Beatrijsgaarde 1
7329 BK Apeldoorn

+31 (0)6 13 60 75 30
r.noordhuis@RSONL.nl

Bijlages

Handreiking Interoperabiliteit op basis van IHE-XDS

15 november 2019
Versie: 1.0, Definitief

Inhoudsopgave

Auteurs

- Bennie Assink, ZorgNetOost
- Robert Breas, MedicalPHIT
- Jaap-Jan de Rooij, REN
- Jan Feenstra, MedicalPHIT
- Sjaak Gondelach, Trijn
- Walter de Haan, EZDA
- Dini Klaassen, RijnmondNet
- Leendert Nooitgedagt, Stichting Gerrit
- Vincent van Pelt, Nictiz
- Bas van Poppel, VZVZ

Revisiebeheer

Versie	Datum	Auteur	Toelichting	Status
0.1	20-11-2018	Jan Feenstra	Bijlages Handreiking Interoperabiliteit	Concept
0.97	27-12-2018	Sjaak Gondelach	Geheel aangepaste versie	Concept
0.98	24-01-2019	Sjaak Gondelach		Concept
1.0	25-01-2019	Sjaak Gondelach	Laatste aanpassingen	Definitief

Voor vragen, opmerkingen of aanvullingen kunt u contact opnemen met RSO NL via www.RSONL.nl of Nictiz.

Bijlage 1: Interoperabiliteitsmodel

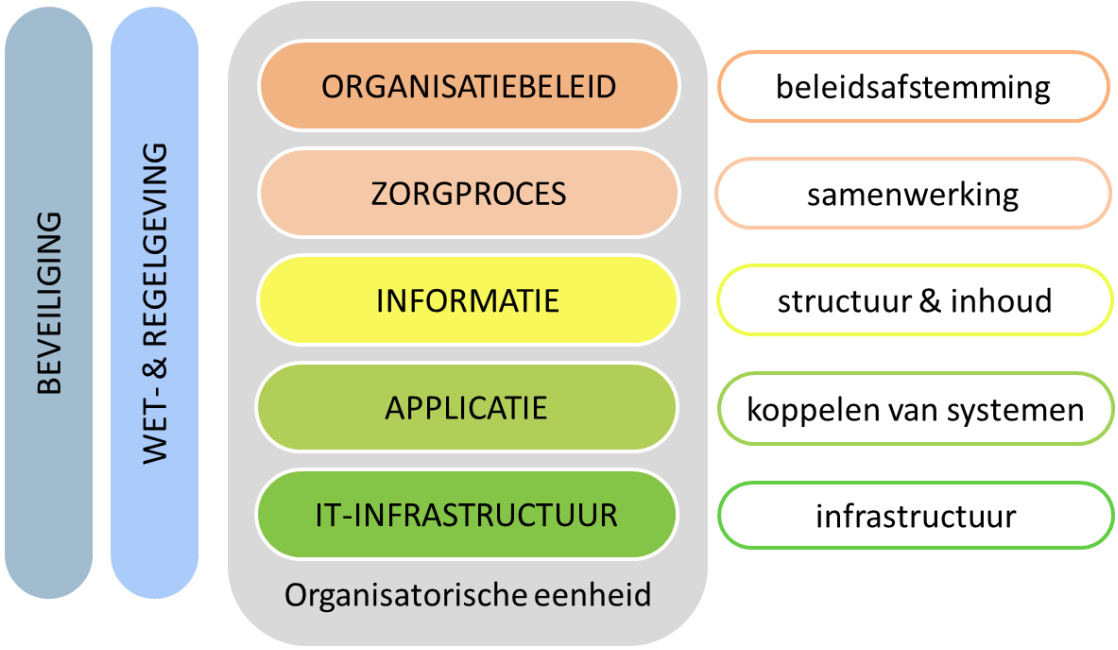
Interoperabiliteit - Afspraken op meerdere niveaus

De term 'interoperabiliteit' is veelomvattend. Het beschrijft alle maatregelen die moeten worden genomen, door meerdere stakeholders, om te komen tot veilige, betrouwbare en efficiënte informatie-uitwisseling. Een van de definities van interoperabiliteit:

> Interoperabiliteit is de mogelijkheid van verschillende autonome, heterogene systemen, apparaten of andere eenheden (bijvoorbeeld organisaties of landen) om met elkaar te communiceren en interacteren. Om dit te bewerkstelligen zijn standaarden, protocollen en procedures nodig voor de afstemming van de verschillende entiteiten op elkaar. (Wikipedia)

Model voor Interoperabiliteit

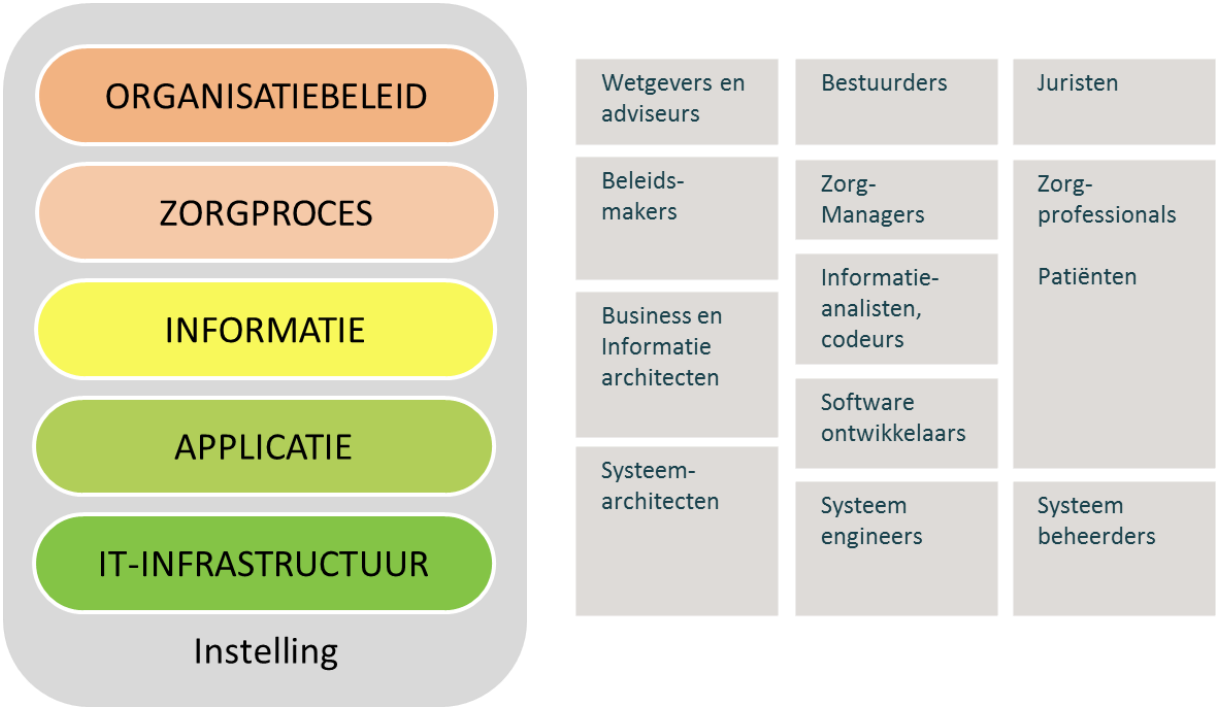
Voor een goed inzicht in de verschillende aspecten die relevant zijn bij het opzetten van interoperabiliteit tussen systemen is het Nictiz meerlagenmodel opgesteld. Het meerlagenmodel, dat inmiddels ook op Europees niveau[1] is geadopteerd als standaardmodel (eHealth Network), toont de verschillende aandachtsgebieden die betrokken zijn bij het tot stand brengen van interoperabele systemen. Er zijn verschillende indelingen en modellen mogelijk, maar dit model vermijdt technische termen en maakt duidelijk, dat er afspraken moeten worden gemaakt op en tussen alle niveaus, en dat er afstemming moet zijn tussen alle betrokken partijen.



Figuur 11 – Het Lagenmodel voor Interoperabiliteit

[1] Antilope – zie http://www.antilope-project.eu/wp-content/uploads/2013/05/D1.2a-Educational-material-presentation-v1_4.pdf

In onderstaand figuur zijn de verschillende stakeholders aangegeven die bij de verschillende interoperabiliteitsniveaus zijn betrokken:



Figuur 12 - Interoperabiliteit - verschillende stakeholders

De verschillende interoperabiliteitsniveaus van het model worden hieronder kort beschreven.

Wet- en regelgeving

Op dit niveau worden afspraken vastgelegd over de invulling van de relevante wet- en regelgeving. Het gaat dan vooral om afspraken over de implementatie van de wet- en regelgeving (in een aantal inrichtingsprincipes) vast te leggen. Op internationaal niveau wordt deze laag benut voor het afstemmen van wet- en regelgeving in de verschillende landen.

Organisatiebeleid

In deze laag worden afspraken gemaakt op bestuurlijk niveau tussen samenwerkende organisaties: organisatie van de governance, samenwerkingscontracten, raam- en bewerkersovereenkomsten, maar ook aan afspraken over verantwoordelijkheden, privacy en security, toestemming, inrichting van de infrastructuur en dergelijke.

Zorgprocessen

In elk zorgtraject, maar vooral bij ketenzorg, multidisciplinaire behandelteams en andere samenwerkingsverbanden zijn afstemming en samenwerking van vitaal belang. In deze laag worden inzicht in de zorg- en zorglogistieke processen gegeven, use cases en workflows gedefinieerd en informatieoverdracht afgestemd.

Informatie

Op dit niveau vastgelegd welke informatie-elementen, op welk detailniveau, er minimaal dienen te worden uitgewisseld. Ook de mogelijke waarden die een bepaald element kan aannemen worden hier vastgelegd. Daarnaast kunnen elementen kunnen worden gekoppeld

aan codesystemen (terminologie), waardoor ook koppelingen met vertaaltabellen, decision support systemen en dergelijke mogelijk worden.

Applicaties

Op dit niveau worden de afspraken vastgelegd over het technische uitwisselingsformaat van de over te dragen informatie (zoals HL7 CDA, HL7 FHIR of andere formats). Daarnaast worden op dit niveau afspraken over systeem configuraties, en over eisen ten aanzien van de user interface vastgelegd. Welke van de beschikbare gegevens die in de informatielaag zijn gedefinieerd, en hoeveel gegevens er worden overgedragen hangt af van de context, bijvoorbeeld een overdrachtsdocument, ontslagbrief, medicatieoverzicht, multidisciplinair overleg, patient summary. De context bepaalt dus het verpakkingsformaat (applicatielaag), terwijl de inhoud van de zorginformatiebouwstenen zoveel mogelijk hetzelfde blijft (informatielaag).

Infrastructuur

Deze laag regelt de afspraken over de infrastructuur voor de communicatie tussen systemen. Op dit niveau worden afspraken vastgelegd over de inrichting van internet protocollen, IP-nummers, SAML tokens en andere onderdelen die de systemen technisch met elkaar verbinden. In deze laag vallen ook de XDS netwerken.

Security en privacy

De beveiliging en de privacy worden op meerdere niveaus geregeld (dit wordt weergegeven door het verticaal plaatsen van deze laag). Hier worden afspraken gemaakt over de te volgen wetten, normen en richtlijnen, het inbouwen van beveiligingsactiviteiten in de workflow, het afschermen van informatie, de bewaking van de kwaliteit van de informatie, de veilige overdracht van informatie en de beveiliging van de communicatielijnen en de ICT systemen. Logging vormt ook een onderdeel van dit geheel.

Standaarden en profielen, kwalificaties

Afspraken over de te gebruiken standaarden en profielen (implementatiehandleidingen) moeten ook op meerdere lagen van interoperabiliteit worden gemaakt. Door het gebruiken van standaarden en profielen is het mogelijk om gebruik te maken van de gestandaardiseerde testmogelijkheden die door standaardisatie-organisaties als IHE, HL7 (FHIR) en PCH Alliance (CHA) worden aangeboden. Hierdoor wordt de kwaliteit van testen, en de mogelijkheid om onderdelen van de software te kwalificeren beter geregeld.

Governance

Het beheer van de Registry en de bijhorende systemen (bijvoorbeeld voor logging, beveiliging, patiënt toestemming en dergelijke) wordt in deze laag vastgelegd. In veel gevallen zal een RSO de aangewezen partij zijn voor het beheren en exploiteren van deze centrale componenten, maar ook een zorginstelling of een categorale organisatie kan deze rol uitvoeren. De governance betreft de organisatie, het beheer en het onderhoud van de systemen.

Opmerking: De verticale lagen worden vaak weggelaten omdat ze impliciet als onderdeel in elke laag wordt verondersteld.

Bijlage 2: Convenant Uitwisseling Persoonsgegevens in de Zorg

DE ONDERGETEKENDEN

B.V. <RSO_NAAM>, gevestigd en kantoorhoudend te <ADRES>, te dezen rechtsgeldig vertegenwoordigd door <NAAM>, directeur. <RSO_NAAM> voert het programma ZorgNetOost uit, daarom spreken we in dit document van “ZorgNetOost” als uitvoerende partij. In het kader van de AVG treedt ZorgNetOost op als Verwerker;

en deelnemers, hierna afzonderlijk aan te duiden als “Zorgaanbieder” en gezamenlijk aan te duiden als “de Zorgaanbieders”. In het kader van de AVG treden de Zorgaanbieders op als Verwerkingsverantwoordelijke.

ZorgNetOost en de Zorgaanbieders hierna gezamenlijk aan te duiden als “Partijen”.

