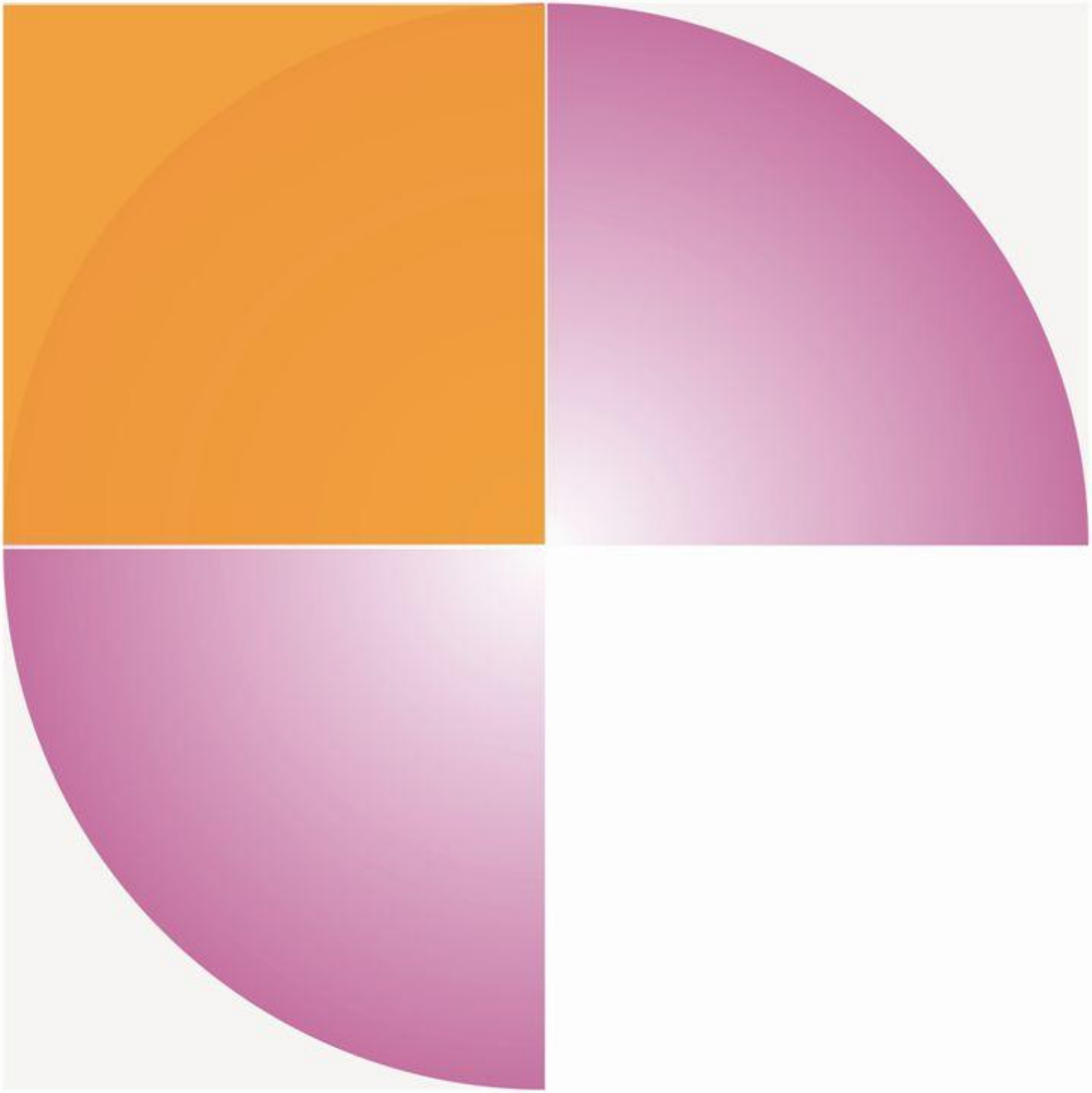
Toepassing BPPC-profiel

Richtlijn voor implementatie van toestemmingsprofielen binnen XDS-netwerken.

RADIOLOGIE, REGIO, XDS

Betere zorg
door betere informatie

Nictiz



Toepassing BPPC-profiel

Richtlijn voor implementatie van toestemmingsprofielen binnen XDS-netwerken.

RADIOLOGIE, REGIO, XDS

Betere zorg
door betere informatie

Nictiz

Datum
Juli 2012

ID Nummer
KA12012

Auteur(s)
Anton Ekker, Henk Hutink
Albert Jan Spruyt

Voorwoord

Patiënten moeten toestemming geven bij digitale beeldduitwisseling tussen zorgverleners. Om technische verwerking van deze toestemming mogelijk te maken, zijn toestemmingsprofielen nodig. Dit zorgt in de optimale situatie voor borging van de privacy van de patiënt en een werkbare situatie voor de zorgverlener. Op dit moment schiet de wetgeving te kort en zijn er technische beperkingen waardoor niet alle situaties ingevoerd kunnen worden.

Dit document beschrijft de toestemmingsprofielen van de patiënt op XDS-netwerken. Deze richtlijn is door experts opgesteld en beschrijft de Nederlandse verbijzondering van het 'BPPC-profiel' van IHE in Nederland.

Inhoudsopgave

H-1 Juridisch Kader 9

1.1. Introductie 9
1.2. Wet geneeskundige behandelingsovereenkomst (WGBO) 9
1.3. Wet bescherming persoonsgegevens (Wbp) 10
1.4. Wet beroepen individuele gezondheidszorg (Wet BIG) 11
1.5. Kwaliteitswet zorginstellingen (KWZi) 12
1.6. Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGiZ) 12
1.7. Convenant 'digitale beeld- en verslaguitwisseling' 12

H-2 De rechten van de patiënt 13

2.1. Inleiding 13
2.2. Gegevens in het brondossier 13
2.3. Gegevens in de XDS-registry 13

H-3 Toezichthouders 15

3.1. Inleiding 15
3.2. College bescherming persoonsgegevens 15
3.3. Inspectie voor de Gezondheidszorg (IGZ) 15
3.4. Nederlandse Zorg Autoriteit (NZa) 16

H-4 Toegangsmodel tot patiëntgegevens 17

4.1. Inleiding 17
4.2. De toegangsmodel 17
4.3. Identificatie en authenticatie 18
4.4. Autorisatie 18
4.5. Toestemming patiënt 20
4.6. Logging 20

H-5 Toepassing BPPC-profiel 22

5.1. Procedurele impact 22
5.2. Uitgangspunten BPPC-profiel 24
5.3. Mogelijkheden met BPPC-profiel 24
5.4. Functionele eisen 28
5.5. Landelijke policies 29
5.6. Object Identifier 31
5.7. Vastlegging toestemmingsprofielen 32

H-6 Verklarende woordenlijst 33
H-7 Tot slot 34

Inleiding

Als zorgverleners[1] digitale beelden en verslagen op CD's of DVD's met de patiënt meegeven ten behoeve van de patiëntbehandeling in een andere zorginstelling is er sprake van een impliciete toestemming van de patiënt. Zodra beelden en verslagen digitaal worden uitgewisseld is expliciete toestemming van de patiënt vereist. Om medische informatie te delen tussen zorgverleners is het noodzakelijk dat de patiënt toestemming verleent aan zijn zorgverlener. In deze richtlijn wordt beschreven welke toestemmingsprofielen landelijk gedefinieerd zijn voor XDS-netwerken. Dit document is geschreven voor projectleiders die XDS-netwerken implementeren.

Er is veel onduidelijkheid en spraakverwarring om de toestemming van de patiënt voor gegevensuitwisseling juist vast te leggen. De voornaamste redenen zijn: onbekendheid met de interpretatie, ontbreken van inhoudelijke kennis van de wetgeving en onbekendheid over toestemmingsprofielen. Dit document draagt bij aan het op uniforme wijze implementeren van toestemmingsprofielen. Omdat bij lopende discussies op het gebied van de toestemmingsprofielen veel spraakverwarringen zijn, is gekozen om eerst informatie te geven over wetgeving en daarna inhoudelijk in te gaan op de toestemmingsprofielen. Overigens is dit een startdocument. In de toekomst kunnen nieuwe toestemmingsprofielen toegevoegd worden.

Hoofdstuk één beschrijft het juridisch kader. Dit kader geeft aan welke wetgeving, maar ook welke juridische documenten een relatie hebben met de toestemmingsprofielen.

In hoofdstuk twee staan de rechten van de patiënt nader uitgelicht. Dit hoofdstuk verwijst grotendeels naar de regionale gedragscode 'elektronische gegevensuitwisseling in de zorg'.

In hoofdstuk drie wordt kort uitgelegd wie de toezichthoudende organisaties zijn.

In hoofdstuk vier staat beschreven hoe toegang kan worden verkregen tot de patiëntgegevens. De toegang tot patiëntgegevens wordt beschreven aan de hand van de toegangsketen.

Hoofdstuk vijf gaat over de toestemmingsprofielen die geïmplementeerd kunnen worden met behulp van het BPPC-profiel van IHE. In dit hoofdstuk wordt uitgelegd welke mogelijkheden er zijn op het gebied van toestemmingsprofielen, wat de onmogelijkheden zijn en tot slot welke policies er landelijk zijn gedefinieerd.

[1] In dit document worden de begrippen zorgverlener, zorgaanbieder, hulpverlener en beroepsbeoefenaar door elkaar gebruikt.

H-1 Juridisch Kader

1.1. Introductie

Voor digitale beelduitwisseling zijn meerdere wetten relevant. Dit hoofdstuk geeft een korte introductie van de relevante wetten.

Nb. Onderstaande paragrafen zijn overgenomen uit eerder opgestelde documenten die betrekking hebben op het Landelijk Schakelpunt. De Wet EPD is in april 2011 door de Eerste Kamer verworpen. Om deze reden worden komende tijd een aantal paragrafen nog herzien.

1.2. Wet geneeskundige behandelingsovereenkomst (WGBO)

De privaatrechtelijke verhouding tussen hulpverlener en patiënt is geregeld in een afzonderlijke afdeling van het Burgerlijk Wetboek, ook wel aangeduid als de Wet geneeskundige behandelingsovereenkomst (WGBO). De bepalingen in de WGBO zijn grotendeels bedoeld om de positie van de patiënt te beschermen. Zij hebben dan ook een dwingend rechtelijk karakter.

