RSO Nederland

Beatrijsgaarde 1
7329 BK Apeldoorn

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

Handreiking Interoperabiliteit tussen zorgverleners

15 november 2019

RSO Nederland

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

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

1 Inleiding

De zorg in Nederland is in toenemende mate multidisciplinaire keten- of netwerkzorg. De patiënt ontvangt de juiste zorg op de juiste plek: zo mogelijk thuis of bij de huisarts, zo nodig in het regionale ziekenhuis en indien noodzakelijk in een Universitair Medisch Centrum of gespecialiseerde zorginstelling. Hierbij werken zorgverleners van verschillende disciplines samen en is een goede onderlinge afstemming en informatie-uitwisseling van essentieel belang voor de patiëntveiligheid en continuïteit van zorg.

Helaas loopt een goede digitale ondersteuning van gegevensuitwisseling en procesondersteuning voor transmurale zorg, nog sterk achter bij de wensen en behoeftes van zorgverleners. Dossiers en onderzoekresultaten van patiënten worden opgeslagen in elektronische patiëntendossiers van zorgaanbieders in de 1e, 2e of 3e lijn. Deze datasilo's bij de verschillende zorginstellingen zijn momenteel nog maar beperkt in staat met elkaar te communiceren waardoor het digitaal delen van medische gegevens moeizaam verloopt. De patiënt krijgt bij een verwijzing papieren documenten en DVD's met beelden mee, de gegevens worden via de post of per fax verstuurd of informatie is gewoonweg niet beschikbaar voor andere zorgverleners. Het koppelen van zorgsystemen van verschillende zorginstellingen op basis van afgesproken standaarden, moet het delen van medische gegevens verbeteren. Interoperabiliteit, waarbij patiëntgegevens tussen elektronische zorgsystemen kunnen worden uitgewisseld en verwerkt zonder verlies van betekenis of kwaliteit van data, is hierbij voorwaarde.

Landelijk is een duidelijke versnelling te zien in de ontwikkelingen op het gebied van zorg ICT en gegevensuitwisseling tussen zorgverleners onderling en zorgverleners en patiënten. Het Informatieberaad Zorg heeft Outcomedoelen en Versnellingsprojecten gedefinieerd. In december heeft de minister van VWS in een brief aan de Kamer laten weten meer regie te nemen op gegevensuitwisseling in de zorg. Begin dit jaar is het MedMij Afsprakenstelsel en de bijbehorende standaarden voor het gebruik van PGO's door patiënten beschikbaar gekomen. Landelijk loopt er een waaier aan projecten om dit alles te implementeren, zoals: VIPP, PROVES en OPEN. RSO Nederland werkt met het programma TWIN samen met VZVZ en andere partijen aan een landelijk dekkende zorginfrastructuur om gegevensuitwisseling ook technisch mogelijk te maken.

Bij al deze projecten en initiatieven is het van groot belang de interoperabiliteit te bewaken want die komt niet vanzelf. Interoperabiliteit vereist veel overleg, afspraken en het gebruik van standaarden. Deze Handreiking geeft handvatten en een overzicht van alle verplichte, aanbevolen en optionele afspraken voor het realiseren van interoperabiliteit tussen zorginstellingen en zorgregio's om regionale en landelijk dekkende gegevensuitwisseling in de zorg mogelijk te maken. Deze Handreiking bevat veel technologie-onafhankelijke adviezen om interoperabiliteit te bereiken, bijvoorbeeld op het gebied van organisatorische afspraken en zorgprocessen, maar spitst zich toe op het gebruik van IHE-profielen waar het gaat om de technische realisatie. Het volgen van de Handreiking in een XDS implementatie is een randvoorwaarde voor interregionale interoperabiliteit.

De interoperabiliteit waarop deze handreiking zich richt, maakt het mogelijk dat een zorgverlener documenten met medische informatie, kan opvragen die daarvoor beschikbaar zijn gesteld vanuit bronapplicaties bij andere zorgaanbieders, gebruikmakend van een XDS-infrastructuur. De zorgverlener kan in zo'n geval documenten inzien en zo nodig overhalen, met een zogenoemde XDS-viewer die bij voorkeur aan te roepen is vanuit het eigen EPD. In de XDS-viewer kan genavigeerd worden naar de gewenste documenten omdat deze voorzien zijn van specifieke kenmerken, de metadata. De meeste bronsystemen beschikken naar verwachting nog niet over de gewenste IHE interfaces (zij zijn nog geen XDS source), maar zijn meestal wel met beschikbare HL7 interfaces of extractiesoftware, aan te sluiten.

1.1 Regionale Samenwerking Organisaties

In verschillende regio's in Nederland zijn Regionale Samenwerking Organisaties (RSO's) opgericht vanuit de noodzaak om gegevens in de zorg te kunnen delen. Deze RSO's verzorgen betrouwbare diensten waarover patiëntgegevens (beelden, documenten) kunnen worden gedeeld, vaak door gebruik te maken van verschillende technische infrastructuren. Om te voorkomen dat zorginstellingen en RSO's deze infrastructuren ieder op hun eigen manier tot stand brengen en inrichten, is samenwerking gezocht in de vorm van RSO Nederland. RSO Nederland (RSO-NL) is de overkoepelende vereniging van alle regionale samenwerkingsorganisaties in Nederland. De vereniging streeft naar kwaliteit van zorg voor de patiënt en bevordert standaardisatie in zorgcommunicatie voor en door haar leden (RSO NL, 2018). Deze handreiking is daar een uiting en nadere uitwerking van.

1.1.1 IHE en XDS

IHE staat voor Integrating the Healthcare Enterprise en is een internationaal initiatief waarbij in samenwerking met softwareleveranciers en zorgverleners profielen worden ontwikkeld, waarin nauwkeurig is beschreven hoe een bepaald zorgproces en de daarbij benodigde gegevensuitwisseling, digitaal kan worden ondersteund. Hiervoor worden de processen in de zorg uitgewerkt in use cases en vervolgens uitgewerkt op basis van bestaande standaarden (IHE, 2018). Dit leidt tot specificaties (IHE profielen) voor software leveranciers die beschrijven hoe de zorgprocessen het beste met standaarden ondersteund kunnen worden. Een van deze IHE-profielen is XDS (Cross-Enterprise Document Sharing) en in samenwerking met andere IHE-profielen kan hiermee een IHE-infrastructuur worden gerealiseerd om alle soorten van medische-, verpleegkundige- en paramedische gegevens uit te wisselen. IHE-XDS wordt nu nog met name gebruikt om gegevens uit te wisselen tussen ziekenhuizen, maar ook andere zorgaanbieders zoals radiotherapeutische centra, laboratoria, huisartsen, apotheken, JGZ, GGZ en VVT-instellingen kunnen gebruik maken van zo'n infrastructuur. Daarnaast bestaan er IHE-profielen om patiënten toegang te geven tot medische gegevens, toegepast binnen MedMij (2018).

1.1.2 Affinity Domain en bijbehorende afspraken

Zorginstellingen die samenwerken vormen een community. Dit heet in IHE termen een XDS Affinity Domain. Een Affinity Domain bestaat uit een groep zorginstellingen die met elkaar samen werken op het gebied van gegevensuitwisseling, op basis van gezamenlijke afspraken en een gedeelde (IHE-XDS) infrastructuur. De organisatie van Affinity Domains kent in Nederland verschillende vormen:

- Een gedeelde IHE-XDS regio waarbij een aantal zorginstellingen in een regio die zijn aangesloten bij een RSO, tezamen een Affinity Domain vormen;
- Zorginstellingen die samenwerken in een regio en tezamen een Affinity Domain inrichten zonder bij een RSO te zijn aangesloten;
- Zorginstellingen die samenwerken in een regio en zijn aangesloten bij een RSO, maar ieder een eigen Affinity Domain inrichten en die koppelen met andere Affinity Domains;
- Individuele zorginstellingen, die niet zijn aangesloten bij een RSO, die ieder hun eigen Affinity Domain inrichten en deze koppelen met andere Affinity Domains om gegevens te delen.

Deze Handreiking is van toepassing op elk van deze Affinity Domains.

Binnen een Affinity Domain is het noodzakelijk dat er afspraken gemaakt zijn tussen de verschillende deelnemende zorgorganisaties en, waar van toepassing, de RSO. Het gaat hierbij om juridische, bestuurlijke, zorginhoudelijke en technische afspraken. Deze afspraken zijn vastgelegd in een samenwerkingsconvenant, procedures en aansluitvoorwaarden. Hier moeten alle partijen zich aan houden. Op basis van deze gezamenlijke afspraken ontstaat een veilige en betrouwbare omgeving die het delen van medische gegevens binnen een Affinity Domain mogelijk maakt. Patiëntenzorg is echter niet gebonden aan een geografische regio, maar gaat over regiogrenzen (Affinity Domains) heen. De medische gegevens

moeten ook dan de patiënt kunnen volgen via aan elkaar gekoppelde Affinity Domains. Zowel binnen Affinity Domains als bij Affinity Domains die aan elkaar gekoppeld worden, is het nodig om afspraken te maken, zodat Affinity Domains juridisch, bestuurlijk, zorginhoudelijk en technisch een geheel vormen.
Dit document 'Handreiking Interoperabiliteit tussen zorginstellingen op basis van IHE' geeft een aanzet om tot zo'n gezamenlijke set van afspraken te komen.

1.2 Vraagstelling

Verschillende RSO's verlenen IHE-XDS diensten en voeren IHE-XDS projecten uit. Om elkaar te versterken en projecten te versnellen, is het gewenst kennis en ervaringen met elkaar te delen. RSO Nederland heeft hiervoor in 2017 voorstellen gedaan voor een tweetal initiatieven:

- Het doorontwikkelen van de bestaande Handreiking IHE-interoperabiliteit tot een generieke 'norm' waaraan IHE-XDS Affinity Domains moeten voldoen om aan elkaar te koppelen (Nictiz, 2015);
- Het uitwisselen van documenten, kennis en ervaringen om projecten te versnellen en de samenwerking tussen de regio's te bevorderen.