OVERWEGENDE DAT

- Partijen al geruime tijd samenwerken aan elektronische informatie-uitwisseling in Twente en Oost Achterhoek, met als doel het verhogen van de kwaliteit en de efficiency van bestaande en nog te ontwikkelen samenwerking in zorgketens en het verhogen van de doelmatigheid van de zorg in het algemeen door elektronische communicatie en informatie-uitwisseling hetgeen moet leiden tot vermindering van administratieve lasten en overdrachtsproblemen;

- Partijen om deze doelen te bereiken gezamenlijk onder de naam ZorgNetOost een geheel aan infrastructuur en diensten realiseren waarbij zij zijn aangesloten;

- De gegevensuitwisseling via ZorgNetOost dient plaats te vinden in overeenstemming met geldende wet- en regelgeving, in het bijzonder de Wet geneeskundige behandelingsovereenkomst (Wgbo) en de Algemene Verordening Gegevensbescherming (AVG);

- Heldere en toepasbare set (gedrags-)regels en bijbehorende normen voor gegevensuitwisseling tussen Zorgaanbieders, op basis van de normen in de Wgbo en de AVG, nader zijn uitgewerkt in de Gedragscode Elektronische Gegevensuitwisseling in de Zorg (Gedragscode EGIZ). De Verantwoordelijke en Verwerker hechten eraan dat de uitwisseling van Persoonsgegevens zorgvuldig en in overeenstemming met de Gedragscode EGIZ plaatsvindt;

- Met de ondertekening van het Convenant Uitwisseling Persoonsgegevens in de zorg 2018 wordt het Convenant Uitwisseling Patiëntgegevens 2013 overschreven en daarmee ongeldig verklaard.

- De Zorgaanbieders ten aanzien van de gegevensverwerking via ZorgNetOost gezamenlijk zullen optreden als Verantwoordelijke in de zin van de AVG;

- Iedere Zorgaanbieder afzonderlijk optreedt als Verantwoordelijke ten aanzien van de gegevensverwerking middels de zorginformatiesystemen binnen de eigen organisatie;

- IZIT treedt uitsluitend op als Verwerker van de Persoonsgegevens en verwerkt de Persoonsgegevens uitsluitend in opdracht van de Verantwoordelijke. IZIT verwerkt Persoonsgegevens conform de AVG, de Wet geneeskundige behandelingsovereenkomst en overige toepasselijke regelgeving. IZIT sluit daartoe met alle Partijen afzonderlijk een verwerkersovereenkomst af;

- IZIT is gerechtigd om bij de verwerking een of meerdere subverwerkers in te schakelen. Met deze subverwerkers zullen overeenkomsten worden afgesloten waarin alle verplichtingen uit dit Convenant die relevant zijn voor de beveiliging van de verwerkte Persoonsgegevens zullen worden overgenomen;

- Indien bij ZorgNetOost aangesloten zorgaanbieders bezwaar hebben tegen inschakeling van een nieuwe subverwerker, kunnen zij zich richten tot IZIT.

- Zorgaanbieders kunnen bij IZIT een overzicht opvragen van de subverwerkers die door IZIT zijn ingeschakeld. Tevens zal IZIT tijdens bijeenkomsten van de klankbordgroep Privacy & Veiligheid informeren over inschakeling van nieuwe subverwerkers.

- Partijen hun wederzijdse rechten en verplichtingen met betrekking tot de elektronische informatie-uitwisseling via ZorgNetOost wensen vast te leggen in dit Convenant.

KOMEN OVEREEN ALS VOLGT

Artikel 1 – Begrippen

In deze overeenkomst hebben de volgende begrippen, telkens aangeduid met een hoofdletter, in enkelvoud en in meervoud, de volgende betekenis:

AVG	Algemene Verordening Gegevensbescherming
Betrokkene:	degene op wie een Persoonsgegeven betrekking heeft, in dit Convenant de patiënt/cliënt;
Bijlagen:	Bijlagen bij deze overeenkomst, welke hiervan integraal onderdeel uitmaken;
Convenant:	dit Convenant, met inbegrip van de daarbij behorende Bijlagen;
Elektronisch Uitwisselingssysteem:	een systeem waarmee Zorginformatiesystemen van Zorgaanbieders aan elkaar worden gekoppeld of waarmee

	Persoonsgegevens kunnen worden gedeeld of uitgewisseld;
Gedragscode EGIZ:	de Gedragscode Elektronische Gegevensuitwisseling in de Zorg;
Klankbordgroep	de Klankbordgroep Privacy & Veiligheid van ZorgNetOost;
Persoonsgegeven:	elk gegeven betrekking hebbende op een geïdentificeerde of identificeerbare persoon;
Regiegroep:	de Regiegroep van ZorgNetOost;
Verantwoordelijke:	de Verantwoordelijke ten aanzien van de gegevensverwerking via ZorgNetOost als bedoeld in de AVG ;
Verwerker:	de Verwerker in de zin van de AVG, zijnde degene die ten behoeve van de Verantwoordelijke(n) Persoonsgegevens verwerkt, zonder aan diens rechtstreeks gezag onderworpen te zijn;
Wgbo:	Wet geneeskundige behandelingsovereenkomst;
Zorgaanbieder:	een Zorgaanbieder als bedoeld in artikel 1 sub c van de Wet gebruik burger service nummer in de zorg, zijnde een Zorgaanbieder als bedoeld in artikel 1 Kwaliteitswet zorginstellingen dan wel een beroepsbeoefenaar die zijn beroep uitoefent anders dan in het kader van een instelling als bedoeld in artikel 1 van de Kwaliteitswet zorginstellingen;
Zorginformatiesysteem:	het informatiesysteem van een Zorgaanbieder voor de elektronische verwerking van zorginformatie en Persoonsgegevens;
ZorgNetOost	het door Partijen gerealiseerde geheel aan infrastructuur en diensten.

Artikel 2 – Doel en reikwijdte Convenant

2.1 Het doel van dit Convenant is het vastleggen van de (juridische) uitgangspunten rondom de elektronische informatie-uitwisseling van patiëntgegevens via ZorgNetOost en de besluitvorming hierover in het kader van de Algemene Verordening Gegevensbescherming (AVG).

Artikel 3 – Uitgangspunten samenwerking en verplichtingen Partijen

3.1 Partijen zullen optreden als goede Convenant-partners en zullen de in het Convenant genoemde uitgangspunten en doeleinden verwezenlijken.

Artikel 4 – Dienstverlening ZorgNetOost

4.1 ZorgNetOost zal binnen het kader van dit Convenant aan de Zorgaanbieders de volgende diensten verlenen:

- het beheer van het Elektronisch Uitwisselingssysteem inclusief de logging van het gebruik en welk document wordt ingezien;
- het identificeren van knelpunten en/of verder verbetermogelijkheden m.b.t. het gebruik van het Elektronisch Uitwisselingssysteem en op basis daarvan acteren of adviseren;

- het verschaffen van aanvullende kennis en faciliteiten aan instellingen en beroepsbeoefenaren werkzaam in de gezondheidszorg, om de samenwerking in de zorgketens te bevorderen en/of te verbeteren.

Artikel 5 – Governance

5.1 De Partijen stellen een Regiegroep in. Binnen de Regiegroep besluiten de aangesloten zorgaanbieders over de (in)richting van Architectuur en over de (in)richting van Privacy & Veiligheid binnen de regio en wordt de uitwerking ervan geëvalueerd en gemonitord. De Regiegroep laat zich onder andere adviseren door de Klankbordgroep Privacy & Veiligheid.

5.2 ZorgNetOost treedt op als voorzitter van de Regiegroep. De Regiegroep overlegt op basis van de afspraken werkwijze en besluitvorming Regiegroep, zoals aangehecht in Bijlage 1.

5.3 De partijen stellen een Klankbordgroep Privacy & Veiligheid in. Binnen deze Klankbordgroep wisselen ZorgNetOost en aangesloten Zorgaanbieders informatie uit over regionale samenwerking, ontwikkelingen en voortgang met betrekking tot Privacy & Veiligheid in de regio. De Klankbordgroep voorziet de Regiegroep van gevraagd, ongevraagd, vrijblijvend en zwaarwegend advies op het gebied van Privacy & Veiligheid. De Klankbordgroep overlegt op basis van de Afspraken werkwijze en besluitvorming Klankbordgroep, zoals aangehecht in Bijlage 2.

5.4 De partijen wijzen in samenspraak een vertegenwoordiger aan die bevoegd is om namens zijn partij deel te nemen in de Klankbordgroep.

Artikel 6 – Privacy en informatiebeveiliging

6.1 De Verantwoordelijke en Verwerker hanteren beveiligingsmaatregelen die voldoen aan de AVG en NEN7510, NEN7512, NEN7513 en nieuwe NEN normen.

6.2 ZorgNetOost en de door haar ingezette personen zijn verplicht tot geheimhouding van Persoonsgegevens waarvan zij bij het verwerken ten behoeve van de Verantwoordelijke kennis nemen, behoudens en voor zover enig wettelijk voorschrift hen tot openbaarmaking en/of afgifte verplicht. Daarnaast verzekert ZorgNetOost dat de geheimhoudingsverplichting een onderdeel is van de arbeidsvoorwaarden van al haar medewerkers.

6.3 ZorgNetOost zal slechts tegemoet komen aan vorderingen van derde partijen, waaronder overheidsinstanties, tot het verstrekken van (persoons-)gegevens indien zij hiertoe verplicht is op grond van wet- en regelgeving of op grond van een rechterlijke uitspraak.

6.4 ZorgNetOost zal de Verantwoordelijke onverwijld informeren indien een daartoe bevoegde overheidsinstantie een op de wet gebaseerd verzoek of krachtens rechterlijke uitspraak tot verstrekking van Persoonsgegevens heeft gedaan.

6.5 Indien zich een datalek voordoet, meldt de Verantwoordelijke dit bij de Autoriteit Persoonsgegevens en informeert tevens de Betrokkenen. Alleen datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht.

6.6 De Verwerker stelt de Verwerkingsverantwoordelijke op de hoogte indien zich een datalek voordoet.

6.7 Indien Betrokkenen vragen hebben of uitvoering willen geven aan de rechten die worden ontleend aan de AVG, kunnen zij zich richten tot de eigen zorgaanbieder.

Artikel 7 – Duur en beëindiging

7.1 Dit Convenant treedt in werking na akkoord door Partijen en wordt aangegaan voor onbepaalde tijd. Zodra het Convenant door een Partij is ondertekend, zal deze, ook voorafgaande aan ondertekening door alle Partijen, aan de bepalingen van dit Convenant gebonden zijn.

7.2 Opzegging van dit Convenant dient door een Partij per aangetekende brief te geschieden met inachtneming van een opzegtermijn van zes maanden. Bij opzegging door een enkele Partij of meerdere Partijen blijft het Convenant voor de overige Partijen onverminderd van kracht.

7.3 Iedere Partij kan verzoeken om aanpassingen aan het Convenant indienen. Deze worden vervolgens door de Regiegroep beoordeeld en wordt besloten tot wijziging of aanvulling.

7.4 Partijen zullen in overleg treden over beëindiging van dit Convenant indien er geen gegevensverwerking meer plaatsvindt via ZorgNetOost.

Artikel 8 – Bijlagen

8.1 Dit Convenant kent de volgende Bijlagen:

- Bijlage 1: Afspraken werkwijze en besluitvorming Regiegroep;
- Bijlage 2: Afspraken werkwijze en besluitvorming Klankbordgroep Privacy & Veiligheid.

Artikel 9 – Algemene bepalingen

9.1 Wijzigingen van en aanvullingen op het Convenant zijn slechts geldig indien zij door de Regiegroep overeengekomen zijn. Wijzigingen en aanvullingen worden gemeld bij ZorgNetOost, aangezien zij de vergaderingen van de Regiegroep voorzit en de agenda opstelt.

9.2 Op het Convenant is Nederlands recht van toepassing.

Ondertekening Convenant Uitwisseling Persoonsgegevens in de zorg

Zorgaanbieder:	
Naam:	
Handtekening:	
Datum:	

Bijlage 1 bij Convenant Uitwisseling Persoonsgegevens in de Zorg

Afspraken werkwijze en besluitvorming Regiegroep

1. Introductie

1.1. In het Convenant Uitwisseling Persoonsgegevens in de zorg zijn tussen de betrokken partijen afspraken gemaakt over de governance van de AVG wetgeving. In artikel 5.1 van het Convenant is bepaald dat er een Regiegroep in het leven wordt geroepen. De hoofdtaak van de Regiegroep is om het beleid omtrent Privacy & Veiligheid vast te stellen, uit te zetten en te monitoren.

1.2. ZorgNetOost treedt op als voorzitter van de Regiegroep.

1.3. Op basis van het voorgaande maken de Partijen de volgende afspraken over het overleg in de Regiegroep.

2. Leden van de Regiegroep

2.1. De Regiegroep bestaat uit vertegenwoordigers van alle Zorgaanbieders die het Convenant ondertekend hebben.

3. Vergaderingen

3.1. De Regiegroep vergadert drie keer per jaar, of zoveel vaker als nodig is voor een effectieve besluitvorming over uitwisseling van Persoonsgegevens met ZorgNetOost. De vergaderingen vinden plaats ten kantore van ZorgNetOost.

3.2. Partijen worden ondersteund door een secretaris van ZorgNetOost. Deze stuurt uiterlijk een week voor de vergadering een agenda en vergaderstukken aan de leden van de Regiegroep. Iedere Partij kan uiterlijk 14 dagen voor de vergadering bespreekpunten agenderen.

3.3. Indien de Regiegroep besluit zich niet te schikken in het advies van de Klankbordgroep, dient hiervoor een onderbouwing te worden aangedragen bij de Klankbordgroep.