Binnen het vertrouwensmodel is de WGBO in twee opzichten relevant. In de eerste plaats is de hulpverlener op grond van de WGBO verplicht een dossier bij te houden en gedurende een termijn van 15 jaar te bewaren. Deze verplichting wordt ook wel aangeduid als de ‘dossierplicht’.

In de tweede plaats geeft de WGBO de patiënt recht op geheimhouding van zijn dossier. In beginsel mogen (alleen met toestemming van de patiënt) inlichtingen over de patiënt, dan wel inzage in of afschrift van de bescheiden in het dossier aan anderen worden verstrekt. Verstrekking kan echter zonder toestemming plaatsvinden indien wet- of regelgeving daartoe verplicht.

Toestemming van de patiënt is evenmin vereist voor verstrekking aan degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst. In dit geval kan op grond van de WGBO worden uitgegaan van veronderstelde toestemming. Voorwaarde is in dat geval dat de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden.

Bij de toegang tot patiëntengegevens moet duidelijk zijn in welke omstandigheden en in welke vorm toestemming voor de toegang tot of de verstrekking van patiëntengegevens vereist is. In de literatuur zien we de volgende vormen van toestemming voor gegevensverstrekking: veronderstelde toestemming, stilzwijgende toestemming en expliciete toestemming.

Van stilzwijgende toestemming wordt gesproken als de situatie rond de toegang of verstrekking van patiëntengegevens kenbaar is gemaakt voor de patiënt – ‘wie krijgt voor welk doel informatie?’. In dat geval mag een hulpverlener ervan uitgaan dat de patiënt instemt met de gegevensuitwisseling, mits dat uit diens gedrag (woord of gebaar) valt af te leiden. Omdat stilzwijgende toestemming een noodoplossing is die bedacht is in de gezondheidsrechtelijke literatuur en deze zich niet duidelijk onderscheidt van de veronderstelde toestemming, is

in dit rapport gekozen om voor de praktijk het onderscheid te vereenvoudigen tot veronderstelde en expliciete toestemming.

De toestemming van de patiënt voor het verstrekken van diens patiëntengegevens kan bestaan uit veronderstelde (of impliciete) toestemming of uit expliciete toestemming. Toestemming van de patiënt voor de verstrekking van zijn patiëntengegevens mag worden verondersteld onder de volgende voorwaarden:

- de toegang wordt verleend in een concrete situatie (inclusief spoedeisende zorg);
- de patiënt kan redelijkerwijs verwachten dat toegang tot zijn patiëntengegevens wordt verleend
- gegevens voor zorgdoeleinden worden verstrekt (inclusief overdracht van zorg, zorgondersteuning zoals dossierbeheer, financiële afwikkeling en dergelijke);
- de patiënt tegen gegevensuitwisseling geen bezwaar heeft gemaakt; en
- de gegevensverstrekking beperkt blijft tot hetgeen noodzakelijk is voor de ontvanger.

Van de patiënt moet expliciet om toestemming voor de verstrekking van diens patiëntengegevens worden gevraagd, wanneer:

- patiëntengegevens worden verstrekt aan een andere hulpverlener met het oog op een nieuwe behandelepisode;
- patiëntengegevens worden verstrekt naar ontvangers buiten de gezondheidszorg (politie, justitie, werkgever, advocaat) en
- patiëntengegevens worden verstrekt voor wetenschappelijk onderzoek.

1.3. Wet bescherming persoonsgegevens (Wbp)

Indexgegevens en patiëntgegevens worden aangemerkt als 'persoonsgegevens' in de zin van de Wet bescherming persoonsgegevens (Wbp). Dit betekent dat de verwerking van deze gegevens dient te voldoen aan de voorwaarden die de Wbp stelt. Voor het vertrouwensmodel is de Wbp van belang omdat in deze wet algemene beginselen voor gegevensverwerking zijn geformuleerd. Ten slotte kent de Wbp bepaalde rechten toe aan de 'betrokkene'.

Centrale begrippen

De Wbp is van toepassing zodra sprake is van een, al dan niet geautomatiseerde, verwerking van persoonsgegevens. Het begrip 'verwerking' omvat praktisch elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Een persoonsgegeven is 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. Uitgangspunt is dat een persoon identificeerbaar is indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld.

De index- en loggegevens op het XDS-registry hebben betrekking op natuurlijke personen (patiënten). De elektronische uitwisseling van deze gegevens dient dan ook te worden aangemerkt als een 'geautomatiseerde verwerking van persoonsgegevens' in de zin van de Wbp.

Veel normen in de Wbp richten zich tot de 'verantwoordelijke' voor de gegevensverwerking. Dit is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Daarnaast regelt de Wbp de positie van de 'betrokkene'. Dit is degene op wie een persoonsgegeven betrekking heeft. Waar het gaat om patiëntgegevens zal de behandelende zorgaanbieder doorgaans worden aangemerkt als de verantwoordelijke en de patiënt als de betrokkene.

Algemene beginselen van gegevensverwerking

De Wbp formuleert een aantal algemene regels met betrekking tot de toelaatbaarheid en de kwaliteit van gegevensverwerking. Een basisprincipe is dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze dienen te worden verwerkt. Daarnaast gelden de principes van doelbinding en verenigbaar gebruik. Doelbinding houdt in dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden dienen te worden

verkregen. Verenigbaar gebruik betekent dat deze gegevens vervolgens niet worden verwerkt op een wijze die onverenigbaar is met deze doeleinden.

Voor iedere verwerking van persoonsgegevens is een verwerkingsgrond vereist. De Wbp geeft een opsomming van mogelijke verwerkingsgronden. Zo is voor het raadplegen van medische gegevens in de registry door een zorgaanbieder, de toestemming van de betrokkene (lees: de patiënt), de verwerkingsgrond.

Beveiligingsplicht
De verantwoordelijke dient 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 de stand van de techniek. Een voorbeeld van een technische maatregel is het gebruik van de UZI-pas binnen de toegangsketen. Een organisatorische maatregel kan bijvoorbeeld bestaan uit het implementeren van een beleid voor het omgaan met persoonsgegevens.

De beveiligingsplicht in de Wbp is zeer ruim geformuleerd. Om nader te concretiseren wat onder passende maatregelen dient te worden verstaan, kunnen zorgaanbieders aansluiting zoeken bij de bestaande normen voor informatiebeveiliging in de gezondheidszorg (NEN-normen).

Zienswijze CBP
In augustus 2011 heeft CBP een zienswijze geschreven over het doorstartmodel voor landelijke gegevensuitwisseling medische gegevens. De conclusies en de gevolgen van deze zienswijze zijn in dit document verwerkt.

1.4. Wet beroepen individuele gezondheidszorg (Wet BIG)

De Wet BIG heeft als doel om de kwaliteit van de beroepsuitoefening te bevorderen en te bewaken en de patiënt te beschermen tegen ondeskundig en onzorgvuldig handelen door beroepsbeoefenaren. De wet spitst zich toe op de individuele gezondheidszorg, dat wil zeggen: zorg die rechtstreeks is gericht op een persoon.

Beroepsbeoefenaren
De Wet BIG bevat een systeem van titelbescherming voor een beperkt aantal beroepsgroepen. Wie een wettelijk geregeld beroep uitoefent, mag een publiekrechtelijk beschermde beroeps- of opleidingstitel voeren. Om te worden aangemerkt als een beroepsbeoefenaar in de zin van de Wet BIG moet worden voldaan aan een aantal wettelijke eisen. De belangrijkste daarvan hebben betrekking op de opleiding. Door een beschermde titel te voeren is voor derden duidelijk op welk gebied een bepaalde beroepsbeoefenaar deskundig is.

Het systeem van titelbescherming in de Wet BIG is voor de elektronische informatievoorziening (bijvoorbeeld XDS-netwerken) van belang omdat alleen beroepsbeoefenaars en door hen gemandateerde medewerkers hiertoe toegang kunnen krijgen.

Tuchtrecht
Voor bij wet geregelde beroepen voorziet de Wet BIG in tuchtrechtspraak. Deze dient voor het bevorderen en bewaken van de kwaliteit van de beroepsuitoefening. De Wet BIG geeft twee tuchtnormen. De eerste heeft betrekking op zorgvuldigheid bij het verlenen van zorg van de geregistreerde beroepsbeoefenaar ten opzichte van de patiënt. De tweede norm geldt voor alle andere gedragingen die strijdig zijn met het belang van een goede uitoefening van de individuele gezondheidszorg. Tuchtrecht, strafrecht en burgerlijk recht kunnen overigens tegelijkertijd worden toegepast.

Strafbepalingen
De Wet BIG kent naast tuchtrechtelijke maatregelen ook strafbepalingen. Deze gelden voor een ieder die in het kader van beroepsmatig handelen bepaalde wettelijke verboden of verplichtingen niet nakomt. Er zijn drie sancties mogelijk: hechtenis, geldboete en ontzetting uit het beroep.

1.5. Kwaliteitswet zorginstellingen (KWZi)

De Kwaliteitswet zorginstellingen (KWZi) stelt normen voor het verlenen van verantwoorde zorg. Deze normen zijn van toepassing op alle instellingen waar in georganiseerd verband zorg wordt aangeboden. Het gebruik van een -regionale- infrastructuur kan worden beschouwd als onderdeel van het verlenen van verantwoorde zorg. De zorginstelling dient op grond van de KWZi:

- verantwoorde zorg te bieden;
- zorg te dragen voor een op die zorg gerichte adequate organisatie;
- zorg te dragen voor een systematisch kwaliteitssysteem;
- een kwaliteitsjaarverslag te publiceren

De minister van VWS en, in dringende gevallen, de Inspectie voor de Gezondheidszorg (IGZ) zien toe op de naleving van de KWZi.

1.6. Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGiZ)

Bij het uitwisselen van persoonsgegevens moet worden voldaan aan wettelijke voorschriften. Het blijkt daarbij lastig om een goede vertaalslag te maken van wet naar praktijk. Met name het invullen van de patiëntrechten (informatieverstrekking en toestemming) blijkt lastig. Oorzaak is de diversiteit aan, vaak door elkaar lopende, voorzieningen, de diversiteit aan behandelrelaties en de schijnbare onmogelijkheid om alle betrokkenen over alle vormen van uitwisseling begrijpelijk te blijven informeren. De Gedragscode EGiZ voorziet in een oplossing daarvoor. Het geeft praktische richtlijnen voor zorgaanbieders en samenwerkingsverbanden om aan geldende regelgeving te kunnen voldoen. Het doel van de Gedragscode EGiZ is de formulering van een heldere en toepasbare set (gedrags)regels en bijbehorende normen voor gegevensuitwisseling tussen zorgaanbieders.

