tot de informatiebeveiliging en voert de benodigde operationele beveiligingsmaatregelen door. Hij houdt toezicht op de implementatie en correcte werking van de operationele maatregelen door de uitvoerende onderdelen.

In het geval van een beveiligingsincident initieert de Security Officer de afhandeling daarvan binnen Nictiz, en zorgt voor de rapportage aan het bestuur. Hoe de Security Officer zijn taken uitvoert is beschreven in het Beveiligingsplan LSP van Nictiz.[14] De Security Officer koppelt regulier en indien nodig incidenteel terug aan Tactisch Beheer bij VWS over de implementatie en de werking van het informatiebeveiligingsbeleid met betrekking tot AORTA.

De Security Officer is gepositioneerd in de organisatie binnen het cluster 'Operations' van Nictiz en heeft derhalve geen clusteroverstijgende positie. Dit gegeven komt terug in het document Aanbevelingen Toezichtkader EPD.

7.3 De infrastructuur van het EPD

Het AORTA netwerk faciliteert de uitwisseling van patiëntgegevens tussen informatiesystemen van zorgaanbieders. AORTA is door Nictiz ontworpen volgens een aantal architectuurprincipes. Een aantal daarvan zijn van belang voor een goed begrip van de maatregelen die worden besproken in het kader van de controle en het toezicht op het landelijk EPD.

[14] Er is een Beveiligingsplan LSP en een Beveiligingsplan Nictiz, de laatste betreft de interne organisatie.

- *Autonomie en verantwoordelijkheid van de zorgaanbieder:* binnen het AORTA netwerk is de zorgaanbieder verantwoordelijk voor de inrichting en beveiliging van zijn ICT-voorzieningen binnen de gestelde randvoorwaarden welke getoets worden bij kwalificatie voor aansluiting (GBZ-kwalificatie). De zorgaanbieder blijft zelf verantwoordelijk voor de correctheid en de vertrouwelijkheid van patiëntgegevens in zijn eigen systeem;
- *Goed Beheerd Zorgsysteem (GBZ) en XIS-kwalificatie:* de zorginformatiesystemen van zorgaanbieders moeten aan specifieke eisen voldoen ten aanzien van beveiliging en beheer om te kwalificeren voor aansluiting op het LSP.
- *Decentrale opslag:* de opslag van patiëntgegevens vindt plaats in het informatiesysteem (brondossier) van de verantwoordelijke zorgaanbieder. AORTA bevat dus geen centrale database met patiëntgegevens;
- *Landelijk Schakelpunt (LSP):* voor de uitwisseling van patiëntgegevens wordt gebruik gemaakt van een Landelijk Schakelpunt;
- *Verwijsindex:* Voor het snel en efficiënt vinden en toegankelijk maken van de gezochte informatie wordt gebruik gemaakt van een verwijsindex. Deze maakt onderdeel uit van het LSP. In de verwijsindex is weergegeven waar bepaalde patiëntgegevens zijn opgeslagen;
- *Zorg Service Provider (ZSP):* communicatie tussen het zorginformatiesysteem van de zorgaanbieder (een GBZ) en het LSP dient altijd te verlopen via een ZSP. Een ZSP is een ICT-dienstverlener en biedt lokaal de infrastructuur die nodig is voor de aansluiting tussen GBZ en LSP. De ZSP dienstverlener moet aan specifieke eisen voldoen om te kwalificeren als toegelaten ZSP.
- *Vertrouwensketen:* voordat een zorgaanbieder toegang kan krijgen tot de Verwijsindex om gegevens op te vragen dienen de verschillende stappen van de 'vertrouwensketen' te worden doorlopen. Dit zijn achtereenvolgens de procedures voor identificatie, authenticatie, autorisatie en logging.[15]
- *Unieke Zorgverlener Identificatie (UZI)*: om het EPD te kunnen raadplegen, dienen zorgverleners in te loggen met een UZI-pas (als authenticatiemiddel). Deze wordt uitgegeven door het UZI-register (onder verantwoordelijkheid van CIBG).

Het AORTA-netwerk en de voorwaarden van gegevensuitwisseling via het landelijk EPD zijn uitgebreid beschreven in de 'AORTA-documentatie'.[16]

7.4 Het Landelijk schakelpunt

Het uitwisseling van patiëntgegevens in het landelijk EPD gebeurt via het Landelijk schakelpunt (LSP). Een van de belangrijkste functies van het LSP is het verwijzen en routeren van patiëntgegevens en het bijhouden van de zogenaamde ‘verwijsindex’.

Naast een verwijsfunctie heeft het LSP een functie bij het reguleren en controleren van de toegang tot patiëntgegevens. Voordat een zorgaanbieder patiëntgegevens kan raadplegen, dient de identiteit van de zorgaanbieder te worden vastgesteld (identificatie) en geverifieerd (authenticatie). Vervolgens dient te worden nagegaan of de zorgaanbieder bevoegd is tot het raadplegen van patiëntgegevens en, zo ja, welke gegevens hij mag inzien (autorisatie). Een belangrijke voorwaarde daarbij is dat sprake is van een behandelrelatie met de betreffende patiënt.

[15] Zie voor een uitgebreide beschrijving het Vertouwensmodel landelijk EPD van Nictiz.
[16] Deze is te vinden op www.nictiz.nl.

Vervolgens registreert het LSP door middel van logging welke gegevens zijn geraadpleegd. Daarmee kan de rechtmatigheid van de inzage worden gecontroleerd en onrechtmatige toegang worden opgevolgd.

De verwijsindex
In de landelijke verwijsindex wordt bijgehouden welke zorgaanbieders beschikken over patiëntgegevens van een bepaalde patiënt. Beroepsbeoefenaars die daartoe bevoegd zijn kunnen de verwijsindex raadplegen aan de hand van het burgerservicenummer (BSN) van de patiënt. Voorwaarde is dat sprake is van een behandelrelatie met de betreffende patiënt en dat toestemming is verkregen.

Middels de verwijsindex is het Landelijk Schakelpunt in staat om verzoeken voor inzage in patiëntgegevens te routeren naar informatiesystemen van zorgaanbieders die over deze gegevens beschikken. De verwijsindex is nodig omdat het Landelijk Schakelpunt geen centrale database heeft waarin alle patiëntgegevens zijn opgeslagen. Bij de eerste aanmelding van patiëntgegevens door een zorgaanbieder wordt de patiënt hiervan schriftelijk op de hoogte gesteld.