3.4. De volgende zaken behoren in ieder geval tot het overleg van de Regiegroep:

- het vaststellen van de doeleinden en reikwijdte van de gegevensverwerking die betrekking heeft op de AVG wetgeving zoals genoemd in artikel 2 van het Convenant;
- Besluitvorming jaarprogramma ten aanzien van Privacy & Veiligheid.
- Vaststellen, uitwerken, evalueren en monitoren van het beleid ten aanzien van Privacy & Veiligheid.

Bijlage 2 bij Convenant Uitwisseling Persoonsgegevens in de Zorg

Afspraken werkwijze en besluitvorming Klankbordgroep Privacy & Veiligheid

1. Introductie

1.1 In het Convenant Uitwisseling Persoonsgegevens in de zorg zijn tussen de betrokken partijen afspraken gemaakt over de governance van de AVG wetgeving. In artikel 5.3 van het Convenant is bepaald dat er een Klankbordgroep in het leven wordt geroepen. Binnen de Klankbordgroep worden regionale samenwerking, ontwikkelingen en voortgang ten aanzien van Privacy & Veiligheid in de regio besproken.

1.2 Ieder der Partijen wijst een vertegenwoordiger aan die bevoegd is om namens deze partij zijn stem uit te brengen.

1.3 Op basis van het voorgaande maken de Partijen de volgende afspraken over het overleg in de Klankbordgroep.

2. Leden van de Klankbordgroep

2.1 De Klankbordgroep bestaat uit vertegenwoordigers van alle Zorgaanbieders die het Convenant ondertekend hebben. Vertegenwoordigers van Zorgaanbieders die het Convenant niet ondertekend hebben zijn welkom, maar hebben geen stem in de besluitvorming.

3. Vergaderingen

3.1 De Klankbordgroep vergadert vier keer per jaar, of zoveel vaker als nodig is voor een effectieve besluitvorming over uitwisseling van Persoonsgegevens met ZorgNetOost. De vergaderingen vinden plaats ten kantore van ZorgNetOost.

3.2 Partijen worden ondersteund door een secretaris van ZorgNetOost. Deze stuurt uiterlijk een week voor de vergadering een agenda en vergaderstukken aan de leden

van de Klankbordgroep. Iedere Partij kan uiterlijk 14 dagen voor de vergadering bespreekpunten agenderen.

3.3 Indien tijdens een vergadering van de Klankbordgroep wordt besloten dat er onafhankelijk advies vereist is over een specifieke kwestie, zal de hulp worden ingeroepen van een externe onafhankelijke expert.

3.4 De volgende zaken behoren in ieder geval tot het overleg van de Klankbordgroep:

- Informatie uitwisselen over ontwikkelingen en voortgang op het gebied van Privacy & Veiligheid in de regio.
- Gevraagd, ongevraagd, vrijblijvend en zwaarwegend advies uitbrengen aan de Regiegroep met betrekking tot Privacy & Veiligheid.

4. Besluitvorming

4.1 Waar besluiten moeten worden genomen, zal dit met tweederde meerderheid gebeuren, waarbij de overwegingen van degenen die niet instemmen met een besluit genoteerd zullen worden.

4.2 Aan de besluitvorming wordt alleen deel genomen door vertegenwoordigers van Zorgaanbieders die dit convenant hebben ondertekend.

Bijlage 3: Template gecombineerde SLA en DAP

Service Level Agreement

Dit document beschrijft de verantwoordelijkheden van <RSO>, en <NAAM LEVERANCIER> (hierna: <leverancier>), de gemaakte afspraken en de wijze van communicatie rond het operationeel beheer van de centrale <RSO> XDS infrastuctuur.

In de SLA is opgenomen:

- werkwijze met betrekking tot activiteiten op het grensvlak tussen <RSO> en <leverancier>, communicatie tussen beide partijen in het kader van het beheer, het onderhoud en de exploitatie van de betrokken applicaties.
- De verantwoordelijkheden van beide partijen met betrekking tot de overdracht van de gegevens en de hierbij benodigde rapportage en communicatie

De bepalingen in de Overeenkomst zijn integraal en volledig van toepassing op de SLA. Indien en voor zover er sprake is van overlappende bepalingen in de Overeenkomst en de SLA die tegenstrijdig met elkaar zijn, dan gaat de bepaling in deze Overkomst voor.

Aanpassingen en uitbreidingen van de SLA

- Bij een wijziging in de vorm van een uitbreiding of aanpassing van de SLA wordt een additioneel document opgesteld en genummerd en getekend toegevoegd aan deze overeenkomst (Aanpassing/Uitbreiding SLA nr.: XX).
- Uitbreidingen of wijzigingen zijn alleen mogelijk bij wederzijdse goedkeuring door partijen en schriftelijke bevestiging door partijen.

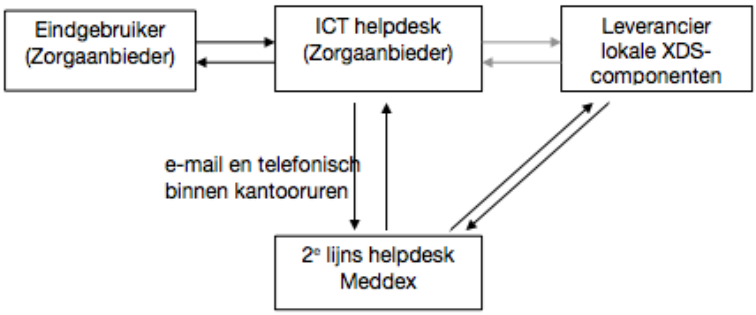
1.1. Verantwoordelijkheden <leverancier>

- Beschikbaar stellen en houden van een centrale (<RSO>) XDS infrastructuur waarmee zorgaanbieders aangesloten bij <RSO>, via een beveiligde verbinding, informatie kunnen uitwisselen.
- Het onderhouden van de infrastructuur
- Monitoren van de infrastructuur.
- Doorgeven van geconstateerde storingen in de infrastructuur.
- Adviseren m.b.t. de wijze van overdracht van gegevens
- Operationeel houden van de beveiligde verbindingen vanuit de aangesloten zorgaanbieders.

1.2. Verantwoordelijkheden <RSO>

- Het borgen dat zorgaanbieders informatie op correcte wijze aanleveren en gebruiken.
- Het borgen dat zorgaanbieders een correct BPPC aanleveren ter ondersteuning van het patiëntmandaat.
- Het ‘enforcen’ van de BPPCs door de Consumers van de ontvangende zorgaanbieders.
- Tijdig (minimaal 2 maanden voor in-productie-name) informeren van <leverancier> indien er wijzigingen in de lokale consumer-/client-systemen bij de zorgaanbieders voorzien zijn, dit met het oog op het waarborgen van de continuïteit van de Dienst, en borgen dat zorgaanbieders een actuele testomgeving beschikbaar stellen en doortesten.
- Het borgen dat zorgaanbieders in geval van storingen op hun lokale infrastructuur tijdig <leverancier> informeren.
- Borgen dat zorgaanbieders in geval van een hotfix of software updates tijdig <leverancier> informeren.

1.3. Organisatie operationeel beheer



1.3.1. De communicatie verloopt volgens het volgende schema:

Eindgebruiker bij een zorgaanbieder neemt contact op met zijn lokale support organisatie. Indien de lokale support organisatie constateert dat zij de eindgebruiker niet kunnen helpen nemen zij contact op met de 2e lijns helpdesk <leverancier>. Alle aangemelde issues worden door de 2e lijns helpdesk <leverancier> binnen kantooruren (07.00 – 18.00) opgepakt. <leverancier> voert de regie over de probleemoplossing.

Bij issues die regelmatig voorkomen en waarvan de oorzaak bij de leverancier van de lokale XDS-componenten ligt, zal de lokale support organisatie voor de snelste afhandeling zelf contact leggen met deze leverancier.

1.3.2. Contacten

In de samenwerking tussen <RSO> en <leverancier> is sprake van de volgende functionarissen met navolgende relevante functieomschrijvingen:

- Eindverantwoordelijke(n)
- Operationeel aanspreekpunt
- ICT organisatie/helpdesk
- 2e lijns helpdesk <leverancier>

Partijen zullen per deelproject aan elkaar kenbaar maken door wie bovengenoemde functies worden bekleed in een contactmatrix.

	<leverancier>
Eind verantwoordelijke	Directeur Tel: <TELEFOON>
Operationeel aanspreekpunt	Manager Operations <RSO>.xds@<leverancier>.nl Tel: <TELEFOON>
2e lijns helpdesk	Support <RSO>.xds@<leverancier>.nl Tel: <TELEFOON>

	<RSO>
Eind verantwoordelijke	Manager <RSO>
Operationeel aanspreekpunt	Servicemanager <RSO>

Indien <RSO> of <leverancier> een deel van de operationele en beheeractiviteiten uitbesteden aan derden blijven <RSO> en <leverancier> zelf de aanspreekpunten, tenzij uitdrukkelijk anders vermeld. <RSO> en <leverancier> zijn ten overstaan van elkaar en de

wetgever verantwoordelijk voor deze uitbestede activiteiten zoals vastgelegd in de samenwerkingsovereenkomst.

1.3.3. 1E LIJNS HELPDESK

De helpdesk van de aangesloten Ziekenhuizen benaderen de 2e lijns helpdesk <leverancier>. Indien de aanmelding telefonisch is registreert de 2e lijns helpdesk <leverancier> in het support systeem. neemt de call van de aan en registreert deze in het systeem van <leverancier>. <leverancier> geeft wegens de registratie en administratie van incidenten er de voorkeur aan dat men e-mail gebruikt voor de aanmelding van ICT incidenten.

De helpdesk van het ziekenhuis zal doorgaans vragen rond de beschikbaarheid van de <RSO> XDS infrastructuur, diensten en de gepresenteerde gegevens kunnen beantwoorden. Wanneer de helpdesk een vraag niet zelf kan beantwoorden, neemt zij contact op met de 2e lijns helpdesk <leverancier>.

De 1e lijns helpdesks van de ziekenhuizen reageren afhankelijk van de spoedeisendheid met afdoende snelheid op vragen van de 2e lijns helpdesk <leverancier>. In geval van hoge spoed zal <leverancier> telefonisch contact opnemen. De reactietijd van de 1e lijns helpdesks van de ziekenhuizen wordt niet meegerekend in de oplostijd.

1.3.4. 2E LIJNS HELPDESK <LEVERANCIER>

Bereikbaarheid: 07.00 – 18.00*
Email : <RSO>.xds@<leverancier>.nl
Telefonisch: <TELEFOON>

* werkdagen (maandag t/m vrijdag) met uitzondering van de algemeen erkende feestdagen (nieuwjaarsdag, 1e en 2e paasdag, Koningsdag, Hemelvaartsdag, 1e en 2e pinksterdag, 1e en 2e kerstdag).

De telefoonlijn is voorzien van een voicemail met een specifieke <RSO> welkomsttekst. Als alle lijnen bezet zijn of de telefoon niet opgenomen kan worden, kan de beller zodoende een voicemail inspreken, dit resulteert tevens direct in een call in het ticketing systeem.

De performance van de <RSO> 2e lijns helpdesk (<leverancier>) is als volgt:

- Minimaal 90% van de telefonische meldingen binnen 1 minuut opnemen.
- Minimaal 95% binnen 2 minuten opnemen (gemeten over een periode van een maand).

<leverancier> neemt conform bovenstaande specificatie op met een piekbelasting van 120% ten opzichte van het gemiddeld aantal calls van het voorgaande maand.

a. Beheer persoonsgegevens

Er worden geen persoonsgegevens anders dan document Metadata, BSN- en Patiëntnummer bewaard. Het BSN-nummer is nodig om te voldoen aan de Nictiz standaard die beschrijft dat BSN-nummer de unieke identifier is.

b. Change Management

Bij elke wijziging (zoals software versie) aan de lokale XDS componenten van een van de betrokken zorgaanbieders aangesloten op <RSO>, wordt <leverancier> tijdig genotificeerd, in beginsel minimaal een week van te voren. Wanneer het gebruik van de <RSO> infrastructuur door de wijziging sterk wijzigt (> 50% meer verkeer of grotere berichten)

dient de zorgaanbieder dit drie tot vier weken van te voren aan <leverancier> aan te geven, en zelf met de testomgeving de werking te testen. Doel is dat <leverancier> tijdig eventueel benodigde wijzigingen aan kan brengen in de Dienst, zodanig dat de data-overdracht snel na de effectuering van de wijziging weer goed doorloopt.

Bij wijzigingen aan de software omgeving van <leverancier> stelt <leverancier> de informatie tijdig beschikbaar betreffende deze wijzigingen en de eventuele impact op systemen en/of gebruikers.

Changes worden in principe geïmplementeerd op basis van OTAP. Wijzigingen worden ontwikkeld, geïnstalleerd op een testomgeving, getest door Zorgaanbieders. Na akkoord door de <RSO> Servicemanager wordt de wijziging uitgerold naar de productie-omgeving.

In geval van calamiteiten (snelle implementatie noodzakelijk) of als er geen impact op eindgebruikers voorzien wordt kan er na overleg tussen <RSO> en <leverancier> besloten om wijzigingen zonder de volledige OTAP procedure uit te voeren (denk aan b.v. noodpatches).