Bij de totstandkoming van de Gedragscode is een aantal uitgangspunten gehanteerd. In de eerste plaats dient de Gedragscode toepasbaar te zijn voor het belangrijkste deel van de bestaande en in de nabije toekomst denkbare oplossingen. In de tweede plaats dienen de normen, mede met het oog op de goedkeuring hiervan door het College bescherming persoonsgegevens (CBP), te voldoen aan de geldende (privacy)regelgeving. Tegelijkertijd moet een balans worden gevonden tussen de handhaving van de rechten van de patiënt en de werkbaarheid in de praktijk.
De reikwijdte van de Gedragscode is zeer ruim. Alle vormen van elektronische informatie-uitwisseling in het kader van de zorgverlening vallen hieronder.

Let op: ten tijde van dit schrijven is de elektronische gedragscode bijna gereed, het wordt eind 2012 ter goedkeuring aan het CBP voorgelegd.

1.7. Convenant ‘digitale beeld- en verslaguitwisseling’

De regionale gedragscode is van toepassing op alle vormen van elektronische informatie. Om informatie uitwisseling mogelijk te maken, zijn aanvullende afspraken nodig. Zo is er een convenant ‘digitale beeld- en verslaguitwisseling’ dat hier invulling aan kan geven. Dit convenant kan per situatie aangepast worden. Zo staat bijvoorbeeld beschreven hoe beelden uitgewisseld kunnen worden tussen regio’s en welke informatie in de regionale verwijsindex wordt opgeslagen ten behoeve van digitale beelden. De indeling van het convenant komt overeen met de indeling van de gedragscode.

Het beschreven convenant is een overeenkomst voor zorginstellingen die onderling beelden en verslagen gaan uitwisselen. Als regionale organisaties of samenwerkende ziekenhuizen onderling aanvullende afspraken willen maken op de regionale gedragscode, dan kan dit vastgelegd worden in een convenant.

H-2 De rechten van de patiënt

2.1. Inleiding

Iedere patiënt die deelneemt aan een vorm van gegevensuitwisseling, bv. via XDS-netwerk, heeft een aantal wettelijke rechten met betrekking tot zijn gegevens. Deze rechten kunnen worden onderverdeeld in twee categorieën:

1. rechten met betrekking tot gegevens in het ´brondossier´ dat door de zorgaanbieder wordt bijgehouden in het zorginformatiesysteem van de zorgaanbieder
2. rechten met betrekking tot gegevens op een elektronische informatievoorziening (bijvoobeeld XDS-netwerk).

Hieronder worden eerst de rechten van de patiënt met betrekking tot de gegevens in het brondossier aangegeven. Vervolgens komen de rechten met betrekking tot de gegevens in de XDS-netwerk aan de orde.

2.2. Gegevens in het brondossier

De patiëntgegevens die in het brondossier (bij XDS-netwerken heet dit 'document source/repository') staan, vallen onder de reguliere rechten die van toepassing zijn op de brondossierhouder. Vaak is dit de zorginstelling.

2.3. Gegevens in de XDS-registry

De rechten van de patiënt staan beschreven in de gedragscode Elektronische Gegevensuitwisseling in de Zorg. Onderstaande artikel is één op één overgenomen uit deze gedragscode. De manier waarop de patiëntrechten kunnen worden uitgevoerd staan beschreven in het convenant 'regionale beeld- en verslaguitwisseling'.

Artikel 4.1 uit de gedragscode:

4.1 De Betrokkene heeft de volgende rechten:

a. recht op informatie over:
   - de Elektronische Voorziening en de doeleinden van de Verwerking van Persoonsgegevens die via de Elektronische Voorziening systemen plaatsvindt;
   - de identiteit van de Verantwoordelijke(n) voor de Elektronische Voorziening;
   - de (categorieën van) Persoonsgegevens die door middel van de Elektronische Voorziening kunnen worden verwerkt;
   - de (categorieën van) Zorgaanbieders die via de Elektronische Voorziening toegang kunnen hebben tot Persoonsgegevens;
   - de mogelijkheid om toestemming voor de Verwerking van Persoonsgegevens te geven, dan wel in te trekken, dan wel om hier bezwaar tegen te maken;
   - de beoogde maximale omvang en de wijze waarop de Betrokkene wordt geïnformeerd bij substantiële uitbreiding van de omvang van de Verwerking van Persoonsgegevens als bedoeld in artikel 5.3 (zie gedragscode voor artikel 5.3).
b. recht op het geven, het onthouden en het intrekken van toestemming voor de Verwerking van persoonsgegevens of, indien toepasselijk, het maken van bezwaar hiertegen;

c. recht op inzage in en correctie van de hem betreffende persoonsgegevens, alsmede recht op een afschrift van deze persoonsgegevens;
d. recht op inzage in de hem betreffende gegevens in de Logging;
e. recht op vernietiging van de hem betreffende gegevens in het medisch dossier. Dit recht geldt niet voor zover het verzoek van de Betrokkene tot vernietiging gegevens betreft waarvan redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de patiënt, alsmede voor zover het bepaalde bij of krachtens de wet zich tegen vernietiging verzet;
f. recht op informatie over geconstateerd misbruik.

In de Gedragscode EGIZ wordt onderscheid gemaakt tussen Push en Pull verkeer. Bij Pull verkeer gelden de aanvullende rechten van de patiënt.

5.5 De Verwerking van Persoonsgegevens vindt slechts plaats nadat de Brondossierhouder hiervoor uitdrukkelijke toestemming van de Betrokkene heeft verkregen. De Brondossierhouder draagt zorg voor registratie van de uitdrukkelijke toestemming en de intrekking hiervan.

5.6 Raadpleging van gegevens door een Dossierraadpleger vindt slechts plaats nadat de aanwezigheid van een Behandelrelatie tussen de Betrokkene en de Dossierraadpleger is vastgesteld overeenkomstig artikel 8. Indien een Behandelrelatie niet kan worden vastgesteld vindt raadpleging slechts plaats nadat de Dossierraadpleger hiervoor uitdrukkelijke toestemming heeft verkregen van de Betrokkene.

Artikel 5.5 en 5.6 worden later in dit document behandeld.

H-3 Toezichthouders

3.1. Inleiding

Het toezicht op het gebruik van de infrastructuren voor gegevensuitwisseling in de zorg wordt uitgeoefend door verschillende toezichthouders. Het College bescherming persoonsgegevens (CBP) is belast met de handhaving van privacyregelgeving. De Inspectie voor de Gezondheidszorg (IGZ) handhaaft met name normen die betrekking hebben op de kwaliteit van de zorgverlening. De Nederlandse Zorgautoriteit (NZa) ziet toe op de naleving van het voor zorgverzekeraars geldende toegangsverbod.

3.2. College bescherming persoonsgegevens

Het CBP houdt toezicht op de naleving en toepassing van de Wet bescherming persoonsgegevens (Wbp) en een aantal andere wetten die het gebruik van persoonsgegevens regelen. Voor de gegevensuitwisseling in de zorg zijn de Wbp en de WGBO relevant. Het CBP is bevoegd om op eigen initiatief of op verzoek van een belanghebbende een onderzoek in te stellen naar de wijze waarop persoonsgegevens worden verwerkt. De verantwoordelijke op wie het onderzoek betrekking heeft is verplicht om, voor zover noodzakelijk, inzage te verschaffen in gegevens en systemen. In het kader van het toezicht kan het CBP zowel bij zorgaanbieders, bij de beheerder van de elektronische informatievoorziening als bij ICT-dienstverleners inzage verlangen in de gegevensverwerking.

Tegenover het CBP kan de verantwoordelijke zich niet beroepen op een geheimhoudingsplicht. Bij overtreding van de genoemde regelgeving is het CBP bevoegd tot het opleggen van een last onder dwangsom, dan wel tot het toepassen van bestuursdwang. Oplegging van een last onder dwangsom houdt in dat aan een overtreder een bevel (‘last’) wordt gegeven om te voldoen aan een wettelijke verplichting. Bij het niet tijdig gevolg geven aan de last is een dwangsom verschuldigd. Met een last onder dwangsom wordt een overtreding ongedaan gemaakt, of worden verdere overtredingen voorkomen. Van bestuursdwang is – kort gezegd – sprake wanneer het CBP feitelijk optreedt tegen handelen of nalaten in strijd met de wet.

Het toezicht door het CBP kan gericht zijn op het handelen van zorgaanbieders (waaronder individuele beroepsbeoefenaren) die zijn aangesloten op een elektronische informatievoorziening. Het CBP kan maatregelen nemen wanneer sprake is van onrechtmatige toegang tot de elektronische informatie voorziening. Het toezicht van het CBP kan daarnaast in ruimere zin betrekking hebben op het handelen van indicatieorganen en zorgverzekeraars.

3.3. Inspectie voor de Gezondheidszorg (IGZ)

De Inspectie voor de Gezondheidszorg (IGZ) handhaaft regels met betrekking tot de kwaliteit van de zorgverlening. Het toezicht op een elektronische informatievoorziening vindt derhalve plaats op grond van de Kwaliteitswet zorginstellingen (KWZi) en de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG). De bepalingen rondom het gebruik van het BSN en de infrastructuren geven nadere invulling aan de verantwoorde zorg die zorgaanbieders moeten leveren.
Om de taakuitoefening door de IGZ mogelijk te maken zijn zorgaanbieders verplicht tot verstrekking van alle inlichtingen en gegevens, waaronder medische persoonsgegevens, die noodzakelijk zijn voor het toezicht op het gebruik van het burgerservicenummer. Het gaat hierbij,

naast inzage in patiëntendossiers, ook om inzage in centrale en decentrale loggegevens. Tevens heeft de IGZ een wettelijk recht op inzage in patiëntendossiers.
De IGZ beschikt over bevoegdheden om corrigerend op te treden door middel van herstelsancties en bestraffende sancties. Hierdoor kan de IGZ onder andere boetes opleggen aan zorginstellingen die in de zorg te kort schieten. Daarnaast beschikt de IGZ, evenals het CBP, over de mogelijkheid om een last onder dwangsom op te leggen.