Feitelijk beheer LSP
Het feitelijk beheer van het LSP is door Nictiz uitbesteed aan een externe partij (nu CSC), die beschikt over de vereiste bijzondere expertise. Deze partij is contractueel verplicht om het beheer overeenkomstig het Programma van Eisen aan het LSP (PvE LSP) uit te voeren. Daarnaast gelden tussen partijen aanvullende afspraken uit het Dossier Afspraken en Procedures LSP (DAP LSP) en de Service Level Agreements.

Doorlopende monitoring LSP
Op de systemen waarmee de primaire processen worden uitgevoerd vindt continue monitoring plaats. Het beheer van deze systemen voldoet aan de NEN7510, waarop getoetst is in externe audits. Op nadere maatregelen van controle en toezicht wordt ingegaan in hoofdstuk 7.7.

Fysieke beveiliging
De ICT-infrastructuur van het Landelijk Schakelpunt bevindt zich in een fysiek beveiligde omgeving en is slechts toegankelijk voor geautoriseerd personeel. De apparatuur in het LSP is beveiligd tegen risico's van schade en storing en ongeautoriseerde toegang.

De beveiliging van het LSP is zodanig ingericht dat elektronisch indringen maximaal wordt voorkomen. Met behulp van ‘intrusion detection’ worden mogelijke afwijkingen snel gedetecteerd en worden middels ‘intrusion prevention’ direct maatregelen getroffen. Daarnaast worden tests uitgevoerd en is voorzien in procedures voor de afhandeling van beveiligingsincidenten. Vermoedens van onrechtmatig gebruik worden conform procedures geëscaleerd. Ook hierop wordt nader ingegaan in hoofdstuk 7.7 Controle en toezichtmaatregelen.

Beheerfuncties
CSC voert diverse operationele beheerfuncties uit. Om beveiligingsredenen worden het beheer van autorisaties, het beheer van de centrale gebruiksregistratie en het beheer van de ICT-systemen door verschillende personen uitgevoerd. De beheerfuncties van het LSP zijn slechts toegankelijk voor aangewezen personen. Ten behoeve van de controle op de juiste werking en naleving van de juiste procedures worden alle beheerhandelingen vastgelegd in een logboek.

Medewerkers van het CSC dienen te voldoen aan de eisen gesteld in de genoemde afspraken tussen Nictiz en CSC en het Programma van Eisen LSP ten aanzien van de vakkennis, ervaring en kwalificaties die noodzakelijk zijn voor de werkzaamheden die zij vervullen. Personeel dat betrokken is bij gegevensverwerkende taken heeft een expliciete geheimhoudingsplicht.

Programma van Eisen LSP
De eisen die worden gesteld aan het LSP zijn vastgelegd in een door Nictiz vastgesteld PvE LSP. Dit PvE gaat gedetailleerd en specifiek in op alle eisen die gesteld zijn aan de exploitatie, de functionaliteit en de implementatie van het LSP.

Exploitatie eisen
Het PvE LSP stelt een groot aantal eisen aan de exploitatie van het LSP. Te denken valt daarbij aan eisen omtrent beschikbaarheid, capaciteit, eigendom van de ICT-voorzieningen en beveiliging. Maar ook aan eisen die de organisatie betreffen of de klantondersteuning. Daarnaast worden eisen gesteld aan de verschillende beheerdiensten die de diverse beheerfuncties dienen uit te voeren.

Functionaliteit eisen
Het LSP voert diverse beheerfuncties uit. Het PvE stelt onder andere eisen aan het beheer van het toegangslog, aan autorisatiebeheer, aan systeembeheer, applicatiebeheer en kwalificatiebeheer. Verder zijn allerlei functies vereist die exploitatie eisen ondersteunen zoals functies met betrekking tot het uitwisselen en routeren van berichten, het valideren en autoriseren van berichten, authenticatiefuncties en logfuncties.

Implementatie eisen
Belangrijke implementatie eisen in het PvE zijn eisen aan de beveiliging, de beschikbaarheid en de betrouwbaarheid van het LSP.

De eisenspecificatie in het PvE LSP vormt de basis voor de acceptatie, het beheer, het onderhoud en de exploitatie van het LSP. De eisen omvatten zowel organisatorische, procedurele, functionele als technische aspecten. Het PvE wordt regelmatig aangevuld en gewijzigd indien de ontwikkeling of samenhang met andere documenten dit vereist. Het PvE LSP is mede gebaseerd op andere documenten van Nictiz: de Bedrijfsarchitectuur, de Informatiesysteemarchitectuur en de Technische architectuur.

Naleving en controle
De Security Officer van Nictiz ziet toe op de naleving van de eisen van het PvE LSP en de afspraken in het beveiligingsplan. Het toezicht en de controle op de veilige werking en het zorgvuldige en rechtmatige gebruik van het LSP en het landelijk EPD wordt daarnaast vanuit Nictiz door middel van diverse andere maatregelen uitgeoefend. Op deze maatregelen wordt in hoofdstuk 7.7 ingegaan.

7.5 Zorg Service Providers (ZSP)

De communicatie tussen het zorginformatiesysteem van de zorgaanbieder (een GBZ) en het LSP dient altijd te verlopen via een ZSP. Een ZSP is een ICT-dienstverlener en biedt lokaal de infrastructuur die nodig is voor de aansluiting tussen GBZ en LSP. De ZSP verbindt de GBZ en het LSP via een besloten datacommunicatienetwerk. De ZSP dienstverlener moet aan specifieke eisen voldoen om te kwalificeren en toegelaten te

worden als ZSP die mag aansluiten op het LSP. Deze eisen zijn gespecificeerd in het Programma van Eisen Zorg Service Provider (PvE ZSP). De kwalificaties worden in opdracht van Nictiz door externe auditors uitgevoerd. Nictiz heeft met de ZSP's een contractrelatie. De controle en het toezicht op de kwalificatie wordt beschreven in hoofdstuk 7.7.