Beide initiatieven zijn opgepakt in de RSO-NL Werkgroep 'IHE Interoperabiliteit', waarin vertegenwoordigers zitten vanuit verschillende RSO's, een vertegenwoordiging van VZVZ (beheerder LSP) en ondersteuning vanuit Nictiz plaatsvindt. De werkgroep heeft als opdracht een nieuwe versie van de Handreiking op te stellen met bijbehorend toetsingskader. Daarnaast heeft de werkgroep een inventarisatie uitgevoerd van bestaande RSO-documenten en deze in de vorm van Best Practices opgenomen in deze handreiking.

1.3 Doelstellingen

De doelstellingen van deze Handreiking, het toetsingskader en de bijlagen zijn:

1. Het delen van kennis, ervaringen en best practices tussen RSO's en andere organisaties op het gebied van interoperabiliteit en bijbehorende IHE profielen om elkaar te versterken;
2. Het geven van een zo volledig mogelijk overzicht van een IHE-XDS implementatie, op alle lagen van het interoperabiliteitsmodel, dat als implementatiehandleiding kan dienen voor nieuwe XDS-initiatieven;
3. Het komen tot een eenduidige (standaard) inrichting van XDS-netwerken in Nederland ter bevordering van de interoperabiliteit tussen deze netwerken;
4. De doorontwikkeling van de Handreiking tot een toetsbare norm waaraan IHE-XDS Affinity Domains moeten voldoen voordat ze met elkaar gekoppeld kunnen worden;
5. Het stimuleren van de samenwerking tussen de RSO's en andere Affinity Domains.

De volledige Handreiking bestaat uit de volgende onderdelen:

A. De nieuwe versie van de 'Handreiking Interoperabiliteit tussen zorginstellingen op basis van IHE';
B. Een set voorbeelddocumenten, slablonen en best practices uit de verschillende RSO's voor (her-) gebruik bij regionale IHE-XDS initiatieven;
C. Een generiek toetsingskader waaraan IHE-XDS Affinity Domains moeten voldoen.

1.4 Doelgroep

Dit document is bedoeld voor bestuurders, managers, informatiearchitecten, analisten en technici die betrokken zijn bij het opzetten, inrichten en/of onderhouden van IHE-XDS Affinity Domains. Aangezien de Handreiking zowel bestuurlijke, organisatorische, zorginhoudelijke als technische aspecten belicht, kan dit document door meerdere doelgroepen worden geraadpleegd. Het interoperabiliteitsmodel is gebruikt voor de hoofdstukindeling en biedt een overzicht van de verschillende onderdelen in dit document. Het geeft

aan dat voor het opzetten van een IHE-XDS Affinity Domain, samenwerking tussen verschillende partijen en verschillende expertises nodig is en dat voldoende aandacht moet worden besteed aan alle interoperabiliteitsniveaus. Een integrale en multidisciplinaire benadering is hierbij noodzakelijk voor het slagen van een XDS-implementatie.

1.5 Scope van deze Handreiking

De IHE-profielen die onder deze handreiking vallen zijn:

1. XDS -Cross Enterprise Document Sharing;
2. XDS-i Cross Enterprise Document Sharing for Imaging;
3. XCA – Cross Community Access;
4. XCA-i - Cross community Acces for Imaging;
5. XDW – Cross Enterprise Document Workflow (optioneel);
6. XUA - Cross-enterprise User Assertion;
7. BPPC – Basic Patient Privacy Concent;
8. ATNA - Audit Trail and Node Authentication;
9. CT - Consistent Time;
10. PDQ – Patient Demographics Query
11. PIX – Patient Identifier Cross-reference
12. XCPD - Cross Community Patient Discovery.

1.6 Leeswijzer

In hoofdstuk 2 tot en met 10 wordt een overzicht gegeven van alle interoperabiliteitsniveaus met daarin adviezen en afspraken op het gebied van wettelijke verplichtingen tot en met de afspraken over gebruikte XDS-metadata. Hierbij is gebruik gemaakt van het interoperabiliteitsmodel, te vinden in bijlage 1 (Nictiz, 2018).

Vervolgens wordt beschreven welke stappen doorlopen moeten worden om te komen tot een IHE-implementatie die daadwerkelijk wordt gebruikt. Voorbereiding en procesanalyse zijn belangrijk, maar ook testmanagement en een op te zetten beheerorganisatie dienen voldoende aandacht te krijgen.

Hoofdstuk 11 beschrijft een praktisch toetsingskader waarmee elk Affinity Domain zelf kan nagaan in hoeverre er aan de landelijke richtlijn, zoals beschreven in deze Handreiking, wordt voldaan en men gereed is om met andere Affinity Domains te kunnen koppelen.

In de bijlages wordt een set aan voorbeeld documenten en sjablonen gegeven, waar RSO's en andere Affinity Domains gebruik van kunnen maken bij een XDS-implementatie.

De Handreiking biedt een landelijke set aan afspraken die het mogelijk maakt IHE-XDS netwerken op dezelfde manier in te richten zodat deze ook op elkaar kunnen aansluiten. Op deze manier komt een veilige en betrouwbare deling van patiëntgegevens tussen zorginstellingen tot stand voor een goede informatievoorziening, waarmee de patiëntveiligheid en continuïteit van de zorg verbetert.

2 Wet, regelgeving, privacy en informatiebeveiliging

De bovenste laag van het interoperabiliteitsmodel betreft de vertaling van de relevante wet- en regelgeving naar toepassing in de praktijk. Wet- en regelgeving stelt eisen ten aanzien van rechten en plichten van verschillende partijen binnen een IHE-XDS Affinity Domain. Een van die zaken is de beveiliging en afscherming van privacy gevoelige informatie. Daarnaast heeft de wet- en regelgeving invloed op inrichting van de governance. Naast wetten zijn er normen en richtlijnen die kunnen worden ingezet om aan de wetgeving te voldoen.

2.1 Ontwikkelingen in de wetgeving

De wet- en regelgeving die van toepassing is op gegevensuitwisseling in de zorg is voortdurend in beweging. Deze versie behandelt de wet- en regelgeving die geldt op 1 juli 2018. Tabel 2.1 geeft een overzicht, waarna de wetten kort worden besproken. De belangrijkste veranderingen sinds de vorige versie van de Handreiking interoperabiliteit (Nictiz, 2015) zijn:

- Vanaf 1 juli 2017 is de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) van kracht, die de Wet gebruik burgerservicenummer in de zorg (Wbsn-z) vervangt.
- Vanaf 25 mei 2018 vervangt de Algemene Verordening Gegevensbescherming (AVG) de Wet bescherming persoonsgegevens (Wbp).

Algemene Verordening Gegevensbescherming. Deze vervangt sinds 25 mei 2018 de **Wbp** (Wet bescherming persoonsgegevens)	AVG
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Deze vervangt sinds 1 juli 2017 de **Wbsn-z** (Wet gebruik Burgerservicenummer in de zorg)	Wabvpz
Wet Cliëntenrechten bij elektronische verwerking van gegevens (Noot: de bepalingen van deze wet zijn opgenomen in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg)	
Wet op de geneeskundige behandelingsovereenkomst	WBGO

Tabel 2.1: De belangrijkste wetten op het gebied van zorginformatie-uitwisseling

2.2 AVG – Algemene verordening gegevensbescherming

De AVG gaat over het beschermen van natuurlijke personen (de zogenoemde 'betrokkenen', bijv. patiënten, cliënten, medewerkers) i.v.m. de verwerking van hun persoonsgegevens en is de Nederlandse vertaling van de GDPR (General Data Protection Regulation) van de EU. De AVG heeft de Wbp vervangen m.i.v. 25 mei 2018.

Een aantal van de belangrijkste rechten van betrokkenen die onder de AVG geregeld zijn, worden hieronder puntsgewijs opgesomd. Omdat ook in de WGBO belangrijke zaken rond dossiervoering in de zorg zijn geregeld, horen er bij deze opsomming tal van nuanceringen. Deze zijn echter in het kader van deze Handreiking achterwege gelaten.

- Het recht op overdraagbaarheid van gegevens;
- Het recht om 'vergeten' te worden;
- Recht op inzage en/of een afschrift te krijgen;
- Recht op rectificatie en aanvulling;
- Het recht op beperking van de verwerking;
- Het recht met betrekking tot geautomatiseerde besluitvorming en profilering, of wel: het recht op een menselijke blik bij besluiten;
- Het recht om bezwaar te maken tegen de gegevensverwerking;
- Het recht op duidelijke informatie over wat er met de persoonsgegevens gebeurt en hoe deze verwerkt worden.

Toezicht op naleving van de AVG en eventuele sancties, vallen onder de Autoriteit Persoonsgegevens. Meer informatie is te vinden bij de Autoriteit Persoonsgegevens (https://www.autoriteitpersoonsgegevens.nl/nl).

2.3 WGBO

Deze wet bevat onder andere bepalingen rondom informatieplicht richting de patiënt, het recht van inzage in het eigen dossier, dossierplicht, recht op vernietiging en toestemmingsvereiste. De zorgverlener is verplicht de patiënt naar redelijkheid te informeren en toestemming voor een behandeling te vragen. De patiënt is verplicht de zorgaanbieder correct en zo volledig mogelijk te informeren.

Voor iedere geneeskundige behandeling, waarbij acuut ingrijpen niet direct is vereist, is mondelinge of schriftelijke toestemming van de patiënt vereist. Zonder deze toestemming kan de hulpverlener geen behandeling starten, voortzetten en mag hij medische informatie niet met een andere zorgverlener delen.

2.4 Wet Cliëntenrechten bij elektronische verwerking van gegevens

De Wet Cliëntenrechten is op 1 juli 2017 in werking getreden. Enkele wettelijke bepalingen zijn daarvan nu nog uitgezonderd: de bepalingen die patiënten het recht geeft op elektronische inzage en elektronisch afschrift en het recht gespecificeerd toestemming te geven. Deze wettelijke bepalingen treden op 1 juli 2020 in werking.