3.4. Nederlandse Zorg Autoriteit (NZa)

De NZa is belast met markttoezicht op het terrein van de gezondheidszorg. Het toezicht door de NZa op de elektronische informatievoorziening is beperkt tot de naleving van het aan zorgverzekeraars gerichte toegangsverbod. Bij overtreding van dit verbod legt de NZa een bestuurlijke boete op. Deze bedraagt voor een afzonderlijke overtreding ten hoogste € 100.000.

H-4 Toegangsmodel tot patiëntgegevens

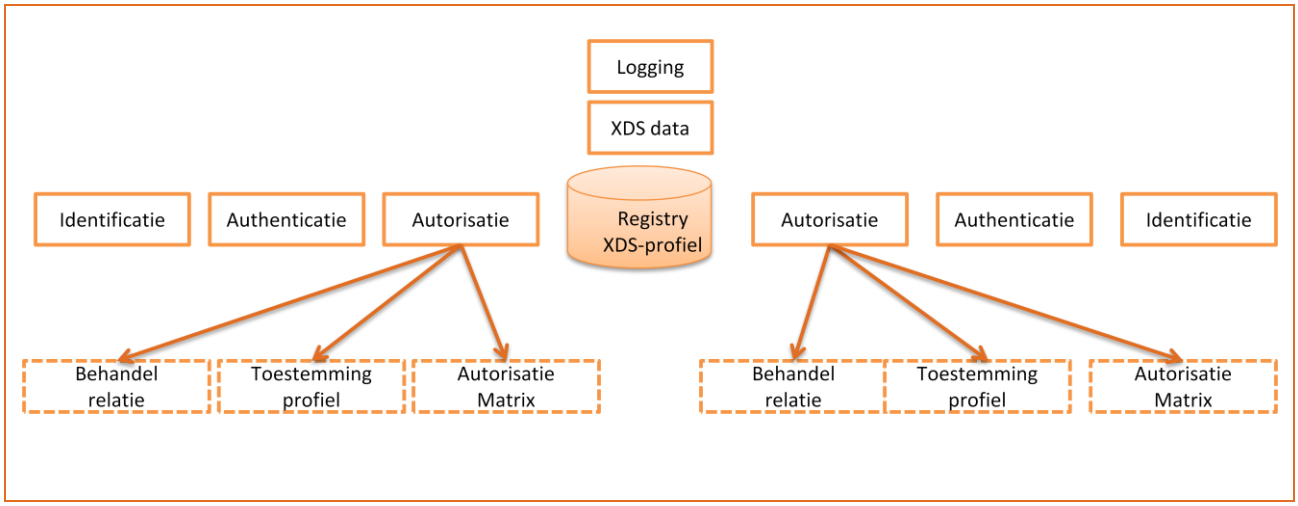
4.1. Inleiding

Patiëntgegevens zijn zeer privacygevoelig. Het is daarom van groot belang dat de toegang tot patiëntgegevens uitsluitend is voorbehouden aan bevoegde zorgaanbieders en de patiënt.

4.2. De toegangsmodel

De toegangsketen heeft betrekking op de toegang van zorgaanbieders tot gegevens in het affinity Domain (XDS-netwerk). Vanuit het perspectief van de zorgaanbieder bestaat de toegangsketen uit vier elementen:

1. Identificatie: identificatie is het startpunt van iedere handeling via de XDS-netwerk. De vervolgstappen in de toegangsketen kunnen zonder identificatie niet worden gezet.
2. Authenticatie: als de identiteit is vastgesteld dient deze te worden geverifieerd. Anders gezegd dient de zorgaanbieder te bewijzen dat hij is wie hij zegt te zijn. Deze tweede stap wordt ook wel aangeduid als 'authenticatie'.
3. Autorisatie: nadat identificatie en authenticatie hebben plaatsgevonden, wordt het autorisatieproces doorlopen. Autorisatie heeft betrekking op de vraag welke gegevens de zorgaanbieder mag inzien en welke gebruikshandelingen hij mag verrichten. Hiervoor is een behandelrelatie, als voorwaarde van de autorisatie, noodzakelijk.
4. Logging: het vierde element van de toegangsketen betreft de registratie van de toegang en het gebruik van patiëntgegevens. Dit element wordt ook wel aangeduid als 'auditlogging'. Door middel van logging kan worden gecontroleerd of inzage rechtmatig heeft plaatsgevonden.



figuur 1. Toegangsmodel

Dit document gaat over het toestemmingsprofiel dat onderdeel uitmaakt van de autorisatie. De toestemming van de patiënt kan vastgelegd worden in een toestemmingsprofiel. Dit profiel heet BPPC-profiel. Dit document gaat niet verder in op identificatie en authenticatie. In dit document

worden daarom ook geen keuzes gemaakt over de wijze van de identificatie en authenticatie. Onderstaande paragraaf over identificatie en authenticatie is toegevoegd ter informatie.

4.3. Identificatie en authenticatie

Identificatie en authenticatie vindt bij voorkeur plaats aan de hand van landelijke identificatiemiddelen. Omdat niet elke zorginstelling en ook niet elke beroepsgroep toegang heeft tot UZI middelen zijn hieronder meerdere mogelijkheden benoemd die de identificatie kunnen waarborgen.

1. UZI passen
2. Lokale passen
3. User identificatie en wachtwoord

Pas-authenticatie is sterker is dan username/password verificatie. Pas authenticatie geeft een hoger betrouwbaarheidsniveau en geniet de voorkeur. Het is van belang dat de identificatiemiddelen aansluiten of gekoppeld kunnen worden aan de identificatiemiddelen die genoemd staan in de richtlijn XDS-metadata. De richtlijn XDS-metadata beschrijft welke wordt meegestuurd bij digitale beeld- en verslaguitwisseling.

4.4. Autorisatie

Autorisatie is het verlenen van bevoegdheden tot het verrichten van bepaalde handelingen. Binnen de toegangsketen, zie figuur 2, heeft autorisatie betrekking op bevoegdheden van zorgaanbieders met betrekking tot index- en patiëntgegevens. Een voorbeeld van een dergelijke bevoegdheid is het kunnen aanmelden of opvragen van patiëntgegevens.

De autorisatie van een zorgaanbieder om patiëntgegevens te raadplegen is gebonden aan drie aspecten:

1. Behandelrelatie: de behandelrelatie van de patiënt en de zorgverlener.
2. Autorisatieprotocol: de informatie waartoe toegang wordt gevraagd.
3. Toestemming patiënt: het consent van de patiënt voor toegang, vastgelegd in BPPC-documenten en registries (in Nederlands: verwijsindex).

Behandelrelatie

De toetsing van de behandelrelatie staat beschreven in de gedragscode ‘Elektronische Gegevensuitwisseling in de Zorg’. De volgende paragraaf is één op één overgenomen uit de gedragscode.

Art. 8 vastlegging en toetsing behandelrelatie:

De Verantwoordelijke draagt zorg voor de instandhouding van technische voorzieningen waarmee de Behandelrelatie tussen de Dossierraadpleger en de Betrokkene kan worden vastgesteld. Dit geschiedt, in volgorde van voorkeur, door middel van:

a. voorafgaande toetsing aan de hand van een registratie van de Behandelrelatie door de Betrokkene met behulp van een digitale handtekening, of;
b. voorafgaande afleiding aan de hand van een registratie van de Behandelrelatie door de Dossierraadpleger persoonlijk met behulp van een digitale handtekening, of;
c. voorafgaande afleiding van de Behandelrelatie aan de hand van feitelijke omstandigheden.

Voorafgaande afleiding van de Behandelrelatie als bedoeld onder sub b en sub c vindt altijd plaats in combinatie met een melding achteraf. Deze melding geschiedt op een (of beide) van de volgende manieren:

- een notificatie aan de Betrokkene, bijvoorbeeld via e-mail of SMS;

- een verslag aan de Brondossierhouder van de raadplegingen die hebben plaatsgevonden ('snuffelverslag').
- De registratie of afleiding van een Behandelrelatie als bedoeld in dit artikel is ten hoogste geldig voor de duur van één jaar, tenzij anderszins duidelijk is wat de duur van de Behandelrelatie is.

De vastlegging en toetsing van de behandelrelatie is de verantwoordelijkheid van de zorgverlener. De toetsing van de behandelrelatie is geen onderdeel van het BPPC-profiel.

Toegang tot de gegevens kan alleen als er sprake is van een behandelrelatie. Er zijn ook situaties waarbij de zorgverlener geen patiëntcontact heeft of waarbij vanwege efficiency redenen de zorgprocessen anders zijn ingericht. Hieronder staan een paar voorbeelden van dergelijke zorgprocessen:

1. Doorverwijzing: patiënt gaat van instelling A over naar instelling B; patiënt moet toestemming geven dat relevante informatie uit zijn medisch dossier wordt doorgestuurd.
2. Intercollegiaal consult: specialist vraagt advies bij een collega in andere instelling.
3. Second opinion: patiënt vraagt advies aan andere zorgverlener.
4. Ketenzorg: meerdere zorgverleners zijn betrokken bij de behandeling van een patiënt.
5. Multidisciplinair overleg: er zijn meerdere zorgverleners betrokken bij de behandeling van de patiënt, echter niet elke zorgverlener heeft patiëntcontact.

Deze zorgprocessen zijn samen te vatten in de volgende twee situaties, waarbij in veel gevallen de naam van de zorgverlener niet op voorhand bekend is:

<u>Hoofdbehandelaar betrekt medebehandelaars bij de zorg</u>
Er is een behandelrelatie. De hoofdbehandelaar moet toestemming van de patient vragen voor het inzetten van mede-behandelaren. Het delen van patiëntinformatie is onderdeel van deze toestemming.

<u>Medebehandelaar betrekken derde partijen bij de zorg</u>
Als een mede-behandelaar een derde partij betrekt in het zorgproces zijn er twee opvattingen in Nederland:

1. deze situatie valt onder de definitie van de behandelrelatie;
2. de zorgverlener moet terug naar de patiënt om toestemming te vragen.