7.6 Goed Beheerd Zorgsysteem (GBZ)

De zorginformatiesystemen van zorgaanbieders moeten aan specifieke eisen voldoen ten aanzien van beveiliging en beheer om te kwalificeren voor aansluiting op het LSP. Een zorginformatiesysteem dat voldoet aan de eisen wordt een Goed Beheerd Zorgsysteem (GBZ) genoemd. Een GBZ dient te voldoen aan de organisatorische, procedurele, functionele en technische eisen die zijn vastgelegd in het Programma van Eisen Goed Beheerd Zorgsysteem (PvE GBZ). Nictiz gaat met de GBZ-en een contractrelatie aan.

XIS-Kwalificatie
Het Informatiesysteem van de zorgaanbieder (een X-Informatiesysteem (XIS)) dient daarbij een XIS-kwalificatie te hebben. Dit is een eis aan het GBZ. Nictiz kwalificeert de systemen van ICT-leveranciers welke voldoen aan alle gestelde XIS-eisen.

Wanneer de kwalificatie verkregen is, zal een GBZ blijvend moeten voldoen aan de eisen. De eisen in het PvE GBZ worden regelmatig up to date gehouden en in nieuwe releases gepubliceerd. Het blijvend voldoen aan de eisen wordt door Nictiz gecontroleerd en getoetst in (her)kwalificaties van de applicatie (XIS) en GBZ-schouwingen. Op deze controle- en toezichtmaatregelen wordt in de volgende paragraaf ingegaan.

7.7 Controle en toezichtmaatregelen

Security Officer
Zoals gesteld in hoofdstuk 7.2 is de Security Officer van Nictiz verantwoordelijk voor het toezicht op de implementatie en correcte werking van operationele maatregelen die voortvloeien uit het informatiebeveiligingsbeleid met betrekking tot AORTA en het Beveiligingsplan LSP binnen Nictiz en ten aanzien van het LSP. De Security Officer zorgt voor het uitvoeren van risicoanalyses met betrekking tot de AORTA architectuur.

Vanuit het operationele beheer ontvangt hij de signalering van informatiebeveiligingsincidenten en gevallen van vermeend misbruik. De Security Officer is verantwoordelijk voor de afhandeling hiervan en rapportage naar aangewezen partijen.

Ook is de Security Officer aangewezen als technisch toezichthouder LSP, waarbij meldingen over normoverschrijdingen ten aanzien van monitoring van het LSP, bij hem gedaan worden en door hem worden afgehandeld (zie *Procedure Monitoring LSP* in deze paragraaf).

Interne maatregelen
Mede gelet op de eisen die in dit hoofdstuk zijn beschreven ten aanzien van de onderdelen van het landelijk EPD, worden veel uiteenlopende controle en toezichtsactiviteiten uitgevoerd.

Door Nictiz zelf worden diverse maatregelen uitgevoerd. Maatregelen die door externe onafhankelijke geaccrediteerde auditors worden uitgevoerd worden hierna besproken.

De door Nictiz uitgevoerde maatregelen om een continu toezicht op verschillende onderdelen en processen te waarborgen betreffen onder ander de volgende. Verwezen wordt naar de hierboven beschreven procedures en eisen waarop deze maatregelen complementerend zijn:

- Interne audit op beveiliging LSP, deze audit werd uitgevoerd in 2007;
- Interne audits op delen van beveiligingsprocessen, deze audit wordt maandelijks uitgevoerd;
- Jaarlijkse algehele risicoanalyse;
- Ad hoc risicoanalyses;
- Onderzoek naar beveiliging tijdens een ontwerpfase;
- Voor elk wijzigingsvoorstel (een 'change request' voor een functie van het LSP of ander onderdeel van de EPD-keten binnen de centrale voorzieningen partijen, teneinde een verbetering door te voeren) wordt binnen Nictiz een impactanalyse uitgevoerd waarbij de impact van de voorgestelde wijzigingen op de informatiebeveiliging van het LSP en de totale EPD-keten wordt bepaald.

Externe controle op Nictiz
Veel controle en toezichtactiviteiten worden door externen uitgevoerd om de onafhankelijkheid en de betrouwbaarheid van het resultaat te garanderen.

Extern uitgevoerde maatregelen betreffen:

- Eenmalige algemene audit Nictiz, uitgevoerd door een geaccrediteerde auditor in 2005 in verband met de startfase van de op het EPD gerichte activiteiten;
- Audit op het Beveiligingsplan LSP door geaccrediteerde auditor in 2006;
- Audit op de implementatie van de de beveiliging van het LSP, uitgevoerd in 2008 door geaccrediteerde auditor;
- Externe audit op de beveiliging van het LSP. Het betreft een jaarlijkse audit die het laatst werd uitgevoerd in 2009. In deze audit wordt ook meegenomen:
    - Het beveiligingsbeleid van beheerder CSC;
    - Toetsing van het LSP continuïteitplan;
    - Toetsing van het LSP Jaarplan Informatiebeveiliging;
    - de procedures Notificatie & Escalatie LSP;
    - Toetsing van de Procedure Logging en autorisatie.
- Indringerstest LSP, uitgevoerd door specialistische geaccrediteerde auditor voor het laatst in 2009. Het betreft een jaarlijkse indringerstest. De test maakt onderdeel uit van de periodieke Grootschalige ketenbrede indringerstest (GKI) die in Hoofdstuk 5 al aan de orde kwam;
- LSP controletest, een jaarlijks door CSC uitgevoerde indringerstest;
- Uitwijktest LSP, een tweejaarlijkse test door CSC;
- Security audit door ISO 27001 certificeringauditor. Deze audit gebeurt eens in de 3 jaar geheel ten behoeve van de certificering en jaarlijks gedeeltelijk (surveillance audit). In deze audit wordt ook meegenomen:
    - Het beveiligingsbeleid van beheerder CSC;
    - Toetsing van het LSP continuïteitplan;
    - Toetsing van het LSP Jaarplan Informatiebeveiliging;

- de procedures Notificatie & Escalatie LSP;
- Toetsing van de Procedure Logging en autorisatie.

Eventuele aanbevelingen uit de audits worden opgevolgd.