Deze wet schept de randvoorwaarden voor het veilig elektronisch delen van gegevens met andere zorgverleners. Elke zorgverlener is vanaf juli 2017 verplicht om zijn patiënten te informeren over de elektronische gegevensuitwisseling en toestemming te vragen voor het beschikbaar stellen van de patiëntgegevens via een elektronisch uitwisselingssysteem.

De belangrijkste rechten van de patiënt die in de Wet Cliëntenrechten geregeld worden, zijn in het kader van deze Handreiking de volgende:

a. Vanaf 1 juli 2020: het recht op (kosteloos) elektronische inzage in of afschrift van zijn dossier;
b. het recht op een overzicht van de logging: categorieën van gegevens die zijn verwerkt, de ontvangers of categorieën van ontvangers van die gegevens en informatie over wie de gegevens beschikbaar heeft gesteld;
c. vanaf juli 2020: Het recht om aan te geven welke categorieën van gegevens gedeeld mogen worden met welke categorieën zorgaanbieders (gespecificeerde toestemming);
d. vanaf juli 2020: het recht op een elektronisch overzicht wie bepaalde informatie in een elektronisch uitwisselingssysteem beschikbaar heeft gesteld en op welke datum en wie informatie heeft ingezien of opgevraagd en op welke datum.

De belangrijkste plichten van een zorgaanbieder bij (elektronische) gegevensuitwisseling zijn:

a. de plicht de patiënt te informeren over zijn rechten bij elektronische gegevensuitwisseling, de wijze waarop hij zijn rechten kan uitoefenen, de werking van het elektronisch uitwisselingssysteem en welke zorgaanbieders zijn aangesloten op het systeem;
b. de plicht om zijn patiënt toestemming te vragen voor het beschikbaar stellen van de patiëntgegevens via een elektronisch uitwisselingssysteem;
c. vanaf juli 2020: de patiënt het recht te geven om zijn toestemming te specificeren (zgn. gespecificeerde toestemming);
d. vanaf juli 2020: een registratie bij te houden van de door zijn patiënten verleende toestemmingen;
e. de patiënt te informeren als er een nieuwe categorie zorgverleners gebruik maakt van het door de zorgverlener gebruikte elektronische uitwisselingssysteem (bijvoorbeeld als de patiënt toestemming heeft gegeven voor uitwisseling binnen de regio en daar nieuwe zorgaanbieders bij komen);
f. het aanpassen, verwijderen, afschermen of vernietigen van medische gegevens op verzoek van de patiënt;
g. het vastleggen van de acties die betrekking hebben op het medisch dossier (logging).

Aanvullend op de Wet Cliëntenrechten worden in een Algemene Maatregel van Bestuur (AMvB) specifieke functionele, technische en organisatorische eisen aan elektronische gegevensuitwisseling gesteld. Dit is het ‘Besluit elektronische gegevensuitwisseling door zorgaanbieders’. Doordat de eisen in een AMvB staan, kan steeds worden ingespeeld op de actuele stand van de techniek.
In het kort regelt de AMvB de volgende zes verplichtingen:

a. het aanstellen van een functionaris voor de gegevensbescherming (FG);
b. het vastleggen van het beleid, waaronder het privacy-beleid, de procedures en verantwoordelijkheden rondom gebruikte elektronische uitwisselingsystemen en interne zorginformatiesystemen;
c. het zorgdragen dat gebruikte elektronische uitwisselingssystemen en interne zorginformatiesystemen voldoen aan de veiligheidseisen en zorgvuldigheidseisen van NEN 7510;
d. het zorgdragen dat overeenkomsten tussen zorgaanbieder en de verantwoordelijke van een elektronisch uitwisselingssysteem voldoen aan NEN 7510;
e. het zorgdragen dat gebruik wordt gemaakt van veilige verbindingen die voldoen aan NEN 7512;
f. het zorgdragen dat de logging van patiëntengegevens voldoet aan NEN 7513.

De genoemde NEN normen worden verderop in dit hoofdstuk beschreven.

Samenvatting

Om aan de wetgeving te voldoen, zullen elektronische uitwisselingsystemen van gegevens, waaronder IHE-XDS, zodanig aangepast en ingericht moeten worden dat zij de gespecificeerde toestemming van de patiënt kunnen ondersteunen. Daarnaast moeten die systemen functionaliteit bieden voor de patiënt:

- Om inzage te geven in de transacties die hebben plaatsgevonden op zijn gegevens: wie heeft, wanneer inzage gehad in welke gegevens in mijn dossier;
- Om inzage te geven in de toestemming die de patiënt eerder heeft gegeven en deze desgewenst aan te passen of in te trekken.

2.5 Wabvpz en het gebruik van het BSN

De *Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg* (overheid.nl, 2008) vervangt sinds 1 juli 2017 de Wbsn-z (Wet gebruik Burgerservicenummer in de zorg).

Aan de beheerder van de infrastructuur worden geen andere eisen gesteld dan die al voortvloeien uit het feit dat deze beheerder persoonsgegevens verwerkt. Wel zal een aantal eisen gesteld moeten worden aan de aangesloten systemen en organisaties.

Het document "PvE GBx Infrastructurele Systeemrollen" (VZVZ, 2018) beschrijft een aantal van deze eisen, waaronder: gebruik Fictieve BSN's, Patiëntadministratie, BSN-verificatie, WID-controle en Register Niet Ingezetenen (RNI). Ook bevat dit document de bijlage "Best Practice verifiëren BSN".

Deze paragraaf gaat nader in op het gebruik van het BSN.

2.5.1 BSN Verificatie en Validatie

Om patiënten in de zorg op een betrouwbare manier te kunnen identificeren, moeten zorgaanbieders, indicatieorganen en zorgverzekeraars het BSN verplicht gebruiken in hun administratie en bij de onderlinge communicatie over patiënten. Om geen twijfel te laten bestaan over de correctheid van het BSN worden er twee acties uitgevoerd: BSN-verificatie en BSN-validatie.

BSN-verificatie

Bij de BSN-verificatie wordt geverifieerd dat bepaalde persoonskenmerken , waaronder naam, geslacht en geboortedatum), bij een BSN horen. Als persoonskenmerken en BSN bij elkaar horen, spreken we van een ‘geverifieerd BSN’.

Voor de verificatie wordt gebruik gemaakt van interfaces van de SBV-Z (Sectorale Berichten Voorziening in de Zorg) die zorgen voor de ontsluiting van het BSN register en de Registratie Niet-ingezetenen.

BSN-validatie

Zodra de nieuwe patiënt voor het eerst in het ziekenhuis komt, wordt aan de hand van een geldig Wettig Identiteits Document (WID: paspoort, rijbewijs, ID-kaart) gecontroleerd of de persoon voor de balie inderdaad degene is die is- of wordt ingeschreven in het EPD. Hierdoor is vanaf dat moment sprake van een ‘gevalideerd BSN’.

Optioneel is het ook mogelijk de geldigheid van het identiteitsbewijs elektronisch te laten controleren m.b.v. een (tweede) koppeling met het SVB-Z voor de WID-controle. Dit kan men bijvoorbeeld doen als er twijfels zijn aan de geldigheid van het identiteitsbewijs. Om een BSN te valideren is deze controle stap echter niet vereist en niet alle zorgaanbieders hebben de koppeling in gebruik.

Het kan voorkomen dat het BSN-nummer van een patiënt wel bekend is binnen een ziekenhuis informatiesysteem, maar dat deze nog niet gevalideerd is aangezien een patiënt zich nog niet geïdentificeerd heeft met een identiteitsbewijs.

2.5.2 Gebruik BSN in de praktijk

Voor gebruik van het BSN bij uitwisseling van gegevens tussen verschillende zorgaanbieders, dient aan de volgende regels voldaan te worden:

1. Voordat gegevens van een patiënt gedeeld mogen worden met een andere zorgaanbieder, moet de brondossierhouder een gevalideerd BSN van de patiënt hebben. Dat wil dus zeggen dat de patiënt fysiek in de zorginstelling is geweest en dat de identiteit van de patiënt is vastgesteld aan de hand van een wettig identiteitsdocument. (N.B.: dit staat dus los van het feit dat de patiënt ook toestemming moet hebben gegeven voor het delen van zijn gegevens).
2. Voor het raadplegen en overhalen van gedeelde patiëntgegevens van een andere zorgaanbieder, is het voldoende dat de patiënt in de eigen organisatie bekend is met een geverifieerd BSN. De patiënt hoeft hiervoor dus nog niet fysiek aanwezig geweest te zijn.

In sommige gevallen, zoals een spoed verwijzing of een intercollegiaal consult, kan het voorkomen dat de patiënt nog niet bekend is in de zorginstelling die een gegevensopvraging doet. Advies is om binnen de RSO afspraken te maken dat men kan vertrouwen op de verificatie van het BSN door de zorginstelling die de medische gegevens heeft vastgelegd en aangemeld voor delen buiten de zorginstelling.

Het proces van validatie van het BSN in de opvragende zorginstelling blijft bestaan. De eerste keer dat een patiënt daar fysiek aanwezig is, geldt de reguliere validatieprocedure.

2.5.3 Uitzonderingssituaties BSN gebruik

In bepaalde situaties hebben patiënten geen of nog geen BSN maar komen ze wel in aanraking met de gezondheidszorg. Dit geldt bijvoorbeeld voor patiënten die niet woonachtig of werkzaam zijn in Nederland. Voor deze patiënten moet het mogelijk zijn om gegevens toch te kunnen delen. Daarnaast zijn bij de uitwisseling van gegevens via IHE-XDS een aantal situaties denkbaar waar geen gevalideerd BSN beschikbaar is.

Bij de invoering van het Burger Service Nummer in Nederland zijn situaties benoemd waarin communicatie mag plaatsvinden met betrekking tot een patiënt, ook als deze nog geen BSN heeft. Als door omstandigheden de identiteit van de patiënt niet kan worden vastgesteld, mag het BSN van deze patiënt niet worden gebruikt in de gegevensuitwisseling.

Als er (tijdelijk) geen BSN beschikbaar is, moeten de medische gegevens aan de hand van alternatieve persoonsgegevens (geslachtsnaam, voornamen, geboortedatum, postcode en huisnummer van het woonadres) worden vastgelegd in de zorgadministratie.