Een voorbeeld:
De patiënt wordt normaliter behandeld door de poortspecialisten. Nader onderzoek van medische gegevens kan uitgevoerd door specialismen (laboratoria, pathologie), die geen klantcontact hebben. Deze specialisten kunnen dan ook geen toestemming vragen aan de patiënt. Toch zijn er situaties waarbij de radiologen, laboranten en pathologen second opinions vragen aan experts die buiten de organisatie of buiten het affinity domain werken.

In deze situatie is een discrepantie tussen wettelijke kaders en werkbare zorgprocessen. In dit document wordt deze discrepantie niet opgelost.

Autorisatieprotocol
Wanneer identificatie en authenticatie hebben plaatsgevonden en een behandelrelatie is vastgesteld, staat vast dat de beroepsbeoefenaar bevoegd is de gegevens in XDS-netwerken te raadplegen. Dit betekent echter niet dat hij toegang krijgt tot alle beschikbare gegevens van de patiënt. De raadpleging moet noodzakelijk zijn voor de behandeling van de patiënt. Om vast te

stellen wat de zorginhoudelijke rol van de beroepsbeoefenaar is, wordt gebruik gemaakt van zogenaamde BIG-rolcodes of kwaliteitregisters.

In een autorisatieprotocol wordt voor ieder type beroepsbeoefenaar aan de hand van de BIG-rolcodes vastgelegd welke gebruikshandelingen hij mag verrichten. Welke beroepsbeoefenaar toegang krijgt, wordt voor iedere zorgtoepassing afzonderlijk bepaald door een autorisatiecommissie waarin relevante beroepsgroepen en belangenorganisaties zijn vertegenwoordigd. Een voorbeeld: huisartswaarneemgegevens zijn uitsluitend toegankelijk voor waarnemende huisartsen en het elektronisch medicatiedossier kan alleen worden geraadpleegd door huisartsen, apotheekhoudende artsen, (ziekenhuis)apothekers en medisch specialisten.

Landelijke autorisatieprotocollen voor XDS-registries voor medisch specialisten zijn er nog niet in Nederland. Desalniettemin zijn er al wel regionale XDS-netwerken voor digitale beelduitwisseling geïmplementeerd. De ervaring uit heeft geleerd dat het opstellen van deze autorisatieprotocollen meerjarige trajecten zijn.

Voor een overzichtelijk gebied als medicatiegegevens (Mg) en HuisartsWaarneemGegevens (HWG) is het mogelijk een matrix op te stellen. Voor een bredere toepassing wordt het al snel een probleem. Daarnaast is de uitwerking van autorisatie niet alleen volledig technisch van aard. De bestaande processen gebruiken ook geen technische oplossing, maar doen een beroep op de eed en de beroepscode.

Ondanks het feit dat er geen instantie is in Nederland die de autorisatieprotocollen heeft geregeld zullen er toch oplossingen gevonden moeten worden. Hieronder staan pragmatische opties om goede zorg te kunnen verlenen.

1. Volgen van landelijk autorisatiebeleid (nader te bepalen).
2. Alle medisch specialisten mogen alle documenten inzien binnen het affinity domein.
3. Alle zorgverleners mogen alle documenten inzien binnen het affinity domein.
4. Alle zorgverleners mogen alle documenten inzien met de affinity domeinen die aan elkaar gekoppeld zijn.
5. De specialisten mogen alleen de documenten inzien die geclassificeerd zijn voor de eigen beroepsgroep. Dit protocol werkt alleen bij second opinions binnen dezelfde medische beroepsgroep. Als voorbeeld de radiologen mogen alleen de radiologische beelden en verslagen inzien.

4.5. Toestemming patiënt

De patiënt moet toestemming verlenen aan de zorgverlener(s) om zijn medische gegevens te delen. IHE heeft een profiel gedefinieerd om de toestemming van de patiënt te uniformeren. Dit profiel heet BPPC-profiel. BPPC staat voor Basic Patient Privacy Consent. Binnen het BPPC-profiel kunnen verschillende ‘policies’ gedefinieerd worden. Een policy zou kunnen zijn: ‘mijn medische gegevens mogen alleen gedeeld worden met ziekenhuizen in provincie Noord Holland’. De patiënt kan kiezen uit voorgedefinieerde ‘policies’. De ‘policies’ staan in hoofdstuk 5.

Zodra een patiënt zijn toestemmingprofiel wijzigt, bijvoorbeeld van een uitdrukkelijke toestemming naar een generiek bezwaar, dan wordt het oude toestemmingsprofiel verwijderd of overruled. Dit gebeurt in XDS door de RPLC (replace) relatie tussen het nieuwe en oude profiel. Daarmee wordt het oude profiel effectief onzichtbaar en is het nieuwe leidend geworden.

4.6. Logging

Telkens wanneer patiëntgegevens worden aangemeld of opgevraagd, worden de volgende ‘log’gegevens bijgehouden:

- het type transactie (opvraging, aanmelding, ...);
- identiteit van de patiënt;
- het identificatienummer van de zorgverlener;

- het soort gegevens dat is verwerkt;
- de datum en het tijdstip van de verwerking.

Logging vindt zowel plaats in de centrale loggingfaciliteit als decentraal op de systemen van zorgaanbieders. 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 zorgaanbieder of beroepsbeoefenaar, of tot de beheerder of eigenaar van het XDS-netwerk.

De beheerder van de registry bewaakt het correct gebruik van een elektronische informatievoorziening. Onderdeel hiervan is het uitvoeren van een analyse van de loggegevens, zowel realtime als achteraf. Dit wordt ook wel aangeduid als 'monitoring', de uitwerking hiervan is nader omschreven in het convenant digitale beeld- en verslaguitwisseling. Op basis van de signaleringen die voortkomen uit de monitoring, verricht de beheerder nader onderzoek om vast te stellen of sprake zou kunnen zijn van misbruik. Zonodig treedt de beheerder hierover in contact met de betreffende zorgaanbieder.

H-5 Toepassing BPPC-profiel

BPPC staat voor het Basic Patient Privacy Consent. BPPC is een IHE-profiel om de toestemming van de patiënt vast te leggen voor een XDS-affinity domain. BPPC-policies, ook wel toestemmingsprofielen genoemd, zijn geschreven teksten. Een patiënt geeft uitdrukkelijke toestemming voor een of meerdere toestemmingsprofielen of maakt generiek bezwaar bij de zorgverlener. De beschrijving van de policies moet zodanig zijn dat patiënten, ICT'ers en zorgverleners het toestemmingsprofiel begrijpen. Deze policies:

- leggen het gekozen privacy beleid met betrekking tot de patiënttoestemming vast;
- faciliteren de handhaving en controle van het privacybeleid.

Om te zorgen dat elk regionaal netwerk op vergelijkbare wijze de toestemming van de patiënt toepast en om te zorgen dat de regionale netwerken op dezelfde wijze de toestemming van de patiënt als het Landelijk Schakelpunt implementeert, is het noodzakelijk om dezelfde afspraken met elkaar te maken.

5.1. Procedurele impact

In deze en volgende paragrafen wordt de casus van 'radiologische beelden' beschreven. De procedurele impact is generiek van aard, er is dus ook een soortgelijke impact bij cardiologie of bij laboratoria.

Het proces op de afdeling radiologie om de toestemming van de patiënt in te bedden zal veranderen. Als zorgverleners digitale beelden en verslagen op CD's of DVD's met de patiënt mee geven ten behoeve van de patiënt behandeling in een andere zorginstelling is sprake van een impliciete toestemming van de patiënt. Zodra beelden en verslagen digitaal worden uitgewisseld is expliciete toestemming van de patiënt vereist. Deze paragraaf beschrijft de handelingen die nodig zijn om de toestemming van de patiënt in te richten. Onderscheid wordt gemaakt voor de handeling bij:

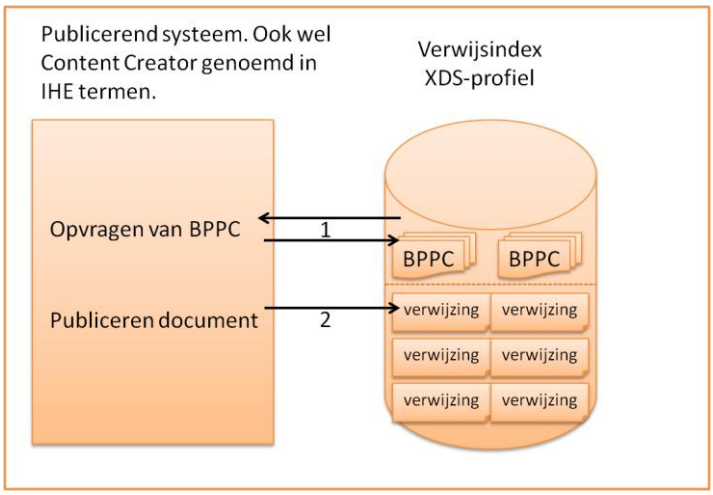
- publiceren van digitale beelden en verslagen;
- opvragen van digitale beelden en verslagen.

Publiceren van digitale beelden en verslagen

Iedere deelnemende patiënt wordt vooraf geïnformeerd. De wijze waarop dit gebeurt, verschilt per instelling. Het moment om toestemming te vragen kan procedureel op drie momenten worden gerealiseerd:

1. Bij de intakebalie in het ziekenhuis. Het ziekenhuis is dan in staat om generiek voor alle medische domeinen toestemming te vragen en dit te borgen in de administraties.
2. Bij de intakebalie of de behandelend arts van de betreffende medische discipline, voorafgaand aan de behandeling. Bijvoorbeeld bij de afdeling Radiologie. De betreffende afdeling is dan in staat om de toestemming van de patiënt te vragen en dit te borgen in zijn systemen.
3. Na uitvoering van het onderzoek, zodra de patiënt wordt geïnformeerd over de uitslag.

Nb. Overigens is optie drie procedureel niet werkbaar. De uitslag kan namelijk ook via de post worden medegedeeld.