De testomgeving dient door <RSO> (aangesloten zorgaanbieders) van voldoende en volledige test data voorzien te zijn conform testscript. Mocht de testomgeving van <RSO> niet in lijn zijn met de live omgeving waardoor bij de in productie name meerwerk verricht dient te worden zal <leverancier> de bestede uren factureren op basis van nacalculatie aan <RSO>.

c. Aansluiten nieuwe gebruiker

<RSO> stemt de voorziene aansluiting van een nieuwe gebruiker (organisatie) 2 maanden van te voren met <leverancier> af. De nieuwe gebruiker en <leverancier> wisselen aansluit-informatie zoals IP-adressen, poorten, endpoints en certificaten met elkaar uit van de testomgevingen bij de nieuwe gebruiker en bij <leverancier>, en testen vervolgens de aanmelding en opvraging van informatie af. <RSO> besluit op basis van de testresultaten of aansluiting op productie akkoord is, en stelt in overleg met <leverancier> een datum af voor in-productie-name. De nieuwe gebruiker en <leverancier> wisselen vervolgens aansluit-informatie uit van de productieomgevingen en testen technisch of de verbindingen goed tot stand komen, om vervolgens op de afgesproken datum de nieuwe aansluiting in productie te nemen.

d. Incidenten

Incidenten worden ingedeeld in 3 verschillende typen/prioriteiten:

Incident-Type	Prio	Responstijd	Target oplostijd	Gegarandeerde oplostijd
Fatale fout	hoog	1 uur*	< 2 uur*	< 8 uur*
Ernstige fout	midden	2 uur*	< 4 uur*	< 12 uur*
Storende fout	laag	4 uur*	< 8 uur*	< 24 uur*

*uitgaande van werkdagen van 8 uur

Fatale fout

- er kan door alle gebruikers niet met de XDS-infrastructuur gewerkt worden: de zorgprocessen worden verstoord, de fout treft alle of een logische groep gebruikers.

Ernstige fout

- er kan door alle gebruikers beperkt met de XDS-infrastructuur gewerkt worden;

niet alle functionaliteit is beschikbaar de zorgprocessen worden ten dele verstoord, de fout treft alle of een logische groep gebruikers.
- er kan door een bepaalde groep gebruikers, bijvoorbeeld alle gebruikers van 'systeem X' of alle gebruikers van 'instelling Y', niet met de XDS-infrastructuur gewerkt worden.

Storende fout

- er kan gewerkt worden met het systeem met behulp van een (relatief) eenvoudige workaround: de fout treft een logische groep gebruikers of individuele gebruikers of instellingen.

Incidenten die aangemeld worden bij de <leverancier> helpdesk, maar buiten de standaard dienstverlening vallen, zal <leverancier> de bestede uren factureren op basis van nacalculatie (€80 per uur) aan <RSO> met een minimale rekeneenheid van een half uur. Dit betreft alleen incidenten op in-productie-genomen aansluitingen

e. Facturatie

Zodra calls die buiten de standaard dienstverlening vallen (zoals vastgelegd in de beantwoording van het programma van eisen) vaker dan 3 keer per kwartaal voorkomen en meer dan 15 minuten tijd per keer vergen, zal <leverancier> deze calls aan <RSO> factureren tegen het afgesproken uurtarief.

De <leverancier> Helpdesk zal bij de 3e repeterende call in een kwartaal direct aan <RSO> rapporteren, zodat <RSO> in overleg kan gaan met de betreffende partij om volgende calls te voorkomen.

f. Autorisatiebeheer

De deelnemende zorgaanbieders zijn verantwoordelijk voor medewerker autorisatie voor toegang op de infrastructuur en de daarin beschikbare gegevens.

g. Technisch beheer

1.3.5. Procedureafspraken

Het betreft de processen met betrekking tot de ontsluiting van de patiëntgegevens via de XDS infrastructuur van <RSO>. De volgende servicelevels worden afgesproken:

1.3.6. Redundantie, Back-up en restore activiteiten

Technisch Beheer van <leverancier> zal de (virtual) machines meenemen in een redundantie en back-up mechanisme.

1.3.7. Availability management

<leverancier> garandeert een uptime van de XDS infrastructuur van 99,7% gemeten over een periode van 3 maanden.
Beschikbaarheid wordt als volgt gemeten.
Beschikbaarheidspercentage = $\frac{T - D - U}{T - U} \times 100\ \%$

T	het totaal aantal uren over de periode
D	het totaal aantal uren over de periode geregistreerde tijd, dat er beperkte of geen toegang tot het functionaliteit was.
U	overeengekomen geplande down tijd

De downtime wordt daarbij altijd gepland in overleg met <RSO>, zodat de gebruikers zo

weinig mogelijk last hebben van de downtime. Service updates en downtime die niet wordt veroorzaak door de <leverancier> software wordt niet meegerekend bij de downtime (U) van de infrastructuur. De uren die gebruikt worden voor het onderhoudswindow zijn buiten kantoortijden.

De operationeel Beheerders van <leverancier> monitoren de werking van de machines waar de <RSO> XDS infrastructuur op draait en ondernemen actie wanneer de machine niet meer draait en/of niet meer via het netwerk benaderbaar is.

1.3.8. Browser compatibilty en accessibility

<leverancier> ondersteunt de actuele en voorgaande versie van de volgende browsers waarin de webviewer te gebruiken is: Internet Explorer, Google Chrome en Firefox.

In praktijk werkt de webviewer ook in oudere versies zoals Internet Explorer 8 of 9, maar <leverancier> behoudt zich het recht voor om eventuele issues in de webviewer niet op te lossen als ze alleen in deze oudere versies voorkomen, en nieuwe functionaliteiten te ontwikkelen voor gebruik in alleen de nieuwere browser-versies.

Tevens dienen Zorgaanbieders de webviewer bereikbaar te maken en houden via firewalls en proxyserver.

h. Overige communicatie tussen opdrachtgever en opdrachtnemer

1.3.9. Contactmomenten

- Samenwerkingsoverleg vindt twee keer per jaar plaats, in januari en juli;
- Operationeel overleg vindt minimaal vier keer per jaar plaats, in januari, april, juli en oktober, en daarnaast in overleg wanneer er aanleiding toe bestaat;

1.3.10. Overlegvormen

Ten behoeve van de afstemming tussen <RSO> en <leverancier> worden verschillende vormen van gestructureerd overleg geïnitieerd. Essentieel zijn het Samenwerkingsoverleg (op strategisch niveau) en het Operationeel overleg.

<u>Samenwerkingsoverleg</u>
Doelstelling:

- Het verbeteren van het totale proces inzake de Dienstverlening met betrekking tot de kwaliteit en organisatie van de Dienstverlening, nu en in de toekomst;
- Het beleidsmatig op elkaar afgestemd houden van de betrokken partijen;

Over alle zaken die niet beschreven staan in dit document, zal in onderling overleg tussen <RSO> en <leverancier> in dit Samenwerkingsoverleg besloten worden.
Deelnemers

- <RSO>: Servicemanager en Manager;
- <leverancier>: Directeur;
  in voorkomende gevallen andere benodigde disciplines of genodigden.

Inhoud:
Besluiten worden genomen over de volgende zaken, voor zover deze binnen de grenzen vallen van het contract:

- organisatorische aspecten teneinde doeltreffendheid en doelmatigheid van de dienstverlening te handhaven c.q. te verbeteren;
- klachten van klanten van <RSO> en plannen voor structurele oplossingen;
- aankomende wijzigingsopdrachten;
- bijsturing op voortgang en prioriteit van de reguliere beheeractiviteiten;
- bijstelling van de inhoud van deze SLA;

Frequentie:
Twee keer per jaar en twee maanden voor het einde van de overeenkomst.

Operationeel overleg
Doelstelling:
Het operationeel op elkaar afgestemd houden van <RSO> en <leverancier> wat betreft De Dienstverlening. In het operationeel overleg wordt de dagelijkse gang van zaken afgestemd en worden eventuele operationele knelpunten besproken. Dit operationeel overleg is tevens een voorbereidend overleg voor het Samenwerkingsoverleg.

Deelnemers
- <RSO>: Operationeel Verantwoordelijken;
- <leverancier>: Manager Operations;

In voorkomende gevallen andere benodigde disciplines.

Inhoud:
Besluiten binnen dit overleg mogen worden genomen ten aanzien van de volgende zaken, voor zover deze binnen de grenzen vallen van het contract en van de afspraken in het managementoverleg tenzij in individuele gevallen anderszins overeengekomen:
- Update aan de contactmatrix zoals benoemd in artikel 1.3.2.
- klachten afhandelen en maatregelen doorvoeren ter voorkoming van herhaling;
- procedures en werkwijzen ter handhaving c.q. verbetering van betrouwbaarheid; doeltreffendheid en doelmatigheid van de dienstverlening;
- controleren van de verwerking van verzoeken aan de XDS infrastructuur;
- voortgang van wijzigingsopdrachten;
- bijsturing op voortgang van de reguliere beheeractiviteiten;
- operationele problemen en ondernomen preventieve en correctieve acties;
- evalueren van operationele procedures en technische aspecten van de XDS infrastructuur;
- besluitvorming ten aanzien van zaken die vanuit het Samenwerkingsoverleg zijn doorverwezen;
- beschikbaarheid ontwikkelomgevingen;

Frequentie:
Operationeel overleg vindt minimaal vier keer per jaar plaats, binnen twee weken na het verstrijken van elk kwartaal, en daarnaast in overleg wanneer er aanleiding toe bestaat

i. Documentatie en rapportages

1.3.11. Soorten documentatie

Het beheer en onderhoud van de volgende documenten wordt verzorgd door <leverancier>:
- Deze Service Level Agreement (SLA)
- Systeemarchitectuur van de XDS infrastructuur
- Beheer documentatie – gebruik logboek-portaal
- Aansluitdocument 2.0
- Rond implementaties/straat landschap met IP adressen, poorten e.d. en afwijkingen van architectuur/codelijst.

1.3.12. Verspreiding van documentatie

Alle wijzigingen in de documentatie worden per direct tussen <leverancier> en <RSO> uitgewisseld.
Het verstrekken van documenten en dossiers aan derden, buiten <leverancier> en <RSO>, vindt uitsluitend plaats na schriftelijke goedkeuring van de wederpartij. Een uitzondering hierop vormen de controle-instanties van beide partijen.
Een papieren exemplaar van de meest recente versie van de in 1.12.1 genoemde documenten wordt bewaard op het secretariaat van <leverancier>.

j. Rapportages

Vanuit <leverancier> maandelijks:

- Overzicht beschikbaarheid van De Dienstverlening
- Maandelijks overzicht incidenten (aantal/aard/oplostijd)
- Beschrijving belangrijke incidenten
- Wijzigingen in de geleverde dienst en voorziene wijzigingen in het berichtenboek.
- Gebruiksrapportage (aanmeldingen/bevragingen/transacties/bron adres/doeladres transacties)
- Uitgevoerde changes
- Toekomstige changes en uitbreidingen dienst

Bij urgente (down/bijna down) issues directe emailnotficatie naar de <RSO> Service Manager plus rapportage na afloop.

Vanuit <RSO>:

- wijzigingen in de aangeleverde gegevens voor zover dat gevolgen heeft op de door <leverancier> geleverde dienst (met name moet gedacht worden aan toevoegingen aan de centraal aangeboden type data en de hoeveelheid data).

<leverancier> verstuurt deze rapportages elk kwartaal naar de <RSO> Service Manager, en maandelijks een overzicht van incidenten.

Bijlage 4: Aansluitdocument

Deze bijlage bevat delen uit het aansluitdocument zoals dat in gebruik is bij RijnmondNet.

Uitgangspunten Beelden- en documentenuitwisseling

De belangrijkste uitgangspunten voor de Beelden- en documentenuitwisseling van Stichting RijnmondNet zijn onderverdeeld in drie onderdelen, te weten juridisch/organisatorisch, functioneel en technisch.

Juridisch/organisatorisch

De Beelden- en documentenuitwisseling is opgezet op basis van IHE-profielen voor het uitwisselen van medische beelden en documenten. IHE-profielen zijn leidend.

Stichting RijnmondNet hanteert de "Gedragscode Elektronische Gegevensuitwisseling in de Zorg, Gedragscode EGiZ (zie **Fout! Verwijzingsbron niet gevonden.**). Stichting RijnmondNet beveelt participanten de gedragscode ten stelligste aan deze binnen de eigen organisatie te hanteren.

Ondertekening door deelnemers van de overeenkomst/convenant met daarin de wederzijdse rechten/plichten. Aspecten die hierin beschreven worden hebben met name betrekking op patiënt privacy, beschikbaarheid van gegevens, beveiliging en onderling vertrouwen.

Functioneel

Bij het aanmelden van beelden en verslagen is een gevalideerd BSN als unieke identifier van de patiënt vereist;

Er is een centrale test, acceptatie en productieomgeving beschikbaar, deze zijn volledig van elkaar gescheiden.

Acceptatie- en productieomgeving dient door alle aangesloten instellingen te worden gebruikt en wordt gebruikt voor keten testen2.

De Nictiz Richtlijn voor implementatie van toestemmingsprofielen binnen XDS-netwerken (versie Richtlijn document BPPC binnen XDS-netwerken) is leidend. (zie **Fout! Verwijzingsbron niet gevonden.**)

Het voorkomen van misbruik van inzage en het opsporen van misbruik bij inzage vanuit de eigen zorginstelling is de verantwoordelijkheid van die betreffende deelnemende zorginstelling.

Alle gebruikers dienen een persoonlijk account te hebben. Groepsaccounts zijn niet toegestaan.

Technisch

Het gebruik van UZI-servercertificaten voor de deelnemende zorginstellingen t.b.v. unieke authenticatie van betrokken applicaties is noodzakelijk voor zowel de acceptatie- als de productieomgeving.

De Nictiz Dataset voor XDS-metadata is leidend. Deze is echter (dd Mrt 2017) nog niet door Nictiz vrijgegeven. Er is daarom een interim procedure voor het omgaan met metadata. Zie bijlage 1 voor deze interim procedure. Zie bijlage 4 voor de IHE-specificaties voor het Stichting RijnmondNet affinity domain.