Externe controle door Nictiz
Daarnaast voert Nictiz vanuit zijn verantwoordelijkheden controle uit op het LSP, de ZSP-en, de XIS en GBZ-en. Dat gebeurt regulier en steekproefsgewijs, maar ook als daartoe aanleiding zou zijn vanwege een incident. Nictiz stelt met de audit en controle de conformiteit met de betreffende PvE vast. Overigens worden deze controles hoofdzakelijk door externe onafhankelijke auditors uitgevoerd in opdracht van en in samenwerking met Nictiz.

GBZ schouwingen
In het kader van de controle op de GBZ-en worden steekproefsgewijze schouwingen uitgevoerd van GBZ-en. Daarbij wordt aan het PvE GBZ getoetst en worden eigen verklaringen van de GBZ-en gecontroleerd. Dit proces is doorlopend en gestart in 2010. Per jaar zal een representatief aantal schouwingen worden uitgevoerd. Voor aanvangsjaar 2010 zal dat aantal rond de vijfenzeventig liggen.

Ook worden door Nictiz kwalificaties van de XIS uitgevoerd (per release), waarbij de applicatie eisen, waaronder beveiligingseisen, worden getoetst.

ZSP kwalificatie
Kwalificatie van ZSP-en geschiedt door externen in opdracht van Nictiz. Dit is een doorlopend proces en ook herkwalificatie valt hieronder, conform de vereisten voor kwalificatie en herkwalificatie in het PvE ZSP. Onderdeel van de kwalificatie is een audit door een externe geaccrediteerde partij.

Beheer maatregelen
Daarnaast worden door Nictiz en CSC een groot aantal beheer maatregelen uitgevoerd die een continu proces van controle inhouden op het beveiligingsbeleid van CSC, het LSP continuiteitplan, het LSP Jaarplan informatiebeveiliging en het Nictiz beveiligingsplan. Verder is er continu toezicht op de procedure voor logging en autorisatie op het LSP.

Intelligent loggen
Binnen het Project Intelligent Loggen is de procedure voor intelligent loggen uitgewerkt en zijn de waarborgen voor optimaal intelligent toezicht op de logging vastgesteld. Het project is afgerond en de resultaten zijn in beheer genomen in de Procedure Monitoring LSP.

Telkens wanneer patiëntgegevens worden aangemeld of opgevraagd, worden de volgende ‘loggegevens’ bijgehouden:
- het BSN van de patiënt;
- het UZI-nummer en het UZI-abonneenummer van de beroepsbeoefenaar en de zorgaanbieder die de gegevens heeft opgevraagd en heeft verstrekt;
- het soort gegevens dat is verwerkt, en
- de datum en het tijdstip van de verwerking.

Logging vindt zowel plaats in de centrale gebruikersregistratie op het LSP als decentraal op de systemen van zorgaanbieders.

De logging is indien noodzakelijk toegankelijk voor de logbeheerder bij CSC. Door het toepassen van intelligente logging kan deze onrechtmatige toegang tot het EPD opsporen en melden volgens de Procedure monitoren LSP. Intelligente logging gebeurt op basis van criteria die een mogelijk onjuist gebruik van het landelijk EPD laten zien, die naar aanleiding van een risicoanalyse zijn vastgesteld en periodiek worden geëvalueerd. Door intelligente logging worden mogelijk verdachte raadplegingen zichtbaar gemaakt binnen het totaal aan logs.

Analyse van de loggegevens
Als beheerder van het LSP is Nictiz verantwoordelijk voor de analyse van de loggegevens die betrekking hebben op het gebruik van het LSP. Om deze analyse te kunnen maken wordt eerst vastgesteld wat normaal gebruik van het LSP is. Daarbij kan bijvoorbeeld mede gekeken worden naar de volgende factoren:
- het aantal opvragingen door een individuele zorgaanbieder;
- het aantal pogingen om een dossier op te vragen waarvoor geen autorisatie aanwezig is;
- het aantal opvragingen via mandatering.

Aan de hand daarvan wordt periodiek een rapportage opgesteld met betrekking tot normoverschrijdingen, mogelijk misbruik en de stabiliteit van het schakelpunt.

Use cases
Ten behoeve van de logginganalyse en het toezicht op de toegang is de mogelijkheid gecreëerd te zoeken naar verdachte opvraagpatronen in de toegangslog. Er zijn momenteel diverse 'use cases' uitgewerkt van mogelijk verdachte opvragingen waarvoor dagelijks automatisch queries worden gedraaid op de webportal, die indien indien dit een resultaat oplevert, hierover een rapportage aan het LSP genereert. Daarnaast vinden ook ad hoc analyses plaats. Mogelijk verdachte opvragingen worden op die manier gesignaleerd en door Nictiz onderzocht en opgevolgd conform de Procedure Monitoring LSP.

Procedure Monitoring LSP
Er zijn diverse procedures ingericht bij Nictiz en CSC om toezicht uit te oefenen op het zorgvuldige en rechtmatige gebruik van het LSP. Naast procedures die al aan de orde gekomen zijn is de Procedure Monitoring LSP van belang.

In deze procedure wordt onderscheid gemaakt tussen twee vormen van monitoring, namelijk security monitoring en real-time security monitoring. De laatste is een procedure die ervoor zorgt dat de technisch toezichthouder van het LSP een telefonische melding ontvangt van de beheerder van het LSP zodra een overschrijding van een norm is gesignaleerd, 24 uur per dag. De Security Officer van Nictiz vervult de rol van technisch toezichthouder. Deze melding gebeurt wanneer een norm voor aantallen opvragingen met dezelfde UZI pas, dan wel met dezelfde applicatie worden overschreden.

Ook in het kader van security monitoring kan een melding worden gedaan bij de technisch toezichthouder. Dit gebeurt, indien er sprake is van een norm overschrijding die blijkt uit de intelligente logging, een maal per dag per email. Daarbij wordt geen inhoudelijk informatie verstrekt, maar een verwijzing naar het type norm overschrijding. CSC voert in aansluiting op de Procedure Monitoring het proces 'Signalering norm overschrijving' uit, teneinde de melding te kunnen maken.

De Security Officer beoordeelt een normoverschrijding op prioriteit. Dan kan resulteren in een melding voor beheer van de AORTA keten. Een aantal meldingen dat kan volgen uit intelligent loggen heeft betrekking op het beheer van AORTA. Deze meldingen kunnen duiden op een fout in de XIS-applicatie. Deze meldingen worden als incident opgelost binnen de reguliere incidentenprocedure.