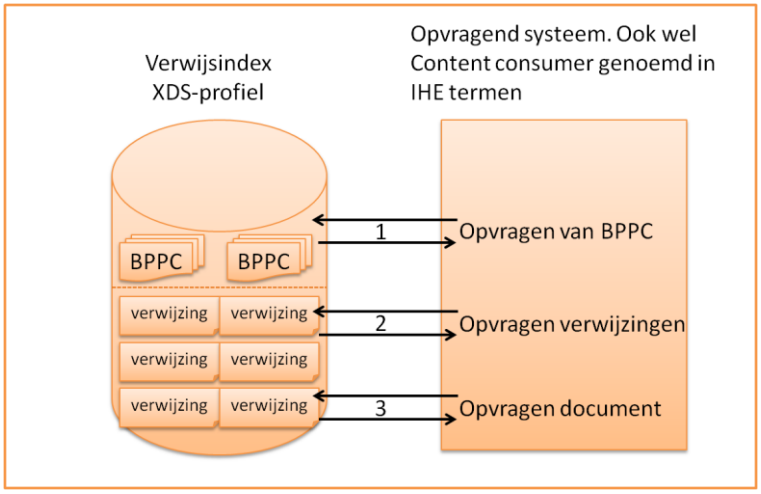
figuur 2. Proces om medische gegevens te publiceren.

De zorgverlener wil in de systemen zichtbaar hebben of en zo ja welke toestemmingprofielen zijn patiënt heeft. Het proces verloopt als volgt:

1. De XIS zal in de registry de toestemmingsdocument(en) met policies opvragen[2]. Dit opvragende systeem heeft twee mogelijke opties:
    a. Er is geen toestemmingsprofiel. De zorgverlener wordt geïnformeerd dat deze patiënt nog een toestemmingsverklaring moet maken.
    b. Het toestemmingsprofiel is aanwezig.
2. Zodra de toestemming van de patiënt is geregeld kunnen documenten, eigenlijk verwijzingen naar documenten, aangeboden worden aan de registry.

Opvragen van digitale beelden en verslagen

Bij het opvragen van documenten is altijd sprake van een behandelrelatie.



figuur 3. Opvragen van documenten.

Zodra een zorgverlener informatie wil ophalen zal hij in zijn systeem moeten bevestigen dat hij een behandelrelatie heeft. Om informatie uit de registry te krijgen worden de volgende systematische processtappen doorlopen.

1. Het opvragend systeem bevraagt de XDS-registry. Er wordt gekeken of de metadata van het document policy-id's bevat die toegang mogelijk maken of verbieden.

[2] Technisch gesproken kun je geen document opvragen in de registry. In essentie is het voldoende de metadata van het BPPC document op te vragen in de registry (opvragen van documenten gebeurt altijd uit een repository).

2. Indien de zorgverlener de juiste rechten heeft, kan het systeem een lijst met de verwijzingen tonen.
3. Op basis van de lijst met verwijzingen kan de zorgverlener het relevante document opvragen.

5.2. Uitgangspunten BPPC-profiel

Voordat privacy policies gedefinieerd kunnen worden is het noodzakelijk om de uitgangspunten te benoemen. Dit betreft de algemene informatie die van toepassing is bij het gebruik van BPPC-profielen. De volgende uitgangspunten zijn van toepassing:

- De policies die worden opgesteld, moeten technisch ondersteund kunnen worden door de informatievelden. Dit kunnen velden zijn uit de dataset 'XDS-metadata'.
- Er worden geen verwijzingen opgenomen in de registry zonder toestemming van de patiënt.
- Voor XDS-netwerken geldt dat niets gepubliceerd mag worden zonder uitdrukkelijke toestemming van de patiënt.

Let op: het afdwingen/toetsen van de policies waarover toestemming is gegeven (policy enforcement) door de patiënt, wordt uitgevoerd door het opvragende systeem (XDS consumer). Dat wil zeggen, het opvragende systeem moet borgen dat de toestemming van de patiënt juist wordt nageleefd. Het is raadzaam om het policy enforcement ook bij de registry te beleggen.

5.3. Mogelijkheden met BPPC-profiel

Het BPPC-profiel heeft op dit moment de onderstaande mogelijkheden. Het is zeer goed mogelijk dat er meer mogelijkheden worden ontwikkeld in de toekomst. Bij het opstellen van de BPPC-profielen gaan we uit van de mogelijkheden die begin 2012 in de IHE-technical frameworks[3] staan vermeld.

In de eerste plaats moet er een algemeen overkoepelend document zijn die de mogelijke toestemmingen en de reikwijdte van het affinity domain beschrijft. Dit document wordt niet op de registry aangemeld, maar is onderdeel van de informatieplicht van de zorgverlener aan de patiënt.

In de tabel op de volgende pagina staan de mogelijke functionele toepassingen van het BPPC-profiel en de adviezen die gemaakt zijn door experts uit de adviesgroep. De adviezen van de experts staan in de tweede kolom. In de derde kolom staat, waar nodig, de onderbouwing van de advies. In de vierde kolom staat een nadere toelichting indien dit relevant is.

'Ja' betekent: deze mogelijkheid is nodig voor de Nederlandse situatie.
'Nee' betekent: deze mogelijkheid is niet nodig of niet haalbaar voor de Nederlandse situatie.

[3] IHE IT Infrastructure Technical Framework, volume 1; integration profiles, blz. 153.

Mogelijke toepassingen die met het BPPC-profiel geregeld kunnen worden:

Mogelijkheid	Advies werkgroep	Argumentatie	Toelichting
Uitdrukkelijke toestemming voor klinisch gebruik	Ja	Uitdrukkelijke toestemming is conform de adviezen van het CBP.	
Generiek bezwaar voor klinisch gebruik	Ja	Dit is wettelijk noodzakelijk. Maar let op: Het bezwaar mag niet met een BPPC-policy worden geregistreerd in de XDS-registry.	Indien een patiënt een generiek bezwaar heeft dan moet het generiek bezwaar in het XIS worden geregistreerd.
Generiek bezwaar voor gegevensuitwisseling buiten lokaal (local events) gebruik	Nee	Nee, je hebt sowieso toestemming nodig. Daarnaast is het begrip local events niet duidelijk. Dit kan betekenen: het zorgpad, de behandeling, het ziekenhuis of het affinity domain.	Idem als hierboven.
Inzage toestaan voor noodsituaties (breaking glass)	Ja	Dit is wenselijk bij levensbedreigende en onvoorziene situaties.	
Inzage toestaan voor specifiek geïdentificeerde documenten voor noodsituaties	Nee	Er zijn geen landelijke criteria die de inhoud van de documenten bepalen. Derhalve kunnen de documenten ook niet eenduidig benoemd worden. Daarnaast is dit zorginhoudelijk, functioneel en technisch zeer complex om te realiseren	Landelijke autorisatieprofielen zullen bepalen welke documenten door welke zorgverleners opgevraagd kunnen worden.
Additioneel, inzage toestaan voor onderzoeksdoeleinden	Nee	Er zijn geen landelijke criteria die “onderzoeksdoeleinden” definiëren. Daarnaast hebben wetenschappelijke medische domeinen eigen wetenschappelijke databases.	
Additioneel, inzage toestaan voor specifieke documenten onderzoeksdoeleinden	Nee	Er zijn geen landelijke criteria die de inhoud van de documenten bepalen en er zijn geen landelijke criteria die “onderzoeksdoeleinden” definiëren.	

Alleen toestaan voor functionele rollen (bijvoorbeeld gezondheidszorg of ziekenhuizen)	Nee	Let op: dit wordt geregeld in de autorisatieprotocollen en de toegang tot de systemen (role based access). Dit wordt dus niet geregeld in de BPPC-policies.	Landelijke autorisatieprofielen zullen bepalen welke documenten door welke zorgverleners opgevraagd kunnen worden
Inzage alleen toestaan voor structurele rollen (bijvoorbeeld organisatie X of alle specialisten uit een beroepsgroep.	Nee	Let op: dit wordt geregeld in de autorisatieprotocollen en de toegang tot de systemen (role based access). Dit wordt dus niet geregeld in de BPPC-policies.	Landelijke autorisatieprofielen zullen bepalen welke documenten door welke zorgverleners opgevraagd kunnen worden
Kunnen er meerdere policies worden toegestaan per document.	Ja	Dit is per definitie het geval. Bij het opzetten van een affinity domain is er 1 algemeen policy voor het affinity domain + een policy per registry.	
Is het toegestaan dat de patiënt de toestemming verandert, van uitdrukkelijke toestemming naar generiek bezwaar, of andersom.	Ja	Dit is een wettelijke vereiste.	
Is er een policy nodig die zegt: als een zorgverlener een document opvraagt en van nieuwe informatie voorziet, dat het document daarna niet opnieuw gepubliceerd mag worden.	Nee	Dit valt niet onder BPPC-profielen maar onder publicatie beleid. Zodra een zorgverlener een document opvraagt en aan dit document nieuwe informatie toevoegt. Dan is er sprake van een nieuw brondossier, waarvoor een nieuw policybeleid zal moeten gelden of waarbij een bestaand policybeleid van toepassing kan zijn.	
Inzage toestaan in andere domeinen	Ja	Domeinen zullen organisch groeien. De patiënt en ook de zorgverlener ziet niet in zijn systeem waar de informatie vandaan komt.	Het is hierbij wel van belang dat de toestemming wordt gevraagd aan de patiënt en dat de patiënt hierover wordt geïnformeerd.

Uitdrukkelijke toestemming voor een Personal Health Record naar keuze.	Nee	Nog niet. Het is goed mogelijk dat een affinity domain gaat samenwerken met een specifiek Personal Health Record. Zodra dit relevant wordt zal hiervoor een policy worden ontwikkeld.	
Policies definiëren per confidentiality code (normal, restricted, very restricted).	Ja	Confidentiality codes zijn niet nader geclassificeerd. De arts/patiënt bepaalt zelf of een hoger confidentiality code van toepassing is.	Alle documenten krijgen standaard de optie “normaal”. Een hogere classificatie bepaalt de zorgverlener.
Worden documenten die in de registry staan met een onbekende documentcode zichtbaar bij het bevragen van de registry door de zorgverlener.	Nee	Dit valt niet onder BPPC-policies. Alle documentcodes die worden ontwikkeld moeten eerst worden opgenomen in de dataset XDS. Onbekende policies worden niet getoetst omdat er geen programmatuur voor is ontwikkeld.	
Een patiënt kan toestemming geven voor publicatie voor de behandelende zorgverlener maar ook voor andere zorgverleners. Bijvoorbeeld voor alle zorgverleners in het ziekenhuis of alle behandelaars die bij het Multi-disciplinair overleg zijn.	Ja	Volgens de elektronische gedragscode in de zorg kan de patiënt toestemming geven per brondossierhouder.	
Is het mogelijk om uitdrukkelijke toestemming vast te leggen in een document.	Ja	De toestemming wordt vastgelegd in een document dat wordt geregistreerd op de XDS-registry.	Bij het Landelijk SchakelPunt wordt de uitdrukkelijke toestemming vastgelegd in de applicatie van de zorgverlener.
Lokale rolcodes van ziekenhuizen vastleggen in policies.	Nee	Ziekenhuizen hebben vaak eigen rolcodes. De richtlijn XDS-metadata kent o.a. BIG-rolcodes. De ziekenhuizen moeten hun eigen rolcodes ‘mappen’ met de BIG rolcodes.	