Bij afwezigheid van gevalideerde BSN's is het **advies** om binnen IHE-XDS tijdelijke BSN-nummers te gebruiken die automatisch worden gecorrigeerd (via een HL7 update) zodra het BSN gevalideerd wordt. Dit kan een tijdelijk BSN-nummer zijn of een ander nummer, zoals bijvoorbeeld het lokale patiënt nummer + ZorgorganisatieID.

2.6 Richtlijnen – EGiZ

Bij elektronische gegevensuitwisseling in de zorg ontstaan veel vragen over de interpretatie van wetten en (NEN) nomen. Deze wet- en regelgeving is daarom voor de praktijk verder uitgewerkt in de: 'Gedragscode Elektronische Gegevensuitwisseling in de Zorg' (EGiZ, dec.2016), die door de koepels van zorgverleners en RSO's gezamenlijk is opgesteld. In de gedragscode is aangegeven op welke wijze deze wetten en normen in de praktijk worden toegepast. De EGiZ gedragscode is de leidraad voor implementatie van de juridische aspecten die van toepassing zijn op (inter-) regionale uitwisseling.

2.7 Normen – NEN 7510, 7512, 7513

Om veilig met elektronische medische gegevens om te gaan heeft het Nederlands Normalisatie-instituut (NEN) een aantal normen ontwikkeld. De eerste norm die is ontwikkeld is de NEN 7510, de norm voor Informatiebeveiliging in de zorg. Deze norm is gebaseerd op de Code voor Informatiebeveiliging, de ISO-27000-serie. De NEN 7510 is voor de zorg aangevuld met NEN 7512 vertrouwensbasis voor gegevensuitwisseling en de NEN 7513 logging. De normen gelden zowel binnen als tussen de IHE-XDS Affinity Domains.

2.7.1 NEN 7510, informatiebeveiliging in de zorg (NEN 7510:2017)

De AMvB met betrekking tot elektronische gegevensverwerking door zorgaanbieders, verwijst dwingend naar het toepassen van de NEN 7510, NEN 7512 en NEN 7513. Dit heeft een aantal belangrijke gevolgen.

- De verantwoordelijke voor een elektronisch uitwisselingssysteem, draagt, overeenkomstig het bepaalde in NEN7510, zorg voor een veilig en zorgvuldig gebruik van dat elektronisch uitwisselingssysteem.
- Een zorgaanbieder draagt, overeenkomstig het bepaalde in NEN 7510, zorg voor een veilig en zorgvuldig gebruik van het elektronisch uitwisselingssysteem waarop hij is aangesloten.
- Een rechtspersoon, niet zijnde een zorgaanbieder, die een elektronisch uitwisselingssysteem beheert en in stand houdt, dient er voor te zorgen dat een van de rechtspersoon onafhankelijke organisatie na onderzoek heeft vastgesteld dat de rechtspersoon en het systeem dat hij beheert voldoen aan het bepaalde in NEN 7510 . Deze bevinding dient opgenomen te worden in een door die organisatie ten behoeve van de rechtspersoon opgesteld audit-rapport.

2.7.2 NEN 7512, Vertrouwensbasis voor gegevensuitwisseling (NEN 7512:2015)

In de NEN 7510 wordt een risicoclassificatie uitgewerkt. In de NEN 7512 zijn voor de verschillende risicoklassen minimale eisen opgesteld ten aanzien van authenticatie en identificatie. Hierbij wordt de kans afgezet tegen de gevolgen. De eisen hebben betrekking op:

- De zender (entiteit: persoon, organisatie of de informatiesystemen waarmee de informatie wordt verzonden);
- Het medium;
- De ontvanger.

Binnen deze keten bestaat een authenticatieproces: de bron moet zijn identiteit aantonen en de ontvanger moet deze identiteit kunnen controleren. Het beveiligingsniveau van de gehele keten is bepalend voor de veiligheid waarmee de informatie uitgewisseld wordt.

- De verantwoordelijke voor een elektronisch uitwisselingssysteem draagt overeenkomstig het bepaalde in NEN7512, zorg voor een veilig en zorgvuldig gebruik van dat elektronisch uitwisselingssysteem.
- Een zorgaanbieder draagt overeenkomstig het bepaalde in NEN 7512, zorg voor een veilig en zorgvuldig gebruik van het elektronisch uitwisselingssysteem waarop hij is aangesloten.
- De verantwoordelijke voor een elektronisch uitwisselingssysteem werkt met een zorgserviceprovider die is geautoriseerd op basis van overeenkomstig NEN 7512 vastgestelde criteria.
- Een rechtspersoon, niet zijnde een zorgaanbieder, die een elektronisch uitwisselingssysteem beheert en in stand houdt, dient er voor te zorgen dat een van de rechtspersoon onafhankelijke organisatie na onderzoek heeft vastgesteld dat de rechtspersoon en het systeem dat hij beheert voldoen aan het bepaalde in NEN 7512. Deze bevinding dient opgenomen te worden in een door die organisatie ten behoeve van de rechtspersoon opgesteld audit-rapport.

2.7.3 NEN 7513, logging (NEN 7513:2018)

- Het patiëntdossier vormt een wezenlijk onderdeel van de veilige zorg aan de patiënt. Voor veilige zorg is het essentieel dat gegevens in het dossier integer zijn. Daarbij bevat het dossier in de aard van de registratie zeer privacygevoelige gegevens. Om deze twee redenen, vastgelegd in wettelijke bepalingen, is het van belang om op elk gewenst moment te kunnen achterhalen wie toegang heeft gehad tot het dossier, volgens welke regels die toegang is verkregen en welke acties op de gegevens zijn uitgevoerd;
- De zorgaanbieder als verantwoordelijke voor het zorginformatiesysteem, en de verantwoordelijke voor een elektronisch uitwisselingssysteem, dragen er zorg voor dat de logging van het systeem voldoet aan het bepaalde in NEN 7513. De logging betreft de registratie van a) wie bepaalde gegevens beschikbaar heeft gesteld en op welke datum en b) wie bepaalde informatie heeft ingezien of opgevraagd en op welke datum.

2.8 Verwerkersovereenkomst

Als een zorgaanbieder, de zogenoemde 'Verwerkingsverantwoordelijke', persoonsgegevens laat verwerken[1] door een externe partij, de zogenoemde 'Verwerker', dan is de Verwerkingsverantwoordelijke wettelijk verplicht een Verwerkersovereenkomst met de verwerker af te sluiten. Een verwerker is niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens, maar heeft wel een aantal afgeleide verplichtingen voor onder meer beveiliging en geheimhouding van de gegevens. De verwerkersovereenkomst moet er voor zorgen dat verwerker voldoende waarborgen biedt ten aanzien van de technische- en organisatorische beveiligingsmaatregelen met betrekking tot de verwerking van de aan hem ter beschikking gestelde persoonsgegevens.

In een Verwerkersovereenkomst moeten in ieder geval de volgende onderwerpen aan bod komen:

- de bepaling dat de persoonsgegevens uitsluitend worden verwerkt door Verwerker op basis van schriftelijke instructie van Verwerkingsverantwoordelijke;
- geheimhoudingsplicht;
- beveiliging;
- subverwerkers;
- privacy rechten van de betrokkenen, zoals: recht op inzage, correctie, vergetelheid en dataportabiliteit;
- verwijdering van gegevens na beëindiging van de verwerkingsdiensten;
- medewerking aan audits.

Een RSO of de beheerder van de centrale componenten van een elektronisch uitwisselingssysteem, zoals IHE-XDS, is in termen van de AVG een verwerker. Zorgaanbieders die dergelijke diensten afnemen van een RSO moeten dus een verwerkersovereenkomst afsluiten met de RSO.

Als de RSO op haar beurt diensten inkoopt bij een leverancier (bijv.: een huisarts die IHE-XDS als SaaS-dienst afneemt van een RSO die deze inkoopt bij een leverancier) dan dient de RSO zelf ook weer sub-verwerkersovereenkomsten aan te gaan met de desbetreffende leverancier. Hierin zijn dezelfde verplichtingen vastgelegd als de verwerker richting verantwoordelijke heeft. Het heeft de voorkeur de

[1] Onder 'verwerking van gegevens', valt: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Model Verwerkersovereenkomst van de Brancheorganisaties Zorg te gebruiken, deze is op internet te vinden[2].

2.8.1 Data Protection Impact Accessment (DPIA)

In het Nederlands vertaald: 'Gegevens bescherming effect beoordeling'. In de dagelijkse praktijk wordt deze door vrijwel iedereen: 'Privacy Impact Assessment' (PIA) genoemd. Een PIA moet verplicht uitgevoerd worden indien een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de organisatie gegevens verwerkt. De organisatie beoordeelt zijn eigen processen en bekijkt hoe deze processen een impact hebben of zelfs tot een datalek kunnen leiden, van de persoonsgegevens die worden verzameld, verwerkt of worden opgeslagen.

Het doel van een DPIA is:

- Het vooraf de privacyrisico's van een verwerking in kaart brengen;
- Het vervolgens nemen van maatregelen om de risico's te verkleinen.

Een PIA is verplicht voor organisaties die participeren in een XDS-netwerk. Een RSO kan een PIA opstellen namens het collectief van samenwerkende zorgorganisaties.

2.9 Adviezen

- Gebruik de EGiZ Gedragscode als leidraad voor implementatie van de juridische aspecten die van toepassing zijn op (inter-)regionale uitwisseling. De richtlijnen uit de Gedragscode EGiZ worden toegepast als toetsingskader;
- Maak afspraken tussen zorginstellingen om het aangeleverde en geverifieerde BSN via IHE-XDS te vertrouwen;
- Gebruik bij het ontbreken van een BSN een tijdelijk BSN;
- Biedt de patiënt faciliteiten of functionaliteit om de toestemming vast te leggen, te wijzigen of in te trekken;
- Biedt de patiënt faciliteiten of functionaliteit om de eigen gegevens in te zien incl. de transactielog;
- Stel een PIA op;
- Betrek een FG bij het opstellen en naleven van afspraken zowel op zorginstellingsniveau als op regionaal niveau.
- Stel (verwerkers)overeenkomsten op tussen zorgaanbieder en RSO dan wel beheerders van IHE-XDS infrastructuren
- Controleer dat de Rechtspersoon die een elektronisch uitwisselingssysteem beheert en in stand houdt, NEN 7510 en NEN 7512 gecertificeerd is. Deze certificering moet aangetoond kunnen worden met een audit-rapport dat na onderzoek door een onafhankelijke organisatie is opgesteld.