Ook kan een normoverschrijding na beoordeling door de Security Officer aanleiding geven voor een melding aan een van de formele toezichthouders. In het document Aanbevelingen bij Toezichtkader EPD wordt hierop nader ingegaan. In een aantal gevallen zal direct worden opgetreden door de technisch toezichthouder. Dit betreft bijvoorbeeld normoverschrijdingen waarbij een excessief aantal bevragingen optreedt. In zo'n geval zal deze de melding kunnen escaleren tot een zogenoemde prioriteit 1 incident. De procedure sluit daarbij aan op het Calamiteitenplan landelijk EPD. In zo'n geval kan besloten worden tot afsluiting van een GBZ en/of blokkade van een UZI-pas.

Procedure Vermeend Misbruik
Naast de Procedure monitoren LSP bestaat er een apart proces voor het afhandelen van meldingen in het kader van de Procedure Vermeend Misbruik. Deze procedure volgt een apart traject en gaat over de afhandeling van meldingen die binnenkomen via het klantenloket EPD. Deze procedure, die tevens een toezichtmaatregel inhoudt, wordt besproken in hoofdstuk 9 Controlemogelijkheden van de patiënt.

Hoofdstuk 8 Toezicht door de zorgaanbieder

8.1 Verplichtingen zorgaanbieder

De zorginstelling en de zorgverlener registreren de patiëntgegevens van patiënten die bij hen komen in het kader van de behandeling. Een zorgaanbieder dient te voldoen aan tal van wettelijke verplichtingen ten aanzien van registratie van patiëntgegevens en de administratieve organisatie. Dat betreft ook maatregelen van interne controle en de organisatie daarvan. De Wbp en de WGBO stellen eisen aan de verwerking van de patiëntgegevens. Artikel 13 Wbp verplicht de zorgverlener tot het voorzien in adequate gegevensbeveiliging en daarmee in passende technische en organisatorische maatregelen op dat gebied. Deze verantwoordelijkheid brengt tevens de verplichting met zich mee om op de werkzaamheid en kwaliteit van de getroffen maatregelen toe te zien en deze te controleren.

Daarnaast verplicht het medisch beroepsgeheim van de hulpverlener hem ertoe verantwoordelijkheid te nemen voor de vertrouwelijke en rechtmatige uitwisseling van gegevens van patiënten[17]. In dit opzicht geldt ook de zorginstelling als 'hulpverlener' en geldt voor de instelling een zorgplicht voor het beschermen van het medisch beroepsgeheim.

8.2 Informatiebeveiliging en toezicht

Op grond van artikel 13 Wbp is de zorgverlener zoals gesteld verplicht tot het voorzien in adequate persoonsgegevensbeveiliging en daarmee in passende technische en organisatorische maatregelen op dat gebied. Deze verantwoordelijkheid brengt tevens de verplichting met zich mee om op de werkzaamheid en kwaliteit van de getroffen maatregelen toe te zien en deze te controleren. Uit de beveiligingsverplichting volgt daarmee derhalve automatisch ook de verplichting tot controle en toezicht op de eigen activiteiten wat betreft de gegevensverwerking ten behoeve van het landelijk EPD, hetgeen in de context van dit toezichtkader van belang is. Een adequate gegevensbeveiliging voorziet dus in maatregelen van zelftoezicht en controleactiviteit op de rechtmatigheid van de gegevensverwerking door de zorgverlener als noodzakelijke voorwaarde.

Een goede uitwerking van adequate gegevensbeveiliging in de zorgsector is de NEN 7510, zoals in hoofdstuk 3.7 aan de orde kwam. Daarnaast is het voldoen aan de NEN 7510 norm in de zorg verplicht gesteld in de Regeling gebruik burgerservicenummer in de zorg.

De NEN 7510 geeft algemene richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die een organisatie in de gezondheidszorg moet treffen ter beveiliging van de informatievoorziening. De subnorm NEN 7512 is specifiek gericht op de elektronische gegevensuitwisseling in de zorg.

De NEN 7510 noemt onder andere de volgende aspecten:
- *vertrouwelijkheid:* het beschermen van gegevens tegen onbevoegde kennisname;
- *integriteit:* het waarborgen dat gegevens niet ongecontroleerd worden gewijzigd of verloren gaan;

[17] Op grond van artikel 7:457 BW.

- *beschikbaarheid:* het zekerstellen dat gegevens en informatiediensten op de gewenste momenten beschikbaar zijn voor gebruikers;
- *onweerlegbaarheid:* het waarborgen dat het vastleggen van gegevens of het verzenden van een bericht niet kan worden ontkend.

Om te voldoen aan de normen van de NEN 7510, dient de zorgaanbieder te controleren en toezicht te houden op het structureel in overeenstemming met de gestelde normen werken, waardoor vertrouwd kan worden op maatregelen van intern toezicht en controle op het rechtmatige gebruik van het landelijk EPD bij instellingen die aan de NEN 7510 voldoen.

In dit kader is het van belang dat IGZ, naar aanleiding van eerder onderzoek door IGZ en CBP naar informatiebeveiliging van ziekenhuizen, verlangt dat alle Nederlandse ziekenhuizen in 2010 een audit laten uitvoeren door een externe geaccrediteerde partij op naleving van de NEN 7510. De resultaten daarvan dienen aan IGZ te worden opgeleverd. Hiertoe is door de Nederlandse Vereniging van Ziekenhuizen een toetsingsreglement opgesteld.

GBZ-eisen
Wanneer bij deelname aan het landelijk EPD de zorgaanbieder ertoe overgaat zijn informatiesysteem aan te melden op het LSP dienen zijn informatiesystemen daarnaast te voldoen aan de kwalificatie van Goed Beheerd Zorgsysteem (GBZ). Dat brengt een aantal verplichtingen voor de zorgaanbieder met zich die voortvloeien uit de eisen die gesteld zijn aan het voeren en in stand houden van een GBZ in het PvE GBZ. Deze verplichtingen zijn vastgelegd in de deelnemersovereenkomst die Nictiz sluit met de zorgaanbieder. De eisen sluiten aan op de NEN7510 normering.