De zorgverlener kan de toestemmingsverklaringen op zijn beeldscherm tonen aan de patiënt.	nee	Dit betreft een keuze die los staat van de toestemmingprofielen.	Landelijk geldt hier geen richtlijn voor, het betreft een keuze per leverancier.
Een tijdsduur waarbij de toestemming van de patiënt geldig is.	Ja	De tijdsduur kan per instelling worden bepaald. Advies 5 jaar, deze keuze is gebaseerd op redelijkheid. let op: hierbij geldt de volgende impact. Indien de tijd van de policy is verstreken is er geen rechtsgeldige grond om documenten op de registry te hebben staan. Alle documenten van deze patiënt moeten dan op non-actief worden gezet zodat deze niet benaderbaar zijn. Ook niet in geval van breaking glass. Ook al waren de documenten zelf slechts een week oud. Advies: goede voorlichting aan patiënt is noodzakelijk.	Omdat een toestemmingsprofiel een levenslange geldigheid heeft, wil niet zeggen dat de gegevens levenslang kunnen worden bevraagd. De gegevens worden 15 jaar bewaard Bovendien heeft de patiënt conform de wet altijd het recht de toestemming in te trekken.

Het BBPC-profiel kan niet alle toestemmingen van de patiënt realiseren. De volgende situaties zijn niet mogelijk met het BPPC-pofiel:

1. Patiënt identificeert individuele zorgverleners die toestemming krijgen.
2. Patiënt identificeert individuele zorgverleners die uitgesloten worden.
3. Elke opvraging van een document wordt geautoriseerd door de patiënt.
4. Notificatie aan de zorgverleners die een document gebruiken om de toestemming van de patiënt te herroepen.
5. Terugtrekken van documenten die zijn gebruikt waarbij in een later stadium de toestemming van de patiënt wordt herroepen. Het betekent feitelijk dat je niet kunt wissen uit geheugen van mensen of machines als er ooit inzage is geweest.

5.4. Functionele eisen

Om te komen tot de juiste policies die met het BPPC-profiel geïmplementeerd kunnen worden, moet ook gekeken worden naar de landelijke, regionale en lokale eisen en wensen van de gebruikers. Er zijn functionele eisen op drie niveaus: landelijk, regionaal en lokaal.

Landelijke eisen

De eisen en wensen zijn:

- Toestemming wordt gegeven voorafgaand aan de publicatie van medische gegevens.
- Bij het geven van de toestemming wordt impliciet toestemming gegeven voor het bevragen van de documenten mits er een behandelrelatie bestaat.
- Uitdrukkelijke toestemming wordt afgebakend door regionale begrenzing.

Regionale eisen

Uitwisseling van documenten tussen regionale en categorale (netwerk per medische categorie, bijvoorbeeld MammoXL) netwerken is mogelijk.

Lokale eisen

Lokale toestemmingsvormen die in een eerder stadium zijn gesteld:

1. De patiënt geeft toestemming voor opname van zijn informatie in de verwijsindex ten behoeve van raadpleging uit of via deze index.
2. De patiënt geeft toestemming voor opname van zijn informatie in de verwijsindex, maar wil per geval van raadpleging toestemming kunnen verlenen (deze eis is eerder in dit document beschreven als onmogelijk, een alternatief is het gebruik van de breaking glass policy).
3. De patiënt bepaalt per onderzoek of de onderzoeksinformatie wel of niet in de verwijsindex wordt opgenomen.
4. De patiënt wil niet dat informatie in de verwijsindex wordt opgenomen.

5.5. Landelijke policies

Elk affinity domain moet een document hebben die beschrijft wat de reikwijdte is van het affinity domain. Dit document is nodig zodat zorgverleners aan de patiënt kunnen uitleggen welke informatie en tussen welke zorgverleners uitgewisseld wordt. Vervolgens heeft elke affinity domain een aantal BPPC-policies die de toestemming van de patiënt definieert. De BPPC-policies worden vastgesteld per affinity domain. Het is van cruciaal belang dat elk affinity domain dezelfde policies gebruikt als de andere affinity domains in Nederland.

Op basis van de mogelijkheden van het BPPC-profiel, de onmogelijkheden van het BPPC-profiel, de landelijke eisen, de regionale eisen en de lokale eisen zijn de volgende policies opgesteld om te komen tot een landelijke implementatie richtlijn. Dit zijn dus de policies die elk affinity domain moet ondersteunen om interoperabiliteit tussen en binnen de regio's mogelijk te maken.

Policy	Omschrijving	Toelichting	XDS – LSP relatie
1	Uitdrukkelijk toestemming voor het affinity domain	De patiënt geeft toestemming dat de brondossierhouder mag publiceren en dat alle zorgverleners –mits geautoriseerd- van het affinity domain gegevens mag opvragen. NB. Een extra parameter in deze toestemming betreft de tijdsduur zodat de toestemming niet levenslang vast staat. NB. Een extra parameter in deze toestemming betreft de confidentiality code. Dit kan zijn normal, restricted of very restricted.	Deze nadrukkelijke toestemming komt enigszins overeen met de regionale toestemming die geldig is bij het LSP. Echter het LSP kent geen aparte parameters voor tijd en confidentialiteit.
2	Uitdrukkelijk toestemming voor Nederland	De patiënt geeft toestemming dat de brondossierhouder mag publiceren en dat alle zorgverleners –mits geautoriseerd- binnen Nederland gegevens mag opvragen. LET OP: technisch gezien is dit niet mogelijk. Er zijn namelijk nog geen regionale netwerken aan elkaar gekoppeld.	Deze nadrukkelijke toestemming komt overeen met het wijzigingsvoorstel 'regionale overruling' die mogelijk geldig wordt bij het LSP.

		De patiënt moet wel goed geïnformeerd worden. NB. Een extra parameter in deze toestemming betreft de tijdsduur zodat de toestemming niet levenslang vast staat. NB. Een extra parameter in deze toestemming betreft de confidentiality code. Dit kan zijn Normal, restricted of very restricted.	
3	Breaking glass voor noodsituaties	De patiënt geeft toestemming dat de brondossierhouder mag publiceren, maar dat bij het opvragen van de gegevens door een zorgverlener een extra handeling wordt verricht om de gegevens in te zien. Breaking glass policy geldt voor alle actieve documenten. Dus niet de documenten die op non-actief zijn gezet waarbij de toestemming is verlopen of is ingetrokken. Hiervoor is dus geen rechtsgeldige grond. Er is geen differentiatie naar bijvoorbeeld regio of confidentiality code. De zorgverlener is verantwoordelijk voor de aantoonbaarheid van de breaking glass procedure.	Deze functie is niet ontworpen op het LSP.
4	Generiek bezwaar	Met dien verstande dat dit policy niet in de registry wordt geregistreerd maar in het XIS van de zorgaanbieder.	Deze functie is ook op het LSP van toepassing.

Als een patiënt toestemming geeft voor informatieuitwisseling, dan kan voor elk bericht een ander 'conficentiality code' (vertrouwelijkheidscode) toegekend worden. De afspraken die gelden bij de confidentiality codes zijn één op één afgeleid van de omschrijvingen van de HL7 standaard.

Code	HL7 definitie	Interpretatie t.b.v. BPPC-toepassingen
Normal	Privacy metadata indicating that the information is typical, non-stigmatizing health information, which presents typical risk of harm if disclosed without authorization.	Algemene patiënt gegevens
Restricted	Privacy metadata indicating highly sensitive, potentially stigmatizing information, which presents a high risk to the information subject if disclosed without authorization. May be preempted by jurisdictional law, e.g., for public health reporting or emergency treatment	Medische gegevens
Very restricted	Very restricted access as declared by the Privacy Officer of the record holder	Gegevens waarbij de patient en/of zorgverlener bepalen dat de betreffende informatie very restricted is.

5.6. Object Identifier

Elk BPPC-policy heeft een unieke code nodig. Deze codes worden met behulp van Object Identifiers (OID) geregistreerd. De lijst met Object Identifiers die bij deze profielen horen zijn:

Nr	OID	Omschrijving
1	2.16.840.1.113883.2.4.3.11.24	BPPC-policies
2	2.16.840.1.113883.2.4.3.11.24.1	BPPC-policy 1: "Uitdrukkelijk toestemming voor het affinity domain"
3	2.16.840.1.113883.2.4.3.11.24.1.1	BPPC-policy 1: "Uitdrukkelijk toestemming voor het affinity domain" Bevolkingsonderzoek Borstkanker Nederland
4	2.16.840.1.113883.2.4.3.11.24.1.2	BPPC-policy 1: "Uitdrukkelijk toestemming voor het affinity domain" EZDA Amsterdam
5	2.16.840.1.113883.2.4.3.11.24.1.3	BPPC-policy 1: "Uitdrukkelijk toestemming voor het affinity domain" Rijnmondnet Rotterdam
6	2.16.840.1.113883.2.4.3.11.24.1.4	BPPC-policy 1: "Uitdrukkelijk toestemming voor het affinity domain" St. Gerrit Friesland
7	2.16.840.1.113883.2.4.3.11.24.1.5	BPPC-policy 1: "Uitdrukkelijk toestemming voor het affinity domain" St. Gerrit Groningen
8	2.16.840.1.113883.2.4.3.11.24.1.6	BPPC-policy 1: "Uitdrukkelijk toestemming voor het affinity domain" Zorgring Noord Holland
9	2.16.840.1.113883.2.4.3.11.24.1.7	BPPC-policy 1: "Uitdrukkelijk toestemming voor het affinity domain" Zorgsaam Zeeuws Vlaanderen
10	2.16.840.1.113883.2.4.3.11.24.1.8	BPPC-policy 1: "Uitdrukkelijk toestemming voor het affinity domain" Regio Breda
11	2.16.840.1.113883.2.4.3.11.24.1.9	BPPC-policy 1: "Uitdrukkelijk toestemming voor het affinity domain" Regio Eindhoven

12	2.16.840.1.113883.2.4.3.11.24.1.10	BPPC-policy 1: "Uitdrukkelijk toestemming voor het affinity domain" Sleutelnet Leiden
13	2.16.840.1.113883.2.4.3.11.24.2	BPPC-policy 2: "Uitdrukkelijk toestemming voor Nederland"
14	2.16.840.1.113883.2.4.3.11.24.3	BPPC-policy 3: "Breaking glass voor noodsituaties"
15	2.16.840.1.113883.2.4.3.11.24.4	BPPC-policy 4: "Generiek bezwaar"

Elke toestemmingsprofiel wordt centraal opgeslagen in de registry van het desbetreffende affinity domain. De redenen hiervoor zijn:

- technische haalbaarheid;
- juridisch betere situatie;
- duidelijkheid voor zorgverleners;
- een grote zorginstelling heeft vele systemen, een centrale voorziening is efficiënter. Dit geldt voor zowel de uitdrukkelijke toestemming als in de situatie van geen toestemming;
- breaking glass policy kan niet werken als de toestemming van de patient niet centraal is vastgelegd.