3 Organisatiebeleid – governance

De afspraken over gegevensuitwisseling tussen organisaties, worden gemaakt op bestuurlijk niveau: het niveau van het organisatiebeleid. Het betreft afspraken tussen de samenwerkende organisaties: organisatie van de governance, samenwerkingscontracten, raam- en verwerkersovereenkomsten, maar ook afspraken over verantwoordelijkheden, privacy en security, toestemming, inrichting van de infrastructuur en dergelijke.

[2] https://www.brancheorganisatieszorg.nl/nieuws_list/modelverwerkersovereenkomst-voor-de-zorgsector/

3.1 Noodzaak organisatiebeleid

Het maken van afspraken tussen zorginstellingen, tussen zorginstellingen en RSO's, maar ook tussen regio's, is belangrijk om het geheel te laten werken en daadwerkelijk medische gegevens met elkaar te kunnen uitwisselen. Als er geen afstemming heeft plaatsgevonden, kan de ene zorginstelling bijvoorbeeld eenmalig een brede toestemming van de patiënt vastleggen en iedereen dezelfde rechten geven om gegevens uit te wisselen, terwijl een andere zorginstelling, per uitwisseling toestemming vastlegt en verschillende rollen en rechten vastlegt voor eindgebruikers. Een andere mogelijkheid is dat in een regio uitgebreide trainingen worden gegeven met voorlichting over welke gegevens hoe kunnen worden uitgewisseld, terwijl in een andere regio gebruikers een handleiding krijgen en niet op de hoogte worden gebracht van de mogelijkheden. In beide gevallen zal het moeilijk worden om op een uniforme manier medische gegevens tussen zorginstellingen en regio's uit te kunnen wisselen. Het resultaat zal vermoedelijk zijn dat er geen- of niet optimaal gebruik wordt gemaakt van de mogelijkheden en zorgverleners terug grijpen naar oude manieren om gegevens uit te wisselen zoals CD, fax en post.

3.2 Functie Regionale Samenwerkingsorganisatie's (RSO)

RSO's kenmerken zich doordat zij met mandaat van zorgaanbieders in de regio, communicatie en gegevensuitwisseling faciliteren en daarmee de samenwerking in de zorg versterken. Zij hebben het vermogen om zorgaanbieders te verbinden, op het niveau van infrastructuur en applicaties, maar ook op dat van werkprocessen, organisatie en bestuur. Hierdoor hebben RSO's een belangrijke rol om samenwerkingsafspraken tussen deelnemende partijen op te stellen en af te stemmen.

RSO's dragen ook bij aan kennisontwikkeling, voeren projecten uit, kopen centraal producten en diensten in en beheren regionale netwerken. In het belang van de patiënt dragen RSO's op efficiënte wijze bij aan de continuïteit en kwaliteit van de zorg (2018, RSONL). Een RSO heeft daarom een belangrijke taak om samenwerkingsafspraken tussen deelnemende partijen op te stellen en af te stemmen. De RSO's scheppen, door het hanteren van de richtlijnen in dit document, een belangrijke randvoorwaarde voor interregionale uitwisseling. Zij dragen er zorg voor dat de overeenkomsten die zij in de regio opstellen ook buiten de regio gebruikt kunnen worden.

3.3 Affinity Domain en samenwerkingsafspraken

In deze paragraaf worden de benodigde documenten die nodig zijn voor de samenwerking tussen zorginstellingen en Affinity Domains benoemd. Deze documenten zijn bruikbaar voor alle verschillende organisatievormen waarin Affinity Domains voorkomen:

- Individuele zorginstellingen met een eigen Affinity Domain dat is gekoppeld aan één of meer andere Affinity Domains;
- Verschillende zorginstellingen die samenwerken binnen één Affinity Domain waarbij dat domain ook weer gekoppeld kan zijn aan andere domains;
- Beide hierboven genoemde organisatievormen met of zonder de aanwezigheid van een RSO.

3.3.1 Samenwerkingsconvenant

In een samenwerkingsconvenant worden de afspraken vastgelegd die zorgorganisaties met elkaar maken als zij samenwerken op het gebied van digitale gegevensuitwisseling zoals dat het geval is in een Affinity Domain of door middel van gekoppelde Affinity Domains. In het samenwerkingsconvenant worden alle deelnemende organisaties genoemd en worden hun rollen en verantwoordelijkheden vastgelegd. Vanuit dit document wordt onder meer verwezen naar verwerkersovereenkomsten, waarin afzonderlijke afspraken tussen zorginstellingen en het RSO worden vastgelegd.

In bijlage 2 is een voorbeeld template beschikbaar.

3.3.2 Dienstverleningsovereenkomst (DVO)

In een DVO (of Service Level Agreement – SLA) zijn de afspraken beschreven die behoren bij de operationele IHE-XDS dienstverlening welke geleverd wordt door de RSO of door de leverancier aan de zorgaanbieders als service voor de regio.

3.3.3 Dossier Afspraken en Procedures (DAP)

In het DAP zijn voor de IHE-XDS dienstverlening meer specifieke afspraken opgenomen aanvullend op de DVO. (In bijlage 3 is een template voor een gecombineerde DVO en DAP opgenomen).

In de DAP dienen de volgende zaken te zijn opgenomen:

- WAT spreken we samen af? Bijvoorbeeld het aanvragen van changes;
- HOE worden deze afspraken nageleefd? Bijvoorbeeld door termijnen op te hangen aan verwerking/aanpassing op changes;
- HOE werken de partijen samen (op operationeel en tactisch niveau)? Bijvoorbeeld het invullen van de taakverdeling tav het doorvoeren van changes;
- Namen, adressen en bereikbaarheidsgegevens van de verschillende betrokken partijen.

3.3.4 Aansluitdocument

Het aansluitdocument beschrijft alle technische en organisatorische voorzieningen, voorwaarden en condities die aan een zorginstelling gesteld worden, voordat zij mogen aansluiten bij een Affinity Domain. Bijvoorbeeld IP-configuratie, loggingsvoorzieningen en toepassing van de privacy en security richtlijnen (bijlage 4).

3.4 Aansluitproces nieuwe participanten op Affinity Domain

Wanneer een zorginstelling wil aansluiten op de infrastructuur van een bestaand Affinity Domain, dan kan de volgende procedure worden gevolgd:

- Indienen van een aanvraag voor aansluiting bij een RSO;
- Het bestuurlijk overleg van een RSO beslist over de aanvraag;
- Voordat een project van start gaat, moet zijn voldaan aan de aansluitvoorwaarden;
- Ondertekening van het contract tussen de zorginstelling en de RSO die de rol van leverancier vervult van de XDS-infrastructuur;
- Ondertekenen van de samenwerkingsconvenant met andere aangesloten zorginstellingen voor gegevensuitwisseling;
- Beschrijving van de use case. Hierin is beschreven voor welk specialisme of type gegevens de gegevens uitwisseling zal gelden. Inclusief beschrijving van het proces van de gebruikers;
- De zorginstelling ontwikkelt een projectplan (zie voorbeeld projectaanpak bijlage 5) en stemt dit af met de RSO;
- Configureren en testen van de aansluiting;
- In productie nemen van de aansluiting.

3.5 Adviezen

- Maak voor het vastleggen van afspraken tussen de samenwerkende zorginstellingen, gebruik van de best practices en templates die binnen de verschillende Affinity Domains reeds in gebruik zijn (en die als bijlage bij deze Handreiking zijn toegevoegd).
- Zorg er voor dat, voorafgaand aan de daadwerkelijke uitwisseling van medische gegevens, tenminste de volgende documenten beschikbaar zijn:

    - het samenwerkingsconvenant;
    - een SLA en bijbehorende DAP;
    - het aansluitdocument.
- Doorloop het aansluitproces voordat een nieuwe participant op het Affinity Domein aansluit.

4 Zorgprocessen en use cases

In elk zorgtraject is afstemming en samenwerking van vitaal belang, dit geldt vooral bij ketenzorg, multidisciplinaire behandelteams en andere samenwerkingsvormen. Hiervoor is het nodig dat zorgprocessen van binnen en buiten het Affinity Domain goed in kaart zijn gebracht. Op deze manier ontstaat een goed inzicht om deze processen om te zetten naar definities van workflows en informatieoverdracht. Merk op dat in de processen ook zorgaanbieders van buiten de regio betrokken kunnen zijn.

Dit hoofdstuk geeft inzicht in welke stappen moeten worden doorlopen om de zorgprocessen in kaart te brengen om daarmee de zorgprofessional te ondersteunen bij zijn dagelijkse activiteiten. Dit hoofdstuk beschrijft allereerst de definitie van een use case inclusief een lijst van bestaande use cases. Daarna is een stappenplan beschreven voor de implementatie van nieuwe use cases.

4.1 Use Case

Bij het delen van medische gegevens tussen zorginstellingen en zorgverleners, is het zorgproces het uitgangspunt. De gebruiker moet zo goed mogelijk ondersteuning bij zijn/haar werkproces krijgen. Voordat een technische inrichting plaatsvindt is het noodzakelijk het zorgproces in kaart te hebben. Vaak zijn deze zorgprocessen voor delen van medische informatie ingericht naar ziektebeeld (bijv. neurochirurgie) of specialisme (bijv. radiotherapie). Binnen het beschrijven van een dergelijk proces dienen ook de algemene werkafspraken te zijn meegenomen. Wie zet welke gegevens klaar of haalt deze op, of wie kan er in geval van ontbreken van gegevens gebeld worden. In de praktijk wordt een degelijke procesbeschrijving ook wel een use case genoemd.