---

[2] De testomgeving is beschikbaar sinds 2017 en wordt ook wel "ontwikkelomgeving" genoemd. De huidige partijen zijn aangesloten op de Rijnmondnet acceptatie- en productieomgeving

Belangrijk punt iig is om in de metadata de authorinstitution goed in te vullen met de naam van de zorginstelling en dit af te stemmen met Rijnmondnet (omdat dit veld gebruikt wordt voor de access control). Deze dient daarom ook voor alle documenten van 1 zorginstelling hetzelfde te zijn.
Volgen van de richtlijn voor het gebruik van BSN in de DICOM-header, opgesteld door Nictiz en IHE Nederland (zie **Fout! Verwijzingsbron niet gevonden.**).
De aan de Beelden- en documentenuitwisseling gekoppelde systemen van een zorgorganisatie dienen te voldoen aan de GBZ (Goed Beheerd Zorgsysteem) eisen. De GBZ stelt ook eisen ten aanzien van processen en het netwerk waarop deze systemen acteren.
Stichting RijnmondNet slaat geen beelden en/of verslagen op: deze informatie blijft bij het bron ziekenhuis.
Voor wat betreft het uitwisselen van beelden via XCA (XCA-I) dient zowel RAD-69 als WADO-WS te worden ondersteund door de XCA(I) Source. Als dit niet het geval is, dient contact opgenomen te worden met RijnmondNet voor de mogelijkheden.

Afspraken architectuur, (test-)/acceptatie- en productieomgeving

Algemene afspraken met betrekking tot architectuur:

- Alle XDS gerelateerde transacties over de Stichting RijnmondNet infrastructuur worden centraal gelogd bij Stichting RijnmondNet in een ATNA Repository.
- Aangesloten zorginstellingen zijn tevens verantwoordelijk voor het loggen van de door hen uitgevoerde transacties van alle betrokken systemen naar de RijnmondNet ATNA Repository.
- Stichting RijnmondNet verzorgt rapportages over de centrale logging van de *productieomgeving*, welke tot doel hebben misbruik en technische fouten op te sporen.
- Zo nodig kunnen centrale logginggegevens van de *productieomgeving* worden aangeleverd aan een zorginstelling.
- Op aanvraag kan een specifieke persoon binnen een zorginstelling directe read-only toegang krijgen tot de centrale logginggegevens van de *testomgeving.* Dit in het kader van inzage van testresultaten.
- Een check op meegeleverde metadata bij beelden en documenten zal op centraal niveau, de Register van Stichting RijnmondNet, plaatsvinden.
- Wanneer een zorginstelling de benodigde XDS-componenten betrekt van een leverancier voor plaatsing in de eigen zorginstelling, is deze zorginstelling zelf verantwoordelijk voor het aangaan van een SLA (service level agreement) hiervoor met de betreffende leverancier.
- Voor "previewen" van beelden via XCA is WADO (web access to DICOM objects) of de RAD-69 transactie niet toereikend. De afspraak is om hiervoor het WADO-WS protocol te gebruiken. Ondanks dat deze (nog) niet door IHE in het XCA-I profiel is opgenomen.

Afspraken met betrekking tot test- en acceptatieomgeving

De testomgeving en de acceptatieomgeving van Stichting RijnmondNet hebben als doel om de communicatie (transacties) van aangesloten systemen (actoren) van de zorginstellingen te kunnen testen. Deze omgeving is volledig losgekoppeld van de productieomgeving.

Stichting RijnmondNet biedt binnen de testomgeving de volgende onderdelen aan (zie overzicht Bijlage 2):

- Test Registry, voor het aanmelden van metadata van testbestanden;
- Test XCA-gateway, voor het kunnen queryen;
- Test audit (ATNA) repository, voor het loggen van alle testtransacties;

Afspraken met betrekking tot Productieomgeving

De productieomgeving is de omgeving voor de dagelijkse uitwisseling van beelden en documenten in de praktijk. Voordat een zorginstelling hierop kan aansluiten moet deze eerst succesvolle testresultaten hebben behaald met de systemen op de acceptatieomgeving. Alle aspecten met bettrekking tot het testen staan beschreven in hoofdstuk 6.

Voor de productieomgeving biedt Stichting RijnmondNet de volgende onderdelen aan:

- Registry
- XCA-gateway;
- Audit (ATNA) repository

Elke aansluiting betekent een project van implementatie. Na het in productie gaan van de aansluiting, komt deze in beheer bij Stichting RijnmondNet en haar partners. In de beheerfase is er een andere organisatievorm gericht op beheer en changemanagement. In hoofdstuk 4 staat de Governance uitgewerkt en in hoofdstuk 5 het beheer en onderhoud.

Implementatieafspraken

Wanneer een zorginstelling wil koppelen aan de centrale infrastructuur gelden de volgende afspraken:

- Aanvragen kunnen worden ingediend bij de manager operations van Stichting RijnmondNet. Zie contactgegevens in bijlage 4.
- Het bestuurlijk overleg van Stichting RijnmondNet beslist over de aanvraag.
- Voordat een project van start gaat, moet zijn voldaan aan de voorwaarden zoals beschreven in dit document.
- De zorginstelling ontwikkelt een projectplan op basis van het standaard projectplan en stemt dit af met Stichting RijnmondNet die de rol vervult als leverancier van de centrale infrastructuur.
- Ondertekening van de overeenkomst tussen Stichting RijnmondNet en de zorginstelling.
- Ondertekening van overeenkomst met andere aangesloten zorginstellingen voor gegevensuitwisseling.
- Configureren en testen.
- In productie nemen van de aansluiting.

De zorginstelling draagt zelf alle kosten van de eigen XDS-voorzieningen, inclusief de kosten voor testen en aansluiten aan de zijde van de zorginstelling.

Het proces van het aansluiten op de Beelden- en documentenuitwisseling van Stichting RijnmondNet omvat voor een zorginstelling een aantal projectstappen. In "**Fout! Verwijzingsbron niet gevonden.**" is een stappenplan voor aansluiting op hoofdlijnen beschreven.

Privacy en Security

Uitgangspunten

Gegevensuitwisseling verloopt bij voorkeur over de door Stichting RijnmondNet aangeboden infrastructuur. Hierbij wordt gebruik gemaakt van een gesloten glasvezelnetwerk (ZSP Netwerk). Daarnaast is het mogelijk om als zorginstelling via een beveiligde verbinding (VPN), via een eigen provider, een connectie te maken met de RijnmondNet infrastructuur. (Dit gaat via Change Management van RijnmondNet)
Ter bescherming van privacy van patiënten en om te voldoen aan de wettelijke vereisten, moeten Stichting RijnmondNet en zorginstellingen voldoen aan een combinatie van beveiligingsmaatregelen. Dit betreft in hoofdlijnen:

- Een beveiligde verbinding tussen de RijnmondNet centrale infrastructuur en de XDS-infrastructuur van de zorginstelling.

- Gegevensuitwisseling verloopt o.b.v. een TLS sessie. Gebruik van server-certificaten zijn verplicht voor de systemen gebruikt bij gegevensuitwisseling over de RijnmondNet infrastructuur.
  In bijlage 8 zijn de RijnmondNet publieke certificaten voor de Acceptatie- en Productieomgeving terug te vinden.
- Beveiligingsmaatregelen met betrekking tot de toegang tot patiëntgegevens. Uitwisseling van patiëntgegevens is uitsluitend toegestaan op basis van een gevalideerd Burger Servicenummer (BSN) en alleen wanneer de patiënt toestemming heeft gegeven.
- Patiënt Toestemming: Elke zorginstelling die documenten publiceert, dient ervoor zorg te dragen dat er ook BPPC-documenten worden gepubliceerd in de RijnmondNet omgeving die aangeven wie er toegang heeft tot het patientendossier.
- Audit Logging: wie heeft wat wanneer opgevraagd, ingezien, aangemeld en/of gedownload voor welke patiënt.

In de volgende sectie (‘Algemene beveiligingsmaatregelen’) wordt hier in detail op in gegaan.

Stichting RijnmondNet voldoet aan de huidige wet- en regelgeving zoals beschreven in de WBGO, Wet Bescherming Persoonsgegevens en NEN 7510, 7512 en 7513.

Om te voldoen aan de wettelijke eisen (WBP) sluit Stichting RijnmondNet een bewerkersovereenkomst af met haar leverancier(s).

Algemene technische beveiligingsmaatregelen :

Voor het uitwisselen van gegevens over de Beelden- en documentenuitwisseling, zijn de volgende maatregelen ten opzichte van de beveiliging bij alle betrokken partijen van kracht:

- Gegevensuitwisseling van zorginstellingen via de Beelden- en documentenuitwisseling verloopt bij voorkeur via een directe koppeling met de RijnmondNet infrastructuur. Als alternatief is het mogelijk om als zorginstelling met een andere leverancier een beveiligde verbinding, VPN, met de RijnmondNet infrastructuur op te zetten. De zorginstelling is zelf verantwoordelijk voor deze aansluiting en de bijbehorende kosten.
- Systemen die via de Beelden- en documentenuitwisseling communiceren, doen dit op basis van tweezijdig geauthentiseerde TLS-verbindingen en uitsluitend op basis van UZI-servercertificaten.
- Firewall:
  - IP-adres filtering: Het configureren van IP-adressen van Stichting RijnmondNet en de overige zorginstellingen binnen het Affinity Domain vindt plaats in de desbetreffende firewalls. Dat betekent blokkering bij communicatie vanuit een onbekend IP-adres. Zorginstellingen leveren de benodigde IP-adresgegevens aan Change Management van Stichting RijnmondNet aan.
  - Voor toegang tot de Beelden- en documentenuitwisseling Gateway en Registry server wordt gebruik gemaakt van één toegangspunt (‘chokepoint’).
  - Maakt gebruik van redundantie (‘Defense in Depth’).
  - Met gebruik van verschillende soorten van beveiligingsmiddelen (‘Diversity of Defense’).
  - Wanneer een beveiligingsmiddel faalt, zal geen toegang worden verleend (‘Failure Mode’).

    - Gebruik van 'statefull inspection'. Hierdoor is de toegang tot bepaalde onderdelen van het systeem beperkt en kan ook het systeem zelf maar op bepaalde manieren zijn informatie kwijt.
- Beschikbare beveiligingsupdates van alle relevante software, anti-malware en de noodzakelijke updates van besturingssystemen worden zo snel mogelijk geïnstalleerd.
- Authenticatie:
    - Voor toegang (Query) tot de Beelden- en documentenuitwisseling Registry door geautoriseerde gebruikers is een UZI-zorgverlenerspas of UZI-pas op naam vereist. Registratie van UZI-pasgegevens vindt plaats bij Stichting RijnmondNet; zonder registratie is toegang tot de Beelden- en documentenuitwisseling registry niet mogelijk. Groepspassen of passen "niet op naam" zijn niet toegestaan.
    - Authenticatie vindt plaats in de Consumers. Er dient in het XUA-token richting Rijnmondnet *een of meer rollen* mee gegeven te worden (ipv alleen een Serienummer) waarop gecheckt kan worden of een gebruiker toegang heeft tot Rijnmondnet. Bij de projectwerkzaamheden van Rijnmondnet worden voor deze rol toegangsregels toegevoegd.
- Autorisatie:
    - Voor toegang tot de Beelden- en documentenuitwisseling registry wordt gewerkt met een rollen/rechten structuur waarmee geautoriseerde gebruikers uitsluitend toegang krijgen tot delen van de applicatie waar zij toe gerechtigd zijn. Transacties vinden daarbij plaats op basis van het XUA-profiel.
    - Zij krijgen alleen die informatie te zien waar patiënten toestemming voor hebben gegeven.
- Patienttoestemming: zie paragraaf 4.4
- Logging: alle transacties die plaatsvinden binnen de Beelden- en documentenuitwisseling worden t.b.v. auditing geregistreerd. Dit is conform de specificaties van IHE ATNA. Hierbij gaat het om het loggen van zaken zoals welke gebruiker wat, wanneer heeft aangemeld, opgevraagd en of gedownload.
  Stichting RijnmondNet beheert hiervoor een centrale logging.
  Een zorginstelling is verplicht om een lokale logging van de transacties bij te houden.
- Stichting RijnmondNet en de aangesloten zorginstellingen voeren eenmaal per jaar een audit van hun eigen systemen en bijbehorende procedures uit.

Fysieke toegang: de systemen ten behoeve van de gebruikers staan in de beveiligde ruimte en zijn niet zonder begeleiding van een bevoegd persoon toegankelijk. Elke toegang tot de ruimte wordt geregistreerd.

Toestemming patiënt

Ten aanzien van de toestemming (consent) van de patiënt voor het delen van medische gegevens via de Beelden- en documentenuitwisseling, gelden de volgende afspraken.

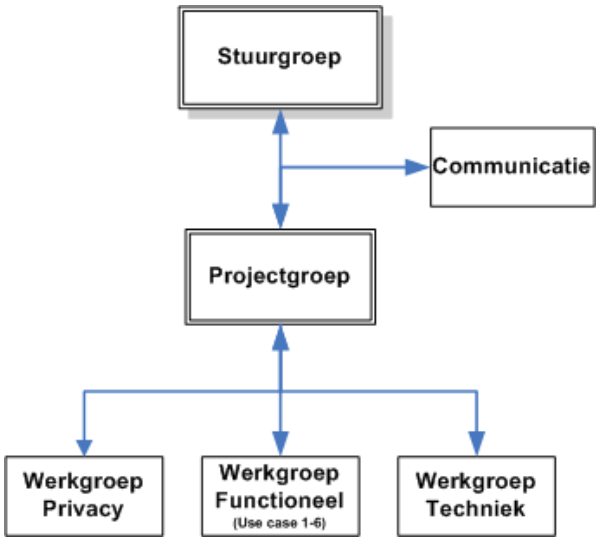
Patiënt Consent:

- De toestemming van de patiënt voor digitale uitwisseling van zijn/haar gegevens wordt vastgelegd in een BPPC (Basic Patient Privacy Consent) document. De patiënt geeft zowel toestemming voor aanmelden als het opvragen van gegevens.
- De zorginstelling slaat dit BPPC-document lokaal op in de eigen Repository en meldt het aan bij de centrale (RijnmondNet) registry;

Beschikbare policies voor het BPPC-document (deze moeten in de eventcodes worden gezet)

Bijlage 5: Voorbeeld aanpak XDS project

Voor de realisatie van een XDS-project conform de bovenstaande stappen is een projectorganisatie gewenst. De verwachting is dat binnen een XDS-project minimaal de onderstaande structuur benodigd is, indien gewenst kunnen groepen gecombineerd dan wel uitgebreid worden. De beschreven projectstructuur is gebaseerd op de Prince 2 methodiek.