De patiëntgegevens in het GBZ dienen beveiligd te zijn tegen ongeautoriseerde toegang. Alleen zorgaanbieders en door hen gemandateerde medewerkers kunnen via het GBZ met behulp van de persoonlijke UZI-pas patiëntgegevens opvragen uit het landelijk EPD.

Op grond van de NEN 7510 zijn zorgaanbieders verplicht een risicoanalyse uit te voeren met betrekking tot hun informatiesystemen en alle externe verbindingen en dienen zij aanvullende beveiligingmaatregelen maatregelen te nemen voor de risico's die hierin worden onderkend. Ook het GBZ zelf moet voorzien zijn van een UZI-servercertificaat om patiëntgegevens te kunnen uitwisselen via een beveiligde verbinding met het LSP.

Het GBZ dient bovendien professioneel te worden beheerd. Dit vergt periodieke controle en eventueel preventief onderhoud. Het GBZ dient een decentrale logging in stand te houden waarin ontvangen opvraagberichten en verzonden opleverberichten worden vastgelegd evenals de gebruikershandelingen op het GBZ.

Controles Nictiz
Van belang voor het toezicht is dat niet alleen de zorgverlener zelf, maar dientengevolge ook Nictiz toeziet op het rechtmatige gebruik van het landelijk EPD, middels de controles op het voldoen aan de eisen van een GBZ (GBZ schouwingen).

ZSP vereisten
Bij deelname aan het landelijk EPD maakt de zorgverlener daarnaast gebruik van de diensten van een ZSP. Een Zorg Service Provider (ZSP) is een partij die een beveiligde

verbinding aanbiedt tussen het GBZ van de zorgaanbieder en het LSP. Op grond van artikel 14 Wbp is de zorgverlener verplicht om schriftelijke afspraken te maken met deze bewerker in de zin van de Wbp omtrent de beveiliging van de gegevensverwerking. Daaruit volgt dat de zorgverlener alleen in zee kan gaan met een ZSP die in overeenstemming met NEN 7510 zijn dienstverlening uitvoert. Dit sluit aan op de ZSP vereisten in het Programma van Eisen ZSP.

Onder andere dient de ZSP een beveiligingsplan op te stellen waarin is aangegeven welke maatregelen de ZSP heeft ingericht voor de beveiliging van alle netwerkkoppelingen (waaronder met de beheersystemen, het LSP, de GBZ-en, de SBV-Z en het UZI-register). De beheerder van de ZSP is verantwoordelijk voor de implementatie en handhaving van deze maatregelen en procedures op grond van de ZSP vereisten.

In het organisatieplan van de ZSP worden organisatorische taken, bevoegdheden en verantwoordelijkheden in het kader van informatiebeveiliging toegekend aan functies in de organisatie. De apparatuur van de ZSP bevindt zich in een fysiek beveiligde omgeving en is slechts toegankelijk voor geautoriseerd personeel van de ZSP.

Toezicht Nictiz
Ten behoeve van de controle op de juiste werking en de navolging van de juiste procedures worden alle beheerhandelingen vastgelegd in logging. ZSP's zijn onderwerp van controle en toezicht door de procedure van noodzakelijke kwalificatie en herkwalificatie door Nictiz.

Van belang voor het toezicht is het feit dat de zorgverlener op grond van artikel 14 Wbp verantwoordelijk is om toe te zien op de adequate gegevensbeveiliging door de bewerker, de ZSP. Daarnaast is van belang dat ook Nictiz in het kader van de correcte werking en uitvoering van het EPD toeziet op de ZSP kwalificaties en de eisen voor gegevensbeveiliging die daarvan onderdeel uitmaken.

Waarborgen voor toezicht
Zodoende zijn er waarborgen voor toezicht en controle op het rechtmatige gebruik van het landelijk EPD bij en door de zorgverlener. Dit is van groot belang in de huidige situatie waarin formele toezichthouders niet zelfstandig alle toezichtactiviteit kunnen en willen uitvoeren en derhalve moeten kunnen steunen op maatregelen van zelftoezicht en interne controle. In het document Aanbevelingen bij Toezichtkader EPD is de aanbeveling van een maatregel opgenomen die erop ziet de waarborgen voor (zelf)toezicht structureel te kunnen garanderen.

Hoofdstuk 9 Controlemogelijkheden van de patiënt

9.1 Wettelijke rechten patiënt

Iedere patiënt die deelneemt aan de mogelijkheid tot gegevensdeling via het landelijk EPD heeft een aantal wettelijke rechten met betrekking tot zijn gegevens. Dat geldt voor zowel de gegevens die door het Landelijk schakelpunt worden verwerkt, als de gegevens die worden verwerkt in het brondossier bij de zorgverlener. De rechten van de patiënt worden geformuleerd in de WGBO, de Wet bescherming persoonsgegevens, de Wet BIG en het voorstel van de Kaderwet EPD. Het klachtrecht van de patiënt is bovendien nader uitgewerkt in de Wet klachtrecht cliënten zorgsector.[18]

Rechten met betrekking tot het LSP
Het LSP bevat een verwijsindex waarin indexgegevens zijn opgenomen die de patiënt betreffen. Ook de logging van acties op het LSP bevat gegevens die de patiënt betreffen. De rechten met betrekking tot de gegevens worden via het Informatiepunt BSN in de zorg en landelijk EPD (het 'Klantenloket EPD') uitgeoefend tegenover de beheerder van het LSP. Daarnaast heeft de patiënt vanaf 2011 de mogelijkheid tot 'online' inzage in zijn gegevens via het 'Patiëntenportaal'.

Bezwaar
Iedere patiënt kan besluiten om niet deel te nemen aan de uitwisseling van gegevens via het landelijk EPD en zijn bezwaar aantekenen. Voorafgaand aan de introductie van het EPD zijn alle inwoners van Nederland per brief van deze mogelijkheid op de hoogte gesteld. Daarnaast ontvangt de patiënt bij eerste aanmelding van patiëntgegevens bij het LSP een persoonlijke brief om hem hiervan op de hoogte te stellen. Daarbij wordt de patiënt geïnformeerd over de werking van het landelijk EPD en gewezen op de mogelijkheid om bezwaar te maken. Ook na de introductie van het EPD kan een patiënt op ieder moment alsnog bezwaar maken en deelname blokkeren. Indien een patiënt alsnog wenst deel te nemen aan het EPD kan het bezwaar worden ingetrokken.