4.1.1 Definitie Use case

Een use case is een specifieke beschrijving van een praktijksituatie in de zorg waarbij voor een concrete situatie het vastleggen en uitwisselen van informatie wordt beschreven aan de hand van actoren (mensen, systemen) en transacties (welke informatie wordt wanneer uitgewisseld). Een use case is een verbijzondering van een specifiek onderdeel van het zorgproces (Nictiz, 2018). De hier gehanteerde definitie van een use case is breder dan de definitie van UML, die een specifiek onderdeel van systeemgebruik beschrijft (UML, 2018). Een use case volgt de definitie van IHE, waarbij het zorgproces wordt beschreven. Hiervoor wordt ook wel de term ‘Business Use Case’ gebruikt. Daarnaast wordt ook de inrichting van het zorg- en werkproces meegenomen op functioneel en technisch gebied. (Bijlage 6 geeft een voorbeeld van een use case beschrijving).

4.1.2 Use cases in Nederland

De onderstaande use cases worden in meer of mindere mate in Nederland ondersteund of op het ogenblik ingericht op basis van IHE-XDS, waarbij onderstaande lijst niet uitputtend is.

- Vervanging CD/DVD met beelden (PACS-I, PACS-II en/of VNA);
- Aanvraag PET-CT inclusief terugmelding resultaat (beeld en verslag);
- Ondersteuning MDO;
- (Aanvraag) Radiotherapie;
- Intercollegiaal consult;
- Overdracht ziekenhuis naar VVT;
- Spoed casus;
- Het delen van complete chirurgische dossiers t.b.v. samenwerking tussen ziekenhuizen.

4.2 Technische uitwerking Use case

Bij de uitwerking van een use case is het aan te raden om de door IHE ontwikkelde methodologie te gebruiken (Nictiz, 2018).

In dit model worden de volgende stappen doorlopen om een use case op te stellen en tot in detail uit te werken. De functionaliteit van de te koppelen applicaties wordt meegenomen in de use case beschrijving, om te veel handmatige stappen te voorkomen.

4.2.1 Functioneel Proces

- Uitwerking huidige proces in tekst en stroomschema's;
- Uitwerking toekomstig proces met IHE-XDS in tekst en stroomschema's;
- Impact op de huidige werkwijze in tijdbesteding en andere handelingen door andere gebruikers.

4.2.2 Technische uitwerking van toekomstig proces met IHE-XDS

- Benodigde componenten;
- Benodigde koppelingen;
- Benodigde configuratie van de bovenstaande componenten / koppelingen;
- Uitwerking in het technisch ontwerp.

4.2.3 Implementatieafspraken en beheerafspraken

- Afstemming met eindgebruikers, wie doet wat. Welke personen zijn verantwoordelijk voor het aanmelden van gegeven. Welke personen halen gegevens binnen;
- Welke verslagen en beelden ga je uitwisselen. Dit kan per use case anders zijn. Leg hierbij ook de mimetypes van de documenten vast;
- Bekendheid onder eindgebruikers wat het nummer voor de helpdesk is in geval van een storing;
- In geval van bijvoorbeeld verwijzing, wie is het aanspreekpunt aan de kant van de verwijzer om in geval van ontbrekende gegevens te bellen.

De uitgebreide beschrijving van de te doorlopen stappen voor de realisatie van een use case, is te vinden in bijlage 7.

4.3 Adviezen

- Werk voorafgaand aan technische implementatie een use case uit en betrek daarbij de eindgebruikers;
- Volg het stappenplan voor het inrichten van een IHE-XDS-omgeving en de afstemming met een RSO;
- Gebruik de voorgestelde blauwdruk als uitgangspositie voor het inrichten van een projectstructuur van het IHE-XDS project.

5 Informatie - IHE-XDS metadata

Het aantal gezondheid gerelateerde documenten en beelden dat in de zorg wordt vastgelegd, neemt voortdurend toe. Om orde aan te brengen, is contextuele informatie nodig: wat voor soort document is het en wie heeft gegevens waarom, waar, waarmee en wanneer vastgelegd? Op het niveau van IHE-XDS metadata wordt vastgelegd welke informatie-elementen, op welk detailniveau, er minimaal dienen te worden uitgewisseld inclusief de mogelijke waarden die een bepaald element kan aannemen. Deze metadata-elementen worden gekoppeld aan terminologiesystemen, waardoor ook koppelingen met vertaaltabellen, decision support systemen en dergelijke mogelijk worden. Dit hoofdstuk geeft op het niveau van de informatielaag weer welke metadata gebruikt worden om de uit te wisselen medische gegevens te categoriseren, zowel voor de ontvanger als de bron van de gegevens.

5.1 Noodzaak harmonisatie van metadata sets

IHE definieert voor XDS een set van metadata attributen (elementen, velden) die moeten worden vastgelegd voor elk document dat bij de Registry wordt aangemeld, en stelt vast welke waarden deze attributen mogen hebben, of deze waarden verplicht of optioneel zijn, hoeveel waarden elk waarde-element mag bevatten (cardinaliteit) en zo voorts. Op basis van deze metadata attributen kan de juiste informatie vanuit verschillende benaderingswijzen efficiënt en betrouwbaar worden gevonden.

5.1.1 Vrijheden IHE-XDS Metadata

Bij een aantal metadata attributen schrijft het IHE-XDS profiel deze waarden niet precies voor, met name voor waardenlijsten waarmee de hoofd- en subcategorie van het document worden vastgelegd. De invulling hiervan wordt overgelaten aan de deelnemers van een IHE-XDS Affinity Domain. Binnen een Affinity Domain hoeft dat geen probleem te zijn. Waarden worden echter vaak ad hoc uitgebreid waardoor er uiteindelijk een inconsistente waardenlijst ontstaat. Wanneer men informatie tussen verschillende IHE-XDS Affinity Domains wil gaan uitwisselen, vormt deze aanpak een probleem aangezien de waardenlijsten niet op elkaar aansluiten. Wanneer de ene arts een onderzoek opslaat onder de rubriek 'Echo onderbuik' en de andere onder de noemer 'US abdomen', zullen beide documenten niet onder dezelfde rubriek worden teruggevonden.

Daarnaast is het nodig, dat de waarden die een bepaald attribuut mag bevatten eenduidig van elkaar zijn te onderscheiden en dat documenten van een bepaald type door verschillende eindgebruikers in telkens dezelfde categorie worden ondergebracht. Als dit niet gebeurt raakt in wezen informatie verloren. Dit risico speelt zeker in de medische setting, waar het snel kunnen vinden van de juiste informatie van levensbelang is. Het onjuist rubriceren van medische documentatie is vergelijkbaar met het terugzetten van een boek in een bibliotheek op een willekeurige plek: als de bibliotheek groot genoeg is, zal het boek niet teruggevonden worden.

5.1.2 Internationale initiatieven

De niet door IHE- XDS gedefinieerde attributen en de noodzaak om daar iets voor te verzinnen speelt in alle landen die met IHE-XDS implementaties bezig zijn. In 2016 heeft Nictiz aan verschillende landen voorgesteld om gezamenlijk na te denken over de keuzes en methodiek voor het invullen van die waardenlijsten. Hiertoe is vervolgens in 2017 de International XDS Metadata Taskforce opgericht. Negen landen in Europa (en de VS) hebben gezamenlijk principes, randvoorwaarden en aanbevelingen gedaan en deze gepubliceerd in de 'XDS-metadata for exchange medical documents and images guideline' (IHE, 2017). Daarna heeft, in vervolg op deze publicatie, de IT Infrastructure Technical Committee van IHE International het Document Sharing Metadata Handbook (IHE, 2018) opgeleverd, waarin algemene inrichtingsprincipes voor XDS-metadata zijn vastgelegd. Beide documenten zijn als basis gebruikt voor de definitie van de nationale XDS-metadata set (zie paragraaf 5.2).

5.2 Nationale IHE-XDS Metadata set

Om een landelijk dekkend netwerk van IHE-XDS Affinity Domains te realiseren moet op landelijk niveau invulling worden gegeven aan alle waarden die de verschillende metadata attributen kunnen bevatten: de hele metadataset en de bijbehorende waardenlijsten moet worden vastgelegd. Daarnaast moeten de verschillende waardenlijsten helder zijn gedefinieerd waardoor de logica van het metadatasysteem aansluit bij die van de eindgebruikers en moeten er regels worden opgesteld voor het gebruik ervan.

Hiervoor is de **nationale IHE-XDS metadataset** ontwikkeld. Mede in het kader van de Handreiking 2018 is een nieuwe versie van de IHE-XDS Metadataset opgeleverd. De Standaard voor Metadata en een korte handleiding zijn te vinden op de website van Nictiz (https://www.nictiz.nl/XDSmetadata).

5.2.1 Governance

Voor de governance van het beheer en het gebruik van de XDS-metadata set gelden de volgende regels:

- Nictiz onderhoudt de relevante waardenlijsten, waaronder de waardenlijsten die worden gebruikt in de XDS-metadata;
- Binnen een Affinity Domain moet een procedure zijn ingericht die ervoor zorgt dat iedereen dezelfde versie van de metadataset gebruikt, om eventuele uitwisselingsproblemen met andere Affinity Domains te voorkomen. Als de huidige Nictiz metadataset niet toereikend is, kunnen er (tijdelijk) aanvullende afspraken worden gemaakt;
- In deze procedure is ook vastgelegd hoe aanpassingen aan de XDS-metadataset worden geregeld. Uitgangspunt is, dat er periodiek een update wordt gepland, die door alle Affinity Domains binnen een bepaalde termijn, bijvoorbeeld drie maanden, wordt geïmplementeerd, op basis van de nieuwe versie van het *Dataset XDS-metadata* document;
- Voorstellen voor toevoegingen of aanpassingen aan de metadataset (waardenlijsten) dienen te worden aangevraagd bij Nictiz. Eventuele aanpassingen worden in een nieuwe versie van de XDS-metadataset gepubliceerd;
- Voor het inrichten van de metadata-infrastructuur van de IHE-XDS Registry moet de meest actuele Nictiz XDS-metadataset voor het inrichten van de metadata binnen het Affinity Domain worden gevolgd. Gezien de verschillen in implementatiesnelheid is het toegestaan om één versie achter te lopen.