Stuurgroep XDS

Vanuit de opdrachtgevers wordt een stuurgroep voor het project geformeerd.

Naam	Organisatie
	Medisch specialist (voorzitter)
	Projectleider XDS implementatie
	Projectleider instelling A
	Projectleider instelling B
	Projectleider leverancier
	Senior gebruik (zorgverlener)

Afhankelijk van fase van het project (proces t.a.v. use case) kan de stuurgroep worden aangevuld met de bedrijfskundig manager vanuit de instellingen. De stuurgroep is verantwoordelijk voor de besluitvorming t.a.v. de wijze waarop XDS in gebruik wordt genomen. Om deze primaire verantwoordelijkheid te kunnen uitvoeren moeten de leden op de hoogte zijn van organisatorische ontwikkelingen binnen de eigen instelling op het gebied van XDS-infrastructuur en de zorgprocessen om sturend te kunnen zijn in de projectmatige aanpak van het project XDS in de regio.

De stuurgroep is verantwoordelijk voor de volgende aspecten / beslissingen:

- Afhandelen van issues, knelpunten en risico's
- Kanaliseren van strategische vraagstukken;
- Afhandelen van (grote) wijzigingen in scope, planning, resources of kwaliteit;
- Afstemming met andere projecten die raakvlakken hebben met het XDS-project;

Bij calamiteiten kan de projectleider besluiten om de stuurgroep bij elkaar te roepen om zaken te bespreken.

Projectgroep

De projectgroep zorgt voor de uitvoering van het project en is verantwoordelijk voor de dagelijkse gang van zaken.

Naam	Organisatie
	Projectleider XDS-implementatie (voorzitter)
	Projectleider leverancier
	Voorzitter werkgroep Privacy
	Voorzitter werkgroep Techniek
	Voorzitter werkgroep Implementatie
	Projectleider RSO

Binnen de projectgroep worden de lopende issues en de projectrisico's besproken en afgehandeld. Voortgang van de issues en de risico's worden gemeld aan de stuurgroep. Indien er problemen aanwezig zijn die binnen de instellingen opgelost dienen te worden en tot stagnering van het project leiden worden deze ook gemeld aan de stuurgroep. Vanuit de projectgroep wordt een procedure afgesproken met de leverancier m.b.t. issue- en wijzigingsmanagement.

Projectleider

De projectleider bewaakt de in- en externe deadlines, de voortgang van de werkzaamheden van de projectorganisatie en legt verantwoording voor het eindresultaat af aan de stuurgroep. De projectleider stemt de aanpak, het verloop en overige zaken af met de projectleiders van de instellingen en de leverancier. De instellingen zijn zelf verantwoordelijk voor het uitwerken en sturen van hun (deel)project en het bereiken van het afgesproken resultaat.

De projectleiding:

- Voorziet het projectteam van visie, leiding en ondersteuning;
- Bereidt het Project Initiatie Document met een mijlpaalplanning voor, ter goedkeuring van de stuurgroep;
- Stelt activiteiten en resultaten per fase op en wijst deze toe aan individuele projectleden;
- Stemt planning en activiteiten af met de verschillende (deel)projectleiders;
- Stuurt het overallproject naar de beoogde resultaten;
- Bewaakt voortdurend de scope van het project;
- Bewaakt voortdurend de projectvoortgang, met in achtneming van de mijlpaalplanning;
- Identificeert ingrijpende veranderingen op het PID (project initiatie document) en de projectplanning en bereidt wijzigingsvoorstellen aan de stuurgroep voor;
- Draagt zorg voor issue en risicomanagement in het project.

Projectleden

Projectleden zijn verantwoordelijk voor activiteiten en resultaten die toegewezen zijn door de projectleiding. Als team hebben zij een gezamenlijke verantwoordelijkheid om het project

tot een goed einde te brengen. Ieder lid is een vertegenwoordiger van het project richting de organisatie.
De interne projectleden dienen de volgende vaardigheden in te brengen:

- Kennis van de eigen organisatie;
- Kennis van de processen in de keten;
- Kunnen aangeven van systeemrelevante informatie;
- Gevoel voor IT zonder dat zij technisch van aard zijn;
- Communicatief sterk;
- Gedrevenheid en doorzettingsvermogen met een positieve en constructieve benadering.

Werkgroep Privacy

Vanuit de deelnemende instellingen nemen de security officers deel aan de werkgroep privacy, samen met de interne projectleiders . Indien gewenst wordt de werkgroep uitgebreidt met deskundige zorgprofessionals.

Naam	Organisatie
	Projectleider (voorzitter)
	Security officer instelling A en/of B
	Functionaris gegevensbescherming instellingen A en/of B
	Jurist instelling A en/of B

Werkgroep Techniek

Vanuit de deelnemende instellingen nemen de technische professionals deel aan de werkgroep techniek om met name de afspraken t.a.v. de regionale inbedding en de daarmee gepaard gaande lokale afspraken vast te leggen. De werkgroep wordt voorgezeten door de projectleider

Werkgroep Functioneel (use case….)

Per use case wordt afhankelijk van het specifieke proces van de use case, een werkgroep ingesteld met procesdeskundigen vanuit beide zorginstellingen. Iedere use case zal starten met een kick-off waarin de uitgangspunten en het faseplan per use case wordt besproken.

Werkgroepen per instelling

Voor het XDS-project is een aantal werkgroepen ingericht. De werkgroepen zijn verantwoordelijk voor de uitvoering van opdrachten die zij via projectgroep of de projectleiding krijgen toegewezen. Binnen de werkgroepen in de instellingen ligt de focus op de vraag op welke wijze de interne bedrijfsprocessen moeten worden aangepast m.b.t. digitaal ontvangen van de overdracht en de technische zaken m.b.t. ICT-infrastructuur. Deelnemers aan de deelprojecten per ziekenhuis zijn tenminste de deelnemers uit de projectgroep XDS. De projectleiders per ziekenhuis zijn verantwoordelijk voor de verdere organisatie en invulling hiervan.

Overlegstructuur

Naam	Frequentie
Stuurgroep	Verschilt per situatie, maar minimaal bij start en oplevering en indien nodig ook tussendoor.
Projectgroep	2-wekelijks / maandelijks

Werkgroep Privacy	2-wekelijks / maandelijks
Werkgroep Techniek	2-wekelijks / maandelijks
Werkgroep Functioneel (use case ..)	2 wekelijks
Werkgroep per instelling / use case	Afhankelijk van de detailplanning per fase wordt bekeken met welke frequentie een werkgroep bijeenkomt.

Rapportage structuur

Periodiek wordt over de voortgang gerapporteerd gebaseerd op het plan van aanpak (advies: conform Prince2, dus "management by exception"). De projectleider rapporteert aan de stuurgroep, projectgroep en andere stakeholders. De projectleiders van de instellingen en leveranciers(s) informeren hun eigen organisatie.

Risicomanagement

In het kader van risicobeheersing worden maatregelen voorgesteld om de risico's te verkleinen dan wel voorzieningen te treffen indien ze alsnog optreden. In dit kader worden door de projectleiders de volgende 'logboeken' bijgehouden:

- Risico logboek: hierin worden alle knelpunten en risico's opgenomen. Daarbij wordt beschreven welke acties zijn genomen en wat de gevolgen zijn voor wat betreft de voortgang, planning en het budget;
- Issue-logboek: hierin worden alle vragen, opmerkingen, zorgpunten, foute aannames, requests for change, e.d. opgenomen. Daarbij wordt beschreven welke acties zijn genomen en wat de eventuele consequenties zijn voor wat betreft voortgang, planning en budget;

De projectrisico's worden gemanaged door de projectgroep.

Request For Change procedure

In deze paragraaf wordt een mogelijke procedure met betrekking tot het indienen van voorstel tot wijziging (request for change, rfc) bij het implementatie project beschreven.
RfC's hebben betrekking op de specificaties, aannames en uitgangspunten voor zover bekend bij de start van het project. De reden voor een dergelijke procedure is het beheersbaar maken en houden van (tijd kritische) projecten.

1. Melding

Een RfC vloeit voort uit een gewenste aanpassing op een geaccordeerd product.
Geaccordeerde producten zijn:

- De overeengekomen specificaties in de offerte.
- De overeengekomen specificaties in het Rfi
- Opgeleverde en geaccordeerde resultaten/producten.
- De aannames of uitgangspunten.
- Plan van aanpak, inclusief planning en resources/middelen

Een voorstel tot wijziging wordt door de projectmanager ingediend bij de stuurgroep.

2. Onderzoek

De RfC wordt, in opdracht van de stuurgroep, door het projectteam of leverancier in behandeling genomen. De betreffende verantwoordelijk geeft de stuurgroep een reactie met betrekking tot de consequenties die de RfC heeft voor o.a. de planning van werkzaamheden, het budget en/of de doorlooptijd van het project.

3. Besluitvorming

De stuurgroep bepaalt de impact van de RfC op scope, projectdoelstelling en risico's en neemt het uiteindelijke besluit. Voordat een wijziging wordt uitgevoerd dient hiervoor een schriftelijke opdracht gegeven te zijn door de stuurgroep.

4. Registratie en afhandeling

Alle RfC's die tijdens de uitvoering van het project worden ingediend worden door de projectleider geregistreerd (issue log) en gearchiveerd. De wijziging wordt opgenomen en verwerkt in de planning en de begroting, hierna wordt de uitvoering ter hand genomen. Alle RfC's worden gecommuniceerd naar alle betrokkenen (in aparte communicatie of via de periodieke rapportage).

Informatie en documentatie

Het projectdossier heeft tot doel alle mogelijke projectdocumentatie toegankelijk te maken. In het dossier worden de projectdocumenten gearchiveerd. Tevens worden de risico's, issues en eventuele rfc's gedocumenteerd. Voor het projectdossier wordt geadviseerd gebruik te maken van een speciale omgeving (Sharepoint, Projectplace, BizInline, etc)

Bijlage 6: Voorbeeld IHE Use Case beschrijving

Internationale IHE database Use cases
https://www.antilope-project.eu/wp-content/uploads/2013/05/D1.1-Refinement_of_Antilope_Use_Cases_v1.2.pdf

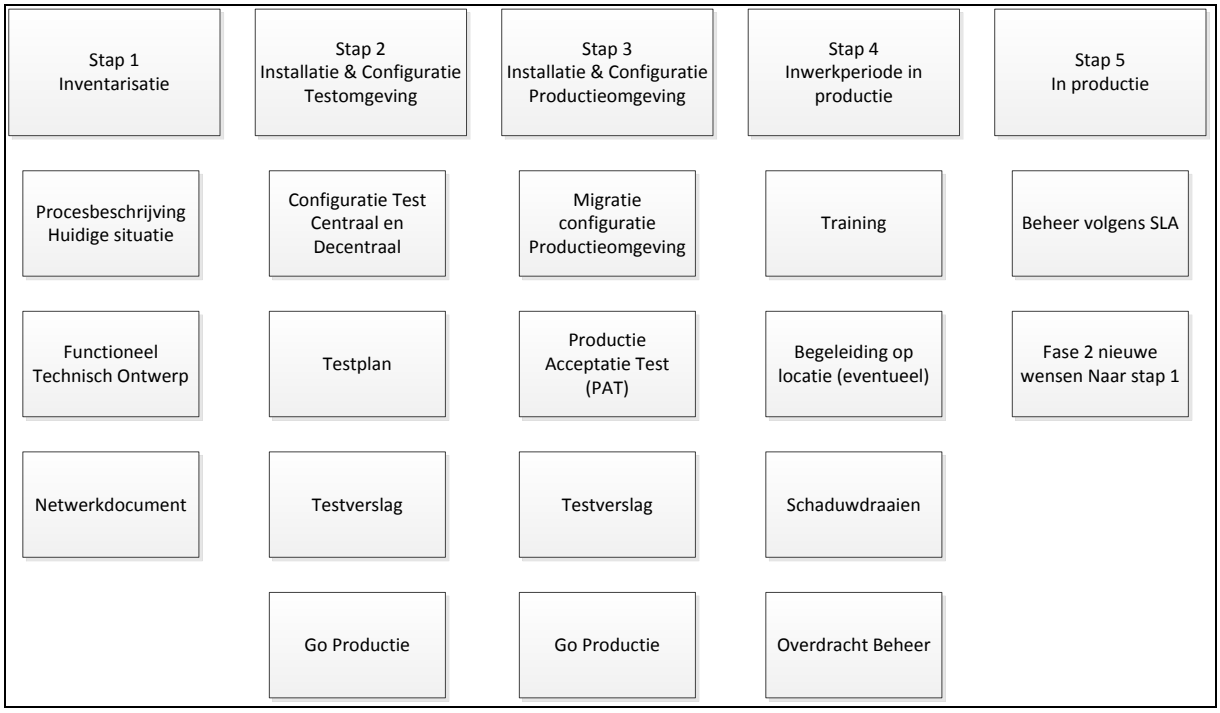
Voorbeeld van een use case beschrijving:

Primaire actor(en):	• Secretariaat Radiotherapie • Radiotherapeut • Medisch specialist • Secretariaat Poli
Beschrijving:	De medisch specialist besluit binnen een MDO dat voor de behandeling van de patiënt radiotherapie noodzakelijk is. De aanwezige radiotherapeut maakt notitie en geeft na afloop de patiëntnaam (-en) door aan het secretariaat Radiotherapie. Hiermee start het proces aanvraag radiotherapie. De Medisch specialist bespreekt uitkomsten MDO met de patiënt en na akkoord patiënt wordt de processtap, afspraak maken met de patiënt, door het secretariaat Radiotherapie in gang gezet.
Scope	De uitwerking richt zich op de aanvragen Radiotherapie die voorkomen uit de Oncologische MDO's binnen het ziekenhuis A en de aanvragen Radiotherapie zonder een MDO, dus direct vanuit een specialisme binnen het ziekenhuis B. In een 2e fase wordt beoordeeld of de ingerichte gewenste situatie voor het ziekenhuis A ook op dezelfde wijze binnen het andere ziekenhuis B gebruikt kan gaan worden. Tevens wordt de benodigde informatie voor Radiotherapie die nu op cd/dvd wordt gestuurd vervangen door de XDS-infrastructuur. Aangezien ziekenhuis C wel deelneemt aan de MDO's maar geen gebruik maakt van de RSO XDS-omgeving zal voor het ziekenhuis C de huidige werkwijze voorlopig in stand worden gehouden (als alternatief kan een web upload / image upload portaal gebruikt worden zoals sommige RSO's of zorginstellingen deze aanbieden). Doel van deze use case is het verbeteren van de aanleverprocedure van benodigde patiëntengegevens voor een aanvraag voor Radiotherapie In de huidige situatie wordt gewerkt met aanlevering op papier, telefonisch, cd/dvd, mail etc. en is vaak niet volledig en/of te laat. Voor het beheersen van de procedure om de gegevens te verzamelen is een workflow gemaakt. De aanvraag voor Radiotherapiebehandeling wordt aangemeld door de behandelend arts, in de meeste gevallen na een MDO. De aanvraag wordt door het secretariaat Radiotherapie ingevoerd in het ZIS en de voorbereidende handelingen in gang gezet. Door het niet, onjuist of te laat aanleveren van benodigde gegevens gaat

	veel tijd verloren voordat de patiënt behandeld kan worden en vergt veel resources bij Radiotherapie. Middels XDS zou het proces versneld kunnen worden. XDS kan faciliteren in het generiek klaarzetten/beschikbaar stellen van de benodigde gegevens. XDS faciliteert niet in het de workflow voor de aanvraag, controleren op aanwezigheid van gegevens, het maken van een afspraak, communicatie tussen diverse partijen, het vastleggen van verslagen. Wel zal met deze use case onderzocht worden of dat middels gebruik van XDW verbeterd kan worden.
Randvoorwaarde	Er is een werkende XDS-infrastructuur. De benodigde onderzoeken (uit-, verslagen en beelden) zijn beschikbaar binnen XDS. Patiënt heeft akkoord gegeven op het beschikbaar stellen van zijn/haar informatie via XDS. Patiënt heeft akkoord gegeven op het voorstel van de medisch specialist om Radiotherapie als behandeling te gaan uitvoeren.
Resultaat	Alle informatie die nodig is om de aanvraag radiotherapie af te ronden is snel, eenvoudig, compleet en accuraat aan te leveren. De afspraak voor de radiotherapeutische behandeling van de patiënt kan gemaakt worden.

Bijlage 7: Stappenplan Realisatie Use Case

Nadat de projectorganisatie is ingericht kan gestart worden met de realisatie van de IHE-XDS use case door de stappen te doorlopen in figuur 1.



***Figuur 1**: Stappen RSO Nederland ontwikkeling XDS use case*

Stap 1: inventarisatie

Voor het afronden van stap 1 in het stappenplan dienen de volgende acties te worden uitgevoerd:

- Het huidige proces in kaart brengen in samenwerking met de eindgebruikers.
- Het gewenste proces in kaart brengen door de mogelijkheden van XDS op te nemen in het huidige proces. Inclusief afspraken over de werkwijze van de eindgebruikers en contactpersonen van de betrokken afdelingen en zorginstellingen.
- Functioneel ontwerp opstellen van het verwijsformulier in samenwerking met de eindgebruikers.
- Het gewenste proces en het FO van het verwijsformulier bespreken met de eindgebruikers.
- Opstellen van het Functioneel Technisch Ontwerp (FTO).
- Inventarisatie van de eindgebruikers en de rechten die zij moeten krijgen. Eigen beheerorganisatie dient de aanvragen voor de uitbreiding van rechten binnen de eigen systemen bij de eigen instelling in te dienen.

Stap 2: installatie en configuratie testomgeving

In deze fase worden aan de hand van het vastgestelde Functioneel Technisch Ontwerp de testomgevingen van de decentrale en of centrale XDS-componenten ingericht en geconfigureerd. Voor het afronden van stap 2 in het stappenplan moeten de volgende acties worden uitgevoerd:

- Configureren en uitrollen van op te nemen documenten
- Indien nodig aanvullen van de centrale LDAP
- Testplan opstellen [zie hoofdstuk 12]
- Testen met applicatiebeheerders + leveranciers (technische testen)
- Testen met functioneel beheerders en gebruikers (functionele testen)
- Indienen Request for Change (RfC) bij RSO voor migratie naar productie
- Opstellen van opleidingsmateriaal
- Aanzet voor proces, formulier en communicatie toestemming patiënt
- Opstellen dataset, afspraken/toetsen metadata

Indien de acceptatietest heeft plaatsgevonden met functioneel beheer van de zorginstellingen en de projectleiders vindt er een Go/No Go moment plaats. Na het afgeven van een Go zullen de projectleiders de opgestelde RfC's indienen bij de ICT-afdelingen van de zorginstellingen. De inhoud van de RFC's is afhankelijk van de benodigde aanpassingen.

Stap 3: installatie en configuratie productieomgeving

In deze fase worden de productieomgevingen ingericht en geconfigureerd. Hierbij wordt de configuratie zoals in de testomgevingen is goedgekeurd, gemigreerd naar de productieomgevingen.

Na afloop van de acceptatietest wordt er een Go of No-Go gegeven voor de overgang naar de volgende fase. Om te komen bij het Go/No Go moment, voor het wel of niet starten van de inwerkperiode moeten de volgende acties in de productieomgeving worden uitgevoerd:

- RfC's geaccordeerd door zorginstellingen
- Migratie van de configuratie naar productie
- Preproductie acceptatie test (PAT) met applicatiebeheerders + leveranciers
- Go/No Go voor PAT (technische goedkeuring)
- Productie acceptatie test (PAT) met functioneel beheerders, PL en key users (functionele goedkeuring)
- Go/No go
- Aanpassing proces
- Opleveren beheerdocumentatie (SLA, DAP etc)
- Opleveren juridische documenten (verwerker overeenkomst, PIA etc)

Stap 4: inwerkperiode in productie

In deze fase worden de medewerkers ingewerkt op de productieomgevingen. Naast de nieuwe werkwijze op de XDS-productieomgeving wordt ook de oude manier van werken nog gehanteerd. Voor het afronden van deze laatste stap in het stappenplan moeten de volgende acties worden uitgevoerd:

- Training
- Begeleiding op locatie (eventueel)
- Schaduwdraaien
- Overdracht en acceptatie naar/door beheer

Stap 5: in productie

In deze fase worden beheerafspraken in de praktijk ingericht en volgens de SLA-afspraken uitgevoerd.
Tevens worden de lessons learned vanuit de evaluatie van het gehele project beschreven. Indien er openstaande en/of aanvullende wensen zijn kan besloten worden dit met uitbreiding van de XDS-infrastructuur of inrichting van de XDS-componenten in te vullen. Hiervoor kan een nieuw project gestart worden.

- Beheer volgens SLA
- Lessons learned, evaluatie van het gehele project
- Project beëindiging
- Indien gewenst voorstel voor nieuw project

Resultaten

Voor de realisatie van de use case worden de volgende zaken opgeleverd:

1. Plan van aanpak en sluitende afspraken met deelnemende pilotpartijen **(voorbereiding)**
2. Functioneel en technisch ontwerp XDS **(voorbereiding & ontwikkeling)**
3. XDS werkend binnen de regio **(test & acceptatie)**
4. Analyses, use cases, inclusief draaiboek/plan voor de werkgroepen **(pilot)**
5. Communicatieplan XDS **(voorbereiding, ontwikkeling, pilot en afronding)**
6. Eindevaluatierapport: **(afronding project)**
    - Met kosten en batenanalyse implementatie XDS
    - Beheermodel voor verdere exploitatie van XDS in de regio
    - Opleidingsplan gebruik XDS

Voor zover mogelijk zullen alle producten **S**pecifiek, **M**eetbaar, **A**cceptabel, **R**ealistisch, **T**ijdgebonden zijn (SMART).

Bijlage 8: IHE Koppelvlakken met bronsystemen

De EPD's zullen met name worden gebruikt om het patiëntendossier te ontsluiten in de vorm van verslagen, patiënt samenvatting, bespreekbrieven en dergelijke.
Ontsluiting kan plaatsvinden via HL7 koppelingen, waarbij gegevens worden uitgestuurd, via extractie software of via een XCA koppelingen.

VNA / PACS II

De Vendor Neutral Archives (VNA) in de diverse organisaties zullen worden ingezet om naast de radiologie beelden ook de overige beeldvormende specialismes te kunnen ontsluiten, waarbij elk ziekenhuis ondertussen in meer of mindere mate een VNA, ook wel PACS II genoemd, tot zijn beschikking heeft om te ontsluiten. Het opnemen van randvoorwaarden op het gebied van interoperabiliteit is van belang om deze na implementatie goed te kunnen koppelen aan regionale IHE-XDS infrastructuren, waarbij een XCA koppeling het meest voor de hand ligt.

Radiologie onderzoeken

Radiologiebeelden kunnen worden ontsloten door handmatig onderzoeken aan te melden bij XDS, waarbij verslagen alleen meekomen als deze als SR zijn opgeslagen in het PACS systeem. De verslagen kunnen via het RIS of EPD als HL7 ORU bericht worden aangemeld bij XDS.

Ontsluiting laboratorium gegevens

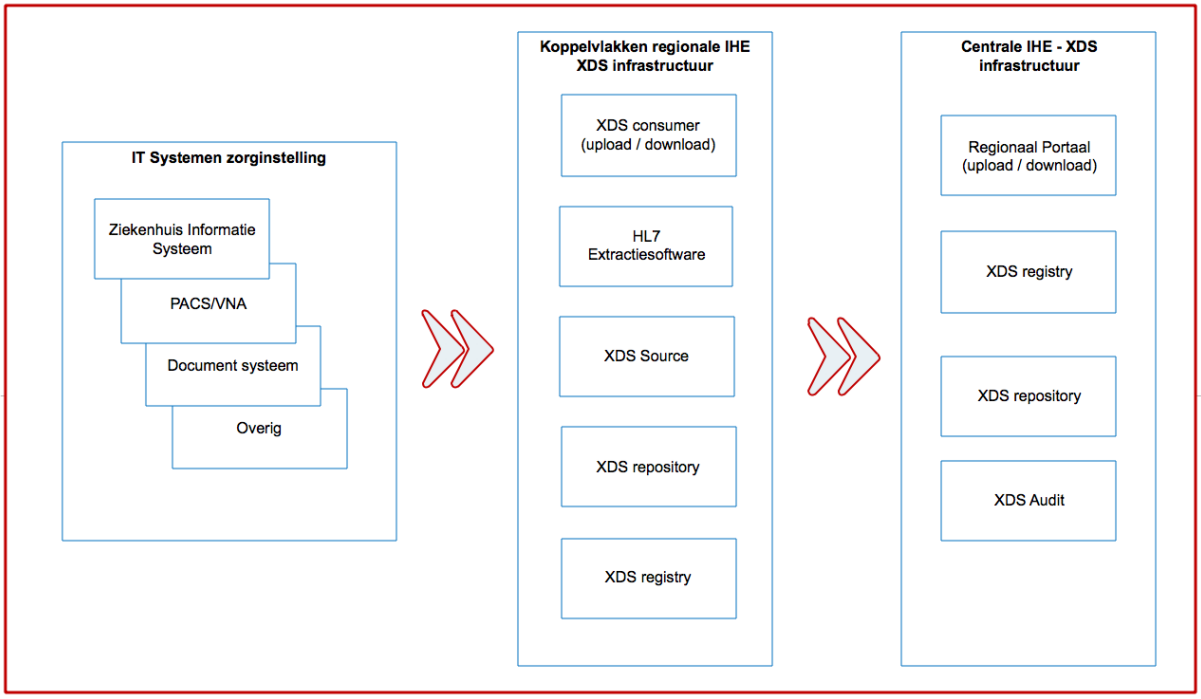
Laboratorium gegevens zijn een enigszins aparte categorie om dat deze vaak elders worden gegenereerd en onder eigendom van de aanvragende instelling vallen. Om deze te ontsluiten is het mogelijk om per ziekenhuis de laboratorium gegevens te ontsluiten, echter in tweede instantie lijkt het eenvoudiger om regionale laboratoria rechtstreeks te ontsluiten richting IHE-XDS infrastructuren, omdat deze voor bijna alle zorginstellingen in de regio diverse labonderzoeken uitvoeren.

Het is aan te raden om de ontsluiting te laten verlopen via de E-lab standaard van Nictiz, waarbij standaard HL7 CDA berichten zijn gedefinieerd. Hierbij is het wel van belang dat in eerste instantie alleen de aanvragende instelling toegang krijgt tot de lab uitslagen.