Als een patiënt **geen toestemming** heeft gegeven, wordt dit **niet** in de registry gepubliceerd, maar in het XIS.

Policies waar veel discussie over is geweest die uiteindelijk niet relevant of niet haalbaar zijn gebleken:

- Uitdrukkelijke toestemming per situatie. Indien een patiënt per behandeling en/of situatie (document/zorgpad) zijn toestemming wil geven dan zal dit een handmatige procedure moeten worden in de applicatie.
- Uitdrukkelijke toestemming voor PHR naar keuze. Op dit moment is het nog niet relevant. Zodra er vraag ontstaat naar dit toestemmingsprofiel, dan zal het ontwikkeld worden.
- Opvragen toegestaan. Volgens de regionale gedragscode is het opvragen van documenten impliciet geregeld zodra de patiënt toestemming heeft verleend én er sprake is van een behandelrelatie.

Een patiënt kan meerdere policies hebben in een affinity domain. Het kan dus voorkomen dat sommige policies tegenstrijdig zijn.

5.7. Vastlegging toestemmingsprofielen

De manier waarop de consent van de patiënt moet worden vastgelegd is wettelijk niet voorgeschreven. De wet schrijft wel voor dat:

- elke zorgverlener toestemming moet vragen aan de patiënt;
- de vastlegging aantoonbaar moet zijn voor controle doeleinden.

Er is dus geen duidelijk wettelijk kader over de vastlegging van de toestemmingsprofielen van de patiënt. De zorgverlener is gebaat bij een laagdrempelige oplossing en voor controledoeleinden is een zo goed mogelijke traceerbaarheid nodig. De achterliggende reden bij het opslaan van deze informatie is dat andere zorgverleners (en andere stakeholders zoals auditers) de toestemming van de patiënt moet kunnen zien en kunnen controleren.

In deze situatie is een frictie tussen wettelijke kaders en werkbare zorgprocessen. Hieronder staan een aantal mogelijke opties, in volgorde van wenselijkheid:

1. De (digitale) handtekening van de patiënt wordt gevraagd en (digitaal) opgeslagen.
2. De (digitale) handtekening van de arts wordt geplaatst en (digitaal) opgeslagen.
3. De zorgverlener plaatst een vinkje in zijn systeem. Tevens wordt de papieren kopie met handtekening van de patiënt in het dossier toegevoegd.
4. De zorgverlener plaatst een vinkje, waarbij logging plaatsvindt zodat achteraf de behandeling traceerbaar is. Bijvoorbeeld naar de afspraken in de agenda of de DBC declaratie.

H-6 Verklarende woordenlijst

Opt-in en Opt-out
Er is veel spraakverwarring over de definitie opt-in en opt-out. In IHE termen wordt met opt-in en opt-out bedoeld of de patiënt wel of geen uitdrukkelijke toestemming geeft. Juridisch gezien is dit anders. Vanuit juridisch oogpunt zijn opt-in en opt-out twee mechanismen die bepalen op welke wijze de toestemming van de patiënt vastgelegd moet worden.

In dit document wordt daarom, net als in de gedragscode Elektronische Gegevensuitwisseling in de Zorg, gesproken over 'uitdrukkelijke toestemming' als de patiënt toestemming heeft gegeven voor het delen van zijn gegevens en 'generiek bezwaar' als zijn gegevens niet gedeeld mogen worden.

Affinity Domain
Volgens IHE technical Framework: "An XDS Affinity Domain is a group of healthcare enterprises that have agreed to work together using a common set of policies and share a common infrastructure". Of in het Nederlands: een XDS-affinity domain is een groep van gezondheidsorganisaties die het delen van patiëntgegevens zijn overeengekomen binnen één infrastructuur en werken met een gezamenlijk beleid.

Brondossierhouder
Het begrip 'brondossierhouder' is niet nader gespecificeerd binnen juridische kaders. In de gedragscode Elektronische Gegevensuitwisseling in de Zorg is het begrip gedefinieerd als 'de instelling waarbinnen het dossier is gemaakt'. Dit kan bijvoorbeeld een huisartsenpost, apotheek, laboratorium, ziekenhuis of een radiotherapeutisch instituut zijn.

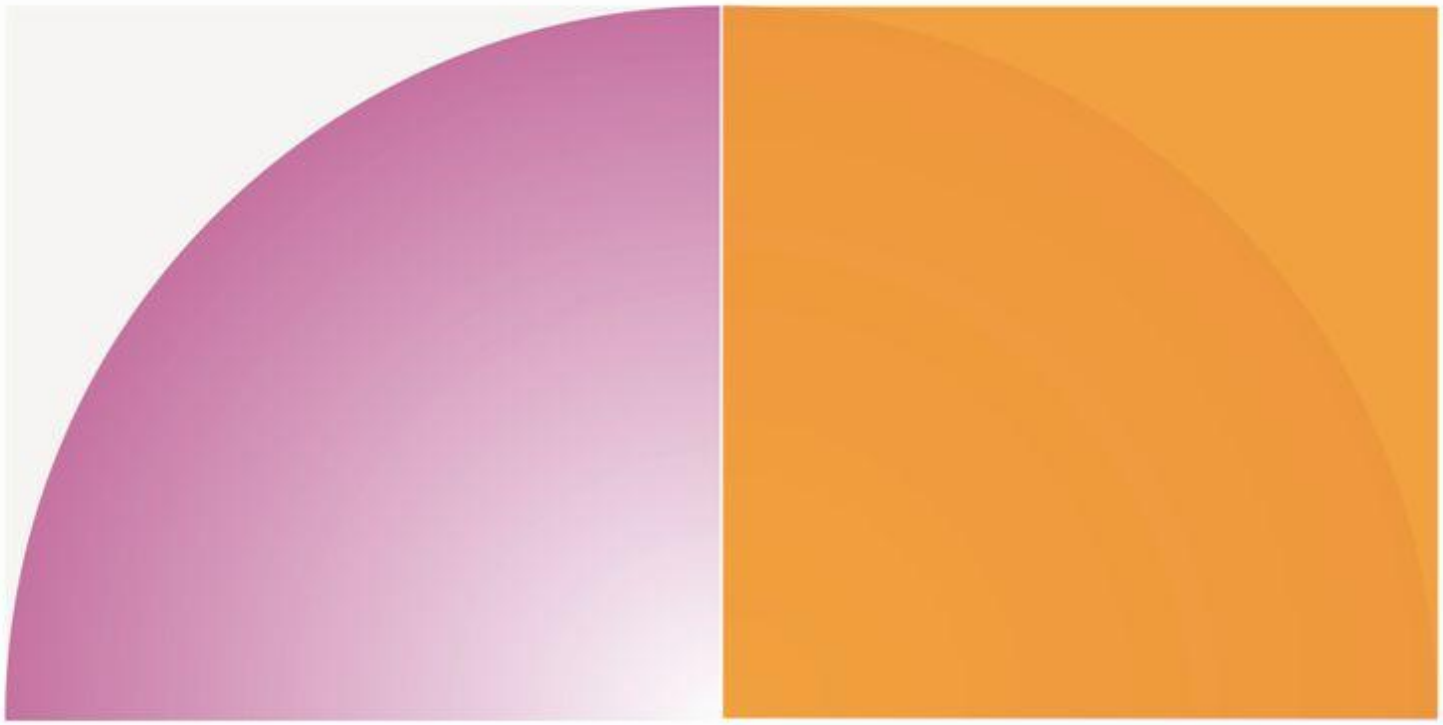
H-7 Tot slot

Dit document is tot stand gekomen in samenwerking met experts uit het veld. Deze experts hebben advies gegeven om te komen tot de juiste toestemmingsprofielen. Daarbij is een aantal documenten als uitgangspunt gehanteerd. Dit zijn:

- Elektronische gegevensuitwisseling in de zorg
- Convenant digitale beeld- en verslaguitwisseling
- Vertrouwensmodel infrastructuur voor zorgcommunicatie
- Inrichting uitdrukkelijke toestemming infrastructuur voor zorgcommunicatie
- Doorstartmodel infrastructuur voor zorgcommunicatie.

De experts die dit document en ook de toepassingsmogelijkheden hebben beoordeeld zijn:

Naam	Organisatie
Mark Sinke	Forcare
Robert-Jan Besselink	E.Novation
Evelien van den Broeke	E.Novation
Brian Sanderse	Amphia Ziekenhuis
Evert Sanders	NvvR
Nicky Hekster	IHE
Anton Ekker	Nictiz
Albert-Jan Spruyt	Nictiz
Beer Franken	Academisch Medisch Centrum
'Dennis Groen	Groen Juridische Diensten'
Arnout Engelen	Topicus
Jan Willem Schoemaker	Erasmus Medische Centrum
Jan van Kuyk	MedicalPHit
Margriet Miedema	Zorgring
Alexander van Duijn	Nictiz
Claartje Hülsmann	IHE Nederland



Nictiz
Postbus 19121
2500 CC Den Haag
Oude Middenweg 55
2491 AC Den Haag

T 070 - 317 34 50
info@nictiz.nl
www.nictiz.nl