Gedifferentieerd bezwaar
Het is patiënten die deelnemen aan het landelijk EPD daarnaast mogelijk om de toegang tot index- en patiëntgegevens voor specifieke personen of instellingen te blokkeren. Dit is vastgelegd in het voorstel voor de Kaderwet EPD. Dit betekent dat de gegevens van de patiënt voor een bepaalde zorgaanbieder of zorgverlener dan wel categorie van zorgaanbieders of zorgverleners volledig worden afgeschermd. Dat een dergelijke mogelijkheid geboden moet worden kan ook worden afgeleid uit de rechten die in de Wbp en de WGBO beschreven zijn, zoals het recht op afscherming van persoonsgegevens en de mogelijkheid tot het maken van bezwaar tegen bepaalde gegevensverwerking(en).

Voorafgaande toestemming bij opvraging
De zorgaanbieder is slechts bevoegd tot het opvragen van gegevens uit het EPD als de patiënt hem daarvoor toestemming heeft gegeven.[19] De patiënt heeft het recht om deze toestemming te onthouden.

[18] De rechten van de patiënt i.v.m. het landelijk EPD worden uitgebreid beschreven in het 'Vertrouwensmodel landelijk EPD', opgesteld door Nictiz.
[19] Artikel 13 f lid 3 Kaderwet EPD.

Indien een zorgaanbieder via de hoofdbehandelaar een verzoek tot hulpverlening heeft ontvangen en er geen direct contact met de patiënt is, mag hij de toestemming veronderstellen, tenzij de patiënt anders te kennen heeft gegeven.

Inzage
Iedere patiënt heeft recht op inzage in zijn indexgegevens en de hem betreffende loggegevens die bij het LSP worden verwerkt.[20] Uit de indexgegevens kan worden afgeleid welke zorgaanbieders patiëntgegevens hebben aangemeld bij het LSP. De loggegevens geven weer welke zorgaanbieders de indexgegevens hebben geraadpleegd. De inzage kan verlopen via het Klantenloket EPD of via de eigen toegang tot het Patiëntenportaal.

Correctie en vernietiging
Indien gegevens in de verwijsindex onjuist zijn of in strijd met een wettelijk voorschrift worden verwerkt kan de patiënt deze via het Klantenloket EPD laten corrigeren, verwijderen of afschermen.[21] Op verzoek van de patiënt zorgt de beheerder van het LSP daarnaast voor gehele of gedeeltelijke vernietiging van de indexgegevens van de patiënt.[22]

Rechten ten opzichte van het dossier
Het lokale zorginformatiesysteem van de zorgverlener bevat het 'brondossier' van de patiënt dat wordt bijgehouden door de zorgaanbieder. De rechten van de patiënt met betrekking tot de patiëntgegevens in het brondossier worden uitgeoefend tegenover de zorgaanbieder.

Inzage en afschrift
Het recht op inzage heeft betrekking op het gehele medische dossier. Dit omvat de gegevens in het brondossier die onderdeel uitmaken van het landelijk EPD en de loggegevens in het informatiesysteem van de zorgaanbieder. De patiënt kan een verzoek tot inzage indienen bij de zorgaanbieder. Via het Patiëntenportaal zal de patiënt in de toekomst ook medisch inhoudelijke gegevens uit zijn brondossiers kunnen bekijken voorzover deze beschikbaar zijn voor uitwisseling via het landelijk EPD.

Correctie en vernietiging
Indien gegevens in het dossier onjuist zijn of in strijd met een wettelijk voorschrift worden verwerkt kan de patiënt deze laten corrigeren, verwijderen of afschermen. Ook kan de patiënt op grond van de WGBO een verzoek doen tot vernietiging van zijn dossier. Een aanpassing of verwijdering werkt door naar het gedeelte van het dossier dat is aangemeld voor het landelijk EPD.

Klachtrecht
Indien een zorgaanbieder bij de uitoefening van zijn taak een wettelijke norm heeft geschonden zijn civielrechtelijke, tuchtrechtelijke of strafrechtelijke acties mogelijk, waaronder ook de mogelijkheid een klacht in te dienen. Naast het tuchtrecht, de Wbp en het voorstel van de Kaderwet EPD biedt de Wet klachtrecht cliënten zorgsector (WKCZ) een mogelijkheid voor klachten wegens onzorgvuldig of onrechtmatige handelen van de zorgverlener of instelling.

[20] Artikel 13 e lid 1 Kaderwet EPD. Deze bepaling is een concretisering van het bepaalde in artikel 35 Wet bescherming persoonsgegevens, waar het inzagerecht in zijn algemeenheid is geregeld en van artikel 7:456 BW dat het inzagerecht specifiek regelt voor het medisch dossier.

[21] Artikel 36 Wbp en voorstel voor Kaderwet EPD.

[22] Artikel 13e lid 2 sub b Kaderwet EPD.

Klachtenprocedure WKCZ
Op grond van de WKCZ dient iedere zorgaanbieder een regeling te treffen die voldoet aan de eisen van de WKCZ voor de behandeling van klachten over een gedraging van hem of van voor hem werkzame personen jegens een patiënt.

Er dient een klachtencommissie in de instelling te worden aangesteld die de klachten behandelt. De zorgaanbieder laat binnen een maand nadat hij de uitspraak heeft ontvangen weten wat hij met het oordeel van de klachtencommissie doet.[23] Is sprake van een ernstige situatie met een structureel karakter, waaromtrent de zorgaanbieder geen maatregelen neemt, dan is de klachtencommissie verplicht de Inspectie voor de Gezondheidszorg (IGZ) hiervan in kennis te stellen.[24]

Gedragingen met betrekking tot het landelijk EPD waarover op grond van de WKCZ zou kunnen worden geklaagd, zijn bijvoorbeeld het niet meewerken aan de uitoefening van patiëntenrechten zoals een verzoek om inzage en het verwerken van onjuiste of onvolledige gegevens.

Tuchtrecht
Op grond van het tuchtrecht kan de patiënt een klacht indienen in verband met overtreding van de normen in de Wet BIG. Dit geldt ook ten aanzien van het gedrag van de hulpverlener met betrekking tot het landelijk EPD.