Overig

Voor overige ICT-systemen zal per geval bekeken moeten worden of deze gegevens vanuit het EPD ontsloten kunnen worden, of dat er een koppeling (b.v. HL7 ORU) gelegd kan worden met de regionale IHE-XDS infrastructuur.

Koppelvlakken zorginstelling en centrale XDS IHE infrastructuren



Bijlage 9: Technische uitwerking koppeling LSP – IHE

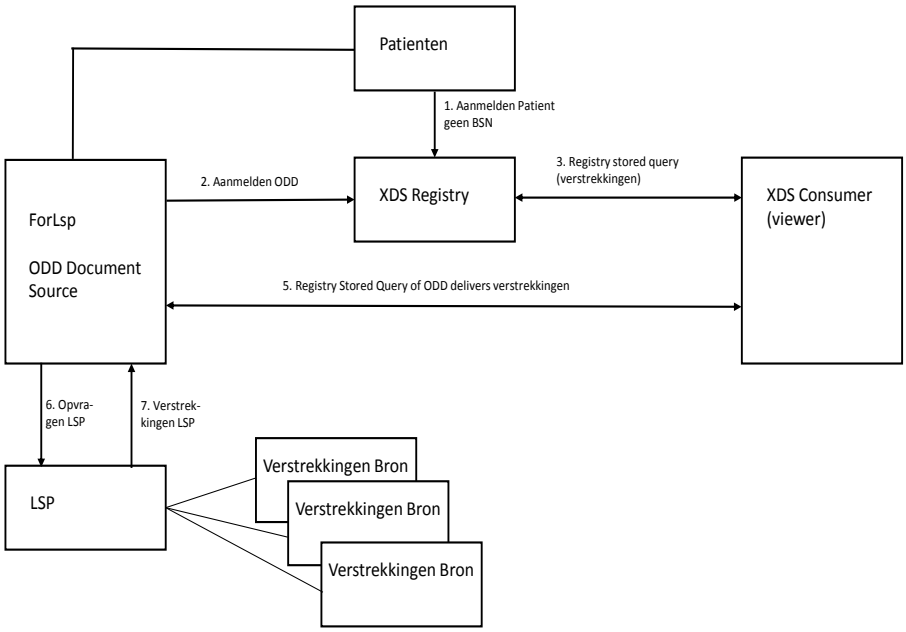
In deze bijlage wordt de koppeling tussen het LSP en een IHE-XDS infrastructuur besproken De hierna volgende informatie moet vooral gezien worden als achtergrond informatie die behulpzaam kan zijn in concrete projecten, aangezien de LSP-XDS koppeling nog verder geconcretiseerd wordt.

Bij het koppelen van LSP en XDS kunnen we twee situaties onderscheiden:

- het verschaffen van LSP gegevens door XDS;
- het verschaffen van XDS gegevens door het LSP.

In deze bijlage worden twee bridges besproken die in een Proof of Concept oplossing ingezet zijn. De hierna volgende informatie moet dan ook gezien worden als achtergrond informatie die behulpzaam kan zijn in concrete projecten.

Verschaffen LSP gegevens door IHE-XDS



Figuur 1: *Bridge die LSP medicatieverstrekkingen aanlevert aan een XDS consumer.*

Door het LSP real-time verschafte medicatiegegevens kunnen met behulp van een zogenoemde On Demand Document (ODD) Source worden getoond in een XDS consumer. Op query time wordt het LSP bericht omgezet naar XDS. Deze oplossing is in de regio Rijnmond in productie geweest, echter thans, januari 2018 wordt het niet meer klinisch gebruikt. Deze oplossing dient een geaccepteerde XIS applicatie te zijn. De UZI pas van de eindgebruiker, die de gegevens in de XDS consumer opvraagt, wordt gebruikt. Hieronder beschrijven wij de werking.

Apotheken in de regio melden verstrekkingen aan bij het LSP. De verstrekkingen kunnen worden opgevraagd met een GBZ mits de opvrager bevoegd is.

In de regio worden andere medische gegevens ontsloten met een XDS infrastructuur. Voor de verstrekkingen, die zich niet in de XDS infrastructuur bevinden, is de volgende oplossing gerealiseerd. Indien de gebruiker, die een XDS consumer (de viewer) gebruikt, medicatie verstrekkingen wil inzien, dan wordt de XDS registry bevraagd voor verstrekkingen. De registry geeft document referenties terug (3). Vervolgens vraagt de viewer de verstrekking documenten op (5) uit de XDS document source. Deze documenten bevatten niet de verstrekkingen maar parameters voor een query naar het LSP. Dit is een zogenoemd on-demand-document (ODD).

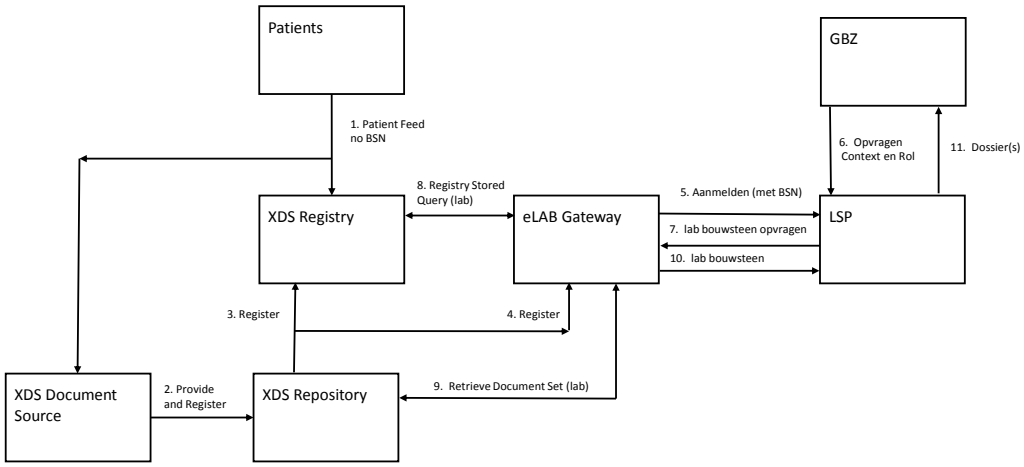
Dit ODD document wordt gebruikt om de verstrekkingen op te vragen bij het LSP (6) met authenticatie op basis van de UZI pas. Het LSP antwoordt met een HL7 V3 bericht (7). Dit bericht wordt omgezet naar het HL7 CDA format dat is afgesproken in de regionale XDS implementatie en wordt teruggegeven aan de viewer.

Omdat vooraf binnen de XDS infrastructuur niet bekend is voor welke patiënten er verstrekkingen zijn vastgelegd, is voor alle patiënten vooraf eenzelfde ODD document aangemeld bij de registry (1).

ODD is een IHE trial implementatie.
Belangrijk is op te merken dat de van het LSP verkregen gegevens niet opgeslagen worden in de XDS infrastructuur omdat de XDS infrastructuur bij toekomstige bevragingen niet dezelfde controles op rechtmatige toegang kan uitvoeren en handhaven.

In de regionale XDS infrastructuur waarvan de ODD Document source component deel uit maakt, worden patiëntgegevens verwerkt waarmee de eigenaar, RijnmondNet, gegevensverwerker in wettelijke zin is geworden. Daartoe zijn de daaruit voortvloeiende verplichtingen ingevuld.

Verschaffen XDS gegevens door het LSP



Figuur 2: Bridge die XDS labuitslagen aanlevert aan het LSP.

In de regio Utrecht is enige tijd een bridge in gebruikt geweest die zorgdroeg voor de aanlevering van lab uitslagen aan een rule engine voor medicatie veiligheid door het LSP afkomstig uit een XDS Affinity Domain. Thans loopt een project in de regio Helmond waarbij verdergaande functionaliteit wordt beoogd, zoals het triggeren van de rule engine. Onderstaand wordt de Utrechtse oplossing op basis van bouwstenen geschetst.

De eLAB standaard faciliteert laboratoriumonderzoek in de eerste lijn, zoals de aanvraag, de monsterafname en de uitslag. De berichten zijn gebaseerd op HL7 CDA R2 en ontworpen voor een XDS infrastructuur.
eLAB uitslagen kunnen opgevraagd worden bij het LSP door de inzet van de zogenaamde eLAB gateway. Deze gedraagt zich naar het LSP als een GBZ en naar een XDS infrastructuur als een Document Consumer.
Onderstaande beschrijving is gebaseerd op Aorta V8 waarin de bouwstenen zijn geïmplementeerd. De werking is als volgt, zie **Fout! Verwijzingsbron niet gevonden.**.

Bij het beschikbaar komen van een eLAB uitslag document zal deze niet alleen aangemeld worden in de XDS registry (3) maar ook aangemeld worden bij de gateway (4) met als bron de XDS infrastructuur. De gateway verzorgt de aanmelding bij het LSP.

Bij het opvragen bij het LSP van dossiers (6) geeft de gebruiker zijn rol en de context van de opvraging mee. Het LSP zal met beslisregels (SDS) bepalen dat (onder andere) alleen bepaalde labuitslagen geretourneerd worden. Vervolgens zal het LSP alle bij haar aangemelde bronnen, waaronder de gateway, bevragen voor de bouwsteen labuitslagen (7).

De gateway zal de vraag voor labuitslagen omzetten naar een query voor labuitslagen bij de registry (8). Vervolgens zal de gateway de documenten waarvan de registry de referenties

heeft geretourneerd, opvragen bij de repository. De geretourneerde CDA documenten, waarin de bouwsteen labuitslagen, worden geconverteerd naar HL7 V3 berichten met daarin *diezelfde* bouwsteen labuitslagen. Voordat de berichten naar het LSP gestuurd worden, worden de geretourneerde labuitslagen gefilterd om te komen tot alleen die uitslagen waartoe de opvrager bevoegd is. Uiteindelijk stuurt de gateway de uitslagen naar het LSP (10).

Beelden

Voor het uitwisselen van beelden is het LSP zoals het nu is ingericht niet geschikt. LSP zal met name aansluiten op IHE XDS infrastructuren, waarbij IHE-XDS-I voor nu buiten scope is geplaatst.

Bijlage 10: Templates Equipment List voor een Affinity Domain

Per IT component binnen de IHE-infrastructuur is het van belang om een goed te documenteren leggen wat de gegevens zijn van elke component en waar deze mee gekoppeld is. In deze bijlages zijn hiervoor een aantal voorbeelden gegeven.

Overzicht per instelling en IT component

Instelling	Omschrijving	Hostname	Intern IP	Extern IP	Service	Poort	Called AET
Zorginstel-ling A	PACS zorginstelling A	hostname PACS A	Intern IP adres van PACS A	Extern IP adres van PACS A	RAD-69	nr	Aangeroepen modaliteit AET
					WADO	nr	Aangeroepen modaliteit AET
Zorginstellling B	PACS zorginstelling B	hostname PACS B	Intern IP adres van PACS B	Extern IP adres van PACS B	RAD-69	nr	LUMC_SN_QR
	Viewer (optioneel)	Hostname viewer	Intern IP adres van viewer	Extern IP adres van viewer	WADO	nr	nvt
	Consumer (wanneer niet op PACS)	Hostname consumer	Intern IP adres van consumer	nvt	RAD-69 of WADO	nr	nvt
RSO	Centrale registry / repository	Hostname registry/repository	intern IP registry/ reposinory	Ext IP registry/ repository	HTTPS	8080	nvt
	PACS (webservice) (optioneel)	Hostname PACS	Intern IP PACS	nvt	WADO	nvt	nvt
	Viewer (optioneel)	Hostname Viewer	Intern IP viewer	nvt	HTTPS	nvt	nvt

Matrix IP nummers, firewall instellingen, clients (voorbeeld)

HostnameClient	Omschrijving	Intern IP	Extern IP client	Calling AET	Poort
hostname	Viewer zorginstelling B	nvt	extern IP	Vragende AET	7070
hostname	PACS zorginstelling C	nvt	extern IP	Vragende AET	7070
hostname	Viewer zorginstelling B	nvt	extern IP	nvt	nr
hostname	PACS zorginstelling C	nvt	extern IP	nvt	nr
hostname	PACS zorginstelling A	intern IP	nvt	Vragende AET	7070
hostname	Viewer zorginsteling C	nvt	extern IP	Vragende AET	8080
hostname	Consumer C	intern IP	nvt	nvt	vnt
hostname	PACS A	nvt	extern IP	nvt	nvt
meerdere gebruikers mogelijk					
Hostname	PACS zorginstelling A	nvt	extern IP	nvt	nr
hostname	Viewer B	nvt	extern IP	nvt	nr
hostname	Consumer B	nvt	extern IP	nvt	nr
hostname	Viewer webservice	intern IP	nvt	nvt	nr
hostname	Viewer RSO	intern IP	nvt	nvt	nvt

Application Entity Titles (AET)

Calling AET (aanvragend systeem)		Called AET (aanleverend systeem)			
		Zorginstelling A	**Zorginstelling B**	**Zorginstelling C**	
Calling AET	Zorginstelling A	x	Zorginstelling_B	Zorginstelling_C	**Zorginst. A**
ext. IP	196.168.1.100	x	196.168.1.130	196.168.1.160	
Port	1230	x	1232	1234	
Calling AET	Zorginstelling B	Zorginstelling_A	x	Zorginstelling_C	**Zorginst. B**
ext. IP	196.168.1.130	196.168.1.100	x	196.168.1.160	
Port	1232	1230	x	1234	
Calling AET	Zorginstelling C	Zorginstelling_A	Zorginstelling_B	x	**Zorginst. C**
ext. IP	196.168.1.160	196.168.1.100	196.168.1.130	X	
Port	1234	1230	1232	X	