5.2.2 Versiebeheer

De volgende afspraken gelden voor het beheer van de standaard en het verder onderhouden van de standaard XDS-metadata set:

- Nictiz beheert de metadata standaard en zal maximaal één keer per jaar een update van deze metadataset opleveren;
- De waarden in de huidige metadataset zullen geldig blijven. Op het moment dat er een nieuwe versie Nictiz Metadataset beschikbaar is, kunnen de extra waarden worden toegevoegd aan de XDS Registry en het Metadata document. De RSO zorgt ervoor dat dit wordt uitgevoerd;
- Bij een nieuwe aansluiting op een Registry dient de participant aan te geven welke metadatawaarden gebruikt zullen worden voor de documenten. Waarden die nog niet geconfigureerd zijn in de Registry, zullen, als de waarden geldig zijn (m.a.w. voldoen aan de beschrijving van de metadatavelden), worden toegevoegd in de Excel Sheet en in de Registry;
- De IHE-XDS Registry wordt zodanig geconfigureerd dat de Registry op het moment van registratie van een nieuw document controleert of de metadata van het document voldoen aan de metadata set van

de Registry. Documenten die hier niet aan voldoen, worden niet geregistreerd: er wordt een foutmelding gegeven aan de Repository.

5.3 Adviezen

- Om interoperabiliteit en eenheid van taal tussen IHE-XDS-netwerken te kunnen waarborgen, is het volgen van de Nictiz metadataset voor IHE-XDS verplicht;
- De “Dataset XDS voor digitale beeld- en documentuitwisseling 2018” geldt als de te volgen inrichting voor XDS-netwerken in Nederland;
- Voor het inrichten van de metadata-infrastructuur van de IHE-XDS Registry moet de meest actuele Nictiz XDS-metadataset voor het inrichten van de metadata binnen het Affinity Domain worden gevolgd. Gezien de verschillen in implementatiesnelheid is het toegestaan om één versie achter te lopen;
- Voorstellen voor toevoegingen of aanpassingen aan de metadataset (waardenlijsten) dienen te worden aangevraagd bij Nictiz. Eventuele aanpassingen worden in een nieuwe versie van de XDS-metadataset gepubliceerd;
- Binnen een Affinity Domain moet een procedure worden ingericht om ervoor te zorgen dat de laatste versie van de metadataset in gebruik is, om eventuele uitwisselingsproblemen met andere Affinity Domains te voorkomen. Nictiz zal in deze procedure aangeven wanneer een nieuwe versie wordt verwacht, en vooraf aankondigen welke aanpassingen er komen.

6 Logging en Auditing (ATNA)

De privacy en security van de gehele keten dienen op meerdere lagen van het interoperabiliteitsmodel te worden vastgelegd. Er 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. Audit logging vormt een onderdeel van dit geheel en wordt in dit hoofdstuk verder uitgewerkt. Binnen IHE is de logging gedefinieerd in het IHE-ATNA profiel.

6.1 Noodzaak en definitie auditlogging

Auditlogging is de registratie van alle activiteiten waarbij privacygevoelige informatie wordt aangemaakt, ingezien, bijgewerkt, gekopieerd, gezocht, verplaatst of gewist.

De NEN 7510 stelt op gebied van auditlogging het volgende:

"*Er behoren audit-logbestanden te worden aangemaakt waarin activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen worden vastgelegd. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.*"

Deze eis uit de NEN 7510 is in de NEN 7513 verder uitgewerkt en voorzien van uitgebreide richtlijnen voor het bijhouden van acties op elektronische patiëntendossiers.

Audit logging biedt de zorgaanbieders die verantwoordelijk zijn voor het goed en rechtmatig laten verlopen van de uitwisseling van patiëntgegevens via IHE-XDS, de mogelijkheid dit te controleren. Met behulp van een auditlogging wordt de mogelijkheid gecreëerd om de integriteit en de vertrouwelijkheid van patiëntgegevens beter te waarborgen.

6.1.1 Gedragscode EGiZ

Bij de inrichting van IHE-XDS zijn de richtlijnen vanuit de EGIZ-gedagscode gehanteerd. De Gedragscode EGiZ zegt over logging het volgende:

Artikel 10 – Logging

10.1 De Verantwoordelijke zorgt ervoor dat in een Elektronisch Uitwisselingssysteem en de daarop aangesloten Zorginformatiesystemen Logging plaatsvindt.

10.2 De Logging biedt een overzicht van de verwerkingshandelingen (acties) die plaats hebben gevonden met betrekking tot Persoonsgegevens. Hiertoe bevat de Logging ten minste de volgende gegevens:

- de acties die hebben plaatsgevonden, waaronder ten minste het vastleggen, bijwerken, bewaren en raadplegen van Persoonsgegevens;
- datum en tijdstip van de actie;
- de identiteit van de Betrokkene;
- de identiteit van de Zorgverlener of medewerker die de actie heeft uitgevoerd;
- de identiteit van de Zorgaanbieder onder wiens verantwoordelijkheid de actie heeft plaatsgevonden.

10.3 De Verantwoordelijke houdt voorzieningen in stand waarmee de Brondossierhouder of de Betrokkene de Logging kan inzien.

10.4 De Verantwoordelijke stelt een beleid vast met betrekking tot:

- de toegang tot de gegevens in de Logging;

- het uitvoeren van een periodieke controle van de Logging op onbevoegde raadplegingen;
- het uitvoeren van specifieke controles op raadplegingen die hebben plaatsgevonden in noodsituaties, en
- de te volgen procedure bij vermeend of geconstateerd misbruik.

6.2 Auditlogging in detail

Er moet afgesproken worden wat er wordt vastgelegd, wie toegang heeft, hoe lang gegevens bewaard moeten worden en wanneer wie controleert op vermeend misbruik.

6.2.1 Vast te leggen logging

Bij de auditregistratie moet worden vastgelegd:

- Wanneer de activiteit plaatsvond (date/timestamp);
- Wat de activiteit inhield (welke transactie);
- Wie de activiteit verrichte (persoon en systeem);
- Waar de activiteit plaats vond (organisatie ID);
- Welke informatie het betreft (documentnummer, unieke ID);
- Welke patiënt het betreft (patiënt ID).

6.2.2 Toegang tot logging

De gedragscode EGiZ stelt in artikel 10.3 dat de Verantwoordelijke voorzieningen in stand moet houden waarmee de Brondossierhouder en de Betrokkene (patiënt/cliënt) de logging in kunnen zien. Op termijn is het wenselijk dat patiënten (naast zorgverleners) online inzage krijgen.

Zolang dat niet mogelijk is, moet de mogelijkheid aanwezig zijn om via de eigen zorgaanbieder de logging te raadplegen. De procedure die hiervoor wordt gehanteerd luidt als volgt:

1. De zorgverlener of patiënt neemt contact op met de zorgaanbieder die informatie uitwisselt via IHE-XDS;
2. De zorgaanbieder vergewist zich er van dat de identiteit van de betreffende zorgverlener of patiënt juist is door het opvragen van een geldig identiteitsbewijs;
3. De security-officer, of ander daar voor aangestelde persoon, van de zorgaanbieder neemt contact op met de verantwoordelijke bij de RSO en vraagt de gewenste logging gegevens op;
4. De verantwoordelijke bij de RSO stelt de gewenste logging gegevens op een veilige manier beschikbaar.

6.2.3 Bewaartermijn van logginggegevens

In de loggegevens die vanuit IHE-XDS worden gegenereerd, worden behalve het BSN geen persoonsgegevens vastgelegd. Met een nader vast te stellen frequentie worden vanuit de loggegevens rapportages opgesteld die vervolgens aangeboden worden aan de deelnemende zorginstellingen. Wanneer onregelmatigheden en ongeoorloofde acties worden geconstateerd, heeft de zorginstelling een bepaalde tijd nodig om actie te ondernemen. De NEN7513 stelt dat de belanghebbende(n) termijnen moeten vaststellen voor het bewaren van loggegevens. Hier is verder bij beschreven dat de bewaartermijn minimaal 2 jaar en maximaal 15 jaar is. De algemene bewaartermijn van een medisch dossier is 15 jaar. Huidige of toekomstige wettelijk of in regelgeving bepaalde termijnen prevaleren boven deze bewaartermijnen indien deze afwijken.

6.2.4 Controle op de logging

Minimaal eenmaal per halfjaar moet een RSO of zorginstelling een controle op de logging uitvoeren. Dit zal op basis van steekproeven gebeuren. Een controle op de logging gebeurt ook bij verdenking van misbruik. Verdenking van misbruik kan ontstaan door een melding van een zorgverlener, een medewerker of een patiënt en/of als er ongebruikelijke raadplegingen worden geconstateerd. Bijvoorbeeld ongebruikelijk veel raadplegingen door dezelfde persoon of van dezelfde patiëntgegevens of raadplegingen op ongebruikelijke tijdstippen.

Bij melding van vermeend misbruik vindt controle binnen 24 uur na de melding plaats.

Wat betreft ongebruikelijke raadplegingen: niet elke Audit logging beschikt over de techniek waarmee de security-officer vanuit het systeem automatisch een signaal krijgt dat er sprake is van ongebruikelijke raadplegingen. Daarom kunnen specifieke rapportages gemaakt worden op basis waarvan ongebruikelijke raadplegingen gesignaleerd kunnen worden. Voor het uitvoeren van de periodieke controle, maakt de security-officer van het Affinity Domain hiervoor, per aangesloten zorgaanbieder, een random selectie van alle acties die binnen het IHE-XDS netwerk gelogd worden. De omvang van deze selectie is afhankelijk van de intensiteit waarmee de betreffende zorgaanbieder gebruik maakt van IHE-XDS. Deze selectie wordt op een veilige manier beschikbaar gesteld aan de contactpersoon van de betreffende zorgaanbieder.

Deze verantwoordelijke voor de controle is, op grond van de eigen kennis en informatie, in staat om vast te stellen of er sprake is geweest van onbevoegde raadplegingen. De verantwoordelijk bericht de security-officer van het Affinity Domain over de uitkomsten.