Klacht over gegevensverwerking bij CBP
Nadat een patiënt een klacht heeft ingediend bij de verantwoordelijke zorgverlener of instelling staat op grond van de Wbp de mogelijkheid open de klacht bij het CBP in te dienen met het verzoek tot behandeling, ingeval van overtreding van de normen in deze wetgeving of aanverwante wetgeving zoals de WGBO. Vervolgens staat ook een gang naar de rechter open.

Het voorstel voor de Kaderwet EPD voorziet daarnaast in een mogelijkheid jegens een zorgverlener of instelling een klacht in te dienen bij het Klantenloket EPD met betrekking tot enige norm in de kaderwet.

9.2 Controle van de toegang en maatregelen

Telkens wanneer patiëntgegevens worden aangemeld of opgevraagd, worden een aantal loggegevens bijgehouden.[25] Logging vindt zowel plaats in de centrale gebruikersregistratie op het LSP als decentraal op de systemen van zorgaanbieders.

Patiënten zullen via het Klantenloket EPD en het Patiëntenportaal inzicht hebben in de loggegevens. Ook kan inzage van de loggegevens in het lokale GBZ verzocht worden bij de zorgverlener. Patiënten kunnen langs deze weg de raadpleging van hun gegevens monitoren en onterechte raadpleging of vermoedens daarvan opvolgen. Bij raadpleging van de loggegevens door de patiënt worden de naam van de zorgaanbieder en de betreffende beroepsbeoefenaar getoond. Daarnaast is het mogelijk om een selectie te maken van loggegevens van een specifieke zorgaanbieder of beroepsbeoefenaar. Daarbij wordt onderscheid gemaakt tussen bestaande en

[23] Artikel 2 lid 5 WKCZ.
[24] Artikel 2a WKCZ.
[25] Zie hoofdstuk 7.7 Controle en toezichtsmaatregelen, onder *Project Intelligent Loggen,* voor een opsomming van de gegevens.

nieuwe behandelrelaties.

Indien een patiënt twijfelt aan de rechtmatigheid van een raadpleging of de juistheid van de gegevens in het log, kan hij zich wenden tot de betreffende zorginstelling of zorgverlener of tot het Klantenloket EPD. Ook kan hij in zo'n geval direct gebruik maken van de overige patiëntenrechten en zich wenden tot de formele toezichthouders.

De logging zal op grond van de wetgeving ook toegankelijk zijn voor de toezichthouders. Zij kunnen de loggegevens onder omstandigheden benaderen om onrechtmatige toegang tot het EPD te kunnen opsporen, vaststellen of sanctioneren.

Klantenloket EPD
Hierboven is voor verschillende rechten aangegeven wanneer men zich tot het klantenloket kan wenden. Bij de uitwerking van het voorstel voor de Kaderwet EPD is bepaald dat het Klantenloket EPD de integrale dienstverlening aan de burger dient te borgen. Het klantenloket dient het centrale aanspreekpunt voor de burger te worden inzake het landelijke EPD (maar is zoals hierboven is beschreven dus niet het enige aanspreekpunt voor de patiënt wanneer hij zijn rechten wil uitoefenen en gegevensuitwisseling tussen zorgverleners wil monitoren). Het klantenloket zal ook het Patiëntenportaal beheren waarin de patiënt direct toegang heeft tot zijn gegevens. Het huidige klantenloket, de voorloper van het klantenloket met alle functionaliteiten zoals beschreven in het voorstel voor de Kaderwet EPD, functioneert onder de naam Informatiepunt EPD.

Het Klantenloket EPD is ook het aanspreekpunt voor vermeende gevallen van misbruik van het EPD. Hiervoor is de Procedure Vermeend Misbruik ingericht.

Procedure Vermeend Misbruik
In de hoofdstukken 6 en 7 is deze procedure, die tevens een toezichtmaatregel inhoudt al aan de orde gekomen. Er bestaat een apart proces voor het afhandelen van meldingen in het kader van de Procedure Vermeend Misbruik. Patiënten kunnen een melding van vermeend misbruik indienen bij het Klantenloket EPD. De behandelaar van het klantenloket vraagt vervolgens een feitenrapportage op bij Nictiz. Nictiz doet vervolgens een feitenonderzoek en rapportage inzake de melding aan het klantenloket, dat de melding vervolgens afhandelt conform procedure. Als geen sprake kan zijn van misbruik, bijvoorbeeld indien blijkt dat geen gegevens via het EPD uitgewisseld zijn, wordt de melding afgesloten. Onderdeel van de procedure is nu dat wanneer uit de feitenrapportage een redelijk vermoeden van misbruik ontstaat, de melding wordt doorgeleid aan de meest gerede formele toezichthouder, CBP dan wel IGZ. Ook volgt terugkoppeling aan de burger over de afhandeling.

Patiëntenportaal
Hierboven is het Patiëntenportaal al aan de orde gekomen. Het internet portaal wordt op dit moment ontwikkeld in samenwerking tussen Nictiz en CIBG en het ministerie van VWS. Het Patiëntenportaal zal door het Klantenloket EPD bij CIBG worden beheerd. Het Patiëntenportaal wordt ingericht overeenkomstig het Programma van Eisen voor het Goed Beheerd Patiëntenportaal (PVE GBP). Een van de voorwaarden is dat het Patiëntenportaal (periodiek) dient te kwalificeren als GBP. De kwalificatie wordt uitgevoerd door Nicitiz. Het Patiëntenportaal zal patiënten de mogelijkheid bieden om vanuit huis op een beveiligde manier inzage te krijgen in zijn gegevens die opvraagbaar zijn in het landelijk EPD, maar ook in zijn indexgegevens en de

toegangslogs die aan zijn BSN gekoppeld zijn in het systeem. Tevens zal hij de meeste van zijn rechten kunnen uitoefenen via het portaal zoals in dit hoofdstuk al aan de orde is gekomen. De toegang tot het portaal door de patiënt zal waarschijnlijk gerealiseerd worden met behulp van EPD-DigID. Naar verwachting zal het patiëntenportaal voor gebruik door de patiënt in 2011 gereed zijn. In elk geval zal het portaal gereed moeten zijn wanneer de aansluitverplichting voor zorgverleners voor aansluiting op het LSP zal gelden.