6.2.5 Vermeend en geconstateerd misbruik

Bij (verdenking van) overtreding van de regels voor beschikbaar stellen of raadplegen van patiëntgegevens wordt de aangewezen contactpersoon van de zorgaanbieder, waarbij de zorgverlener is aangesloten, hiervan op de hoogte gesteld. Het eigen beleid van de desbetreffende zorgaanbieder t.a.v. sancties en het informeren van betrokkenen is dan van kracht. De contactpersoon van de betreffende zorgaanbieder informeert de security-officer van het Affinity Domain over de eventuele vervolgacties.

6.2.6 Overige bepalingen

Naast de in dit protocol genoemde partijen hebben ook de daartoe geautoriseerde personen van de leverancier en de beheerder van de IHE-XDS infrastructuur inzage in bepaalde in IHE-XDS vastgelegde informatie. De afspraken en regels die hiervoor gelden zijn vastgelegd in de verwerkersovereenkomst die het Affinity Domain met de leverancier heeft afgesproken. In deze overeenkomst hebben de betrokken partijen vastgelegd voor welke doeleinden de gegevens mogen worden verwerkt, welke beveiligingsmaatregelen moeten worden genomen en welke vormen van toezicht de eigenaar van de gegevens mag uitoefenen.

6.3 Adviezen

- Audit logging is verplicht vanuit de NEN 7510 en NEN 7513:2018;
- Voor auditlogging wordt gebruik gemaakt van het IHE-ATNA profiel;
- Alle activiteiten die binnen een IHE-XDS Affinity Domain plaatsvinden dienen te worden vastgelegd in een audit log;
- Alleen daartoe aangewezen gebruikers (de verantwoordelijke voor de logging, FG, security officers) mogen toegang tot de audit logging krijgen;
- Minimaal eenmaal per halfjaar en bij verdenking van misbruik, moet een RSO of zorginstelling een controle op de logging uitvoeren. Hiervoor dient een procedure te zijn opgesteld.

7 Applicaties – Identity en Access Management

Om als gebruiker toegang te krijgen tot medische gegevens, is het noodzakelijk om een proces van identificatie, authenticatie en autorisatie te volgen.

1. Bij identificatie geeft een gebruiker aan, wie hij is;
2. Authenticatie is de controle waarmee kan worden aangetoond dat degene die zich identificeert ook daadwerkelijk degene is die hij zegt te zijn;
3. Nadat een gebruiker is geauthentiseerd, wordt in de autorisatiestap bepaald tot welke informatie deze toegang heeft, afhankelijk van de rechten die voor de gebruiker zijn geconfigureerd.

Dit hoofdstuk start met de toelichting van het IHE-XUA profiel en geeft vervolgens een overzicht van wat er nodig is op het gebied van authenticatie en autorisatie.

7.1 IHE-XUA profiel

Met behulp van IHE-XDS kan een gebruiker van zorginstelling A, via de IHE-XDS Registry, documenten van zijn patiënt in zorginstelling B raadplegen. Zowel de IHE-XDS infrastructuur als zorginstelling B, moeten hierbij zekerheid hebben over de identiteit van de gebruiker en zijn autorisatie om de documenten te mogen benaderen. Daarnaast is de identiteit van de gebruiker nodig om de transacties te loggen voor audit doeleinden (ATNA).

Hiervoor is het IHE-XUA profiel ontwikkeld. Dit Cross-enterprise User Assertion (XUA) profiel biedt een standaard methode om de identiteit van een service gebruiker (een mens, applicatie of systeem) mee te geven in transacties tussen verschillende organisaties en Affinity Domains. Naast de identiteit is het met XUA ook mogelijk en een aantal andere gegevens over de gebruiker (attributen of claims) mee te geven, zoals:

- De manier waarop de authenticatie van de gebruiker heeft plaatsgevonden en het betrouwbaarheidsniveau;
- Welke (federatieve) organisatie die identiteit heeft vastgesteld;
- De autorisatierol van de gebruiker (ter ondersteuning Role Based Access Control);
- Consent informatie zoals afgegeven door de patiënt;
- Purpose of Use: het beoogde gebruik van de gegevens, bijvoorbeeld voor onderzoeksdoeleinden, bepaalt of een gebruiker toegang krijgt tot deze gegevens.

Bij gebruik van het IHE-XUA profiel kunnen zorginstellingen hun eigen methode blijven gebruiken om gebruikers te identificeren, authenticeren en autoriseren, bijvoorbeeld op basis van de eigen Active Directory of het gebruik van de UZI-pas. Het XUA-profiel biedt hierbij een veilige en betrouwbare manier om gebruikers over organisatiegrenzen heen (federatief) op basis van SSO te identificeren en te autoriseren.

7.1.1 Advies

IHE-XDS schrijft het gebruik van XUA niet voor en bij de verschillende Affinity Domains en RSO's zijn dan ook verschillende methodes voor het doorgeven van de gebruikersidentiteit en autorisatie in gebruik. Voor interoperabiliteit tussen Affinity Domains is het noodzakelijk hier vaste afspraken over te maken

Omdat het ongewenst is dat elke zorginstelling een eigen invulling geeft aan identificatie, authenticatie en autorisatie van gebruikers is het advies om gebruik te maken van het IHE-XUA profiel en daarbij landelijke afspraken te maken over:

- Welke claims (attributen) over een service gebruiker meegegeven kunnen worden (bijvoorbeeld: authenticatiemethode en betrouwbaarheidsniveau, autorisatierol etc.);
- De waardenlijsten van elk van deze claims (bijvoorbeeld: autorisatierol = {medisch specialist, apotheker, SEH-arts etc.}).

7.2 Authenticatie van gebruikers

Voordat een gebruiker toegang krijgt tot de XDS-infrastructuur, moet hij of zij zich bekend maken. Hoe dit gebeurt is afhankelijk van de vraag hoe de gebruiker de XDS-consumer (viewer) krijgt aangeboden. Hiervoor zijn twee methoden beschikbaar:

1. De XDS-consumer wordt beschikbaar gesteld als stand alone webapplicatie of web-portaal;
2. De XDS-consumer wordt geïntegreerd in het EPD van de gebruiker en is van daaruit beschikbaar.

In het eerste geval zal de gebruiker zich meestal nog bekend moeten maken en moeten inloggen, maar ook single-sign-on (SSO) is mogelijk op basis van federatieve authenticatie[3]. Als geen federatieve authenticatie mogelijk is, moet een aparte gebruikers- en gebruikersrechten administratie worden bijgehouden binnen de XDS-infrastructuur. Dit betekent extra beheerlast.

Omdat de XDS-consumer niet in het EPD is geïntegreerd, zal de gebruiker vervolgens de juiste patiënt moeten opzoeken. Omdat de XDS-infrastructuur niets weet over de relaties tussen zorgverleners en patiënten, is een controle op de behandelrelatie in dit geval niet mogelijk.

In het tweede geval is de gebruiker al ingelogd in het eigen EDP-systeem en heeft het dossier van een patiënt geopend. Hierbij controleert het EPD de behandelrelatie tussen de zorgverlener (de gebruiker) en de patiënt. Nu kan de gebruiker de XDS-consumer starten. Dit kan SSO vanuit het EPD waarbij de gebruikersidentiteit en de autorisatierol automatisch bekend worden gemaakt. Bovendien wordt de identiteit van de patiënt in de aanroep van de consumer meegegeven, zodat de gebruiker geen aparte patiëntselectie hoeft uit te voeren.

Integratie van de XDS-consumer in het EPD van de gebruiker is dus makkelijker, veiliger en preferent ten opzichte van een stand alone consumer.

7.2.1 Authenticatiebeleid

Voor authenticatie van gebruikers worden diverse middelen gebruikt. Binnen de zorg zijn de meest bekende voorbeelden de UZI-pas voor zorgverleners en DigiD voor patiënten. Daarnaast wordt binnen een zorginstelling gebruik gemaakt van gebruikersnaam en wachtwoord, vastgelegd in de eigen Active Directory.

Bij authenticatie is het van belang dat de identiteit van een gebruiker (mens, applicatie of systeem) met voldoende zekerheid vastgesteld kan worden. Sinds 1 juli 2016 is in Europa de eIDAS-verordening voor digitale identificatie- en vertrouwensdiensten, van kracht. eIDAS definieert drie betrouwbaarheidsniveaus voor authenticatiemiddelen: Laag, Substantieel en Hoog. Welk betrouwbaarheidsniveau vereist is om in te mogen loggen op een bepaalde dienst, moet vastgesteld worden aan de hand van een risicoanalyse waarin een aantal criteria een rol speelt[4]. Deze criteria hebben te maken met:

[3] Voor uitleg over single-sign-on, zie paragraaf 7.2.2

[4] Zie voor een uitgebreide toelichting: 'Betrouwbaarheidsniveaus voor digitale dienstverlening. Een handreiking voor overheidsorganisaties', versie 4, April 2017, Forum Standaardisatie.

- De wettelijke eisen die gesteld worden aan de dienst;
- De aard van de gegevens en de verwerking ervan die via de dienst beschikbaar zijn;
- De potentiële schade bij misbruik van de gegevens die via de dienst ontsloten worden.

Als deze risicoanalyse wordt toegepast op een IHE-XDS Affinity Domain, dat toegang geeft tot bijzondere persoonsgegevens van patiënten, dan zal de conclusie zijn dat authenticatiemiddelen met betrouwbaarheidsniveau 'Hoog' vereist zijn.

Deze eis geldt ook wanneer zorgprofessionals inloggen op het elektronisch patiëntendossier van hun eigen instelling. In de praktijk loggen zorgprofessionals meestal in met gebruikersnaam plus wachtwoord, zolang zij zich binnen de muren van de eigen organisatie bevinden. Hieraan ligt de redenering ten grondslag dat er binnen de eigen organisatie sprake is van voldoende toezicht en van een veilig beheerd en gesloten netwerk.

De NEN7512: 'Vertrouwensbasis voor gegevensuitwisseling', die door VWS als dwingend voor de zorg beoordeeld wordt, is in dit verband belangrijk. Deze norm stelt dat de authenticatiesterkte wordt bepaald door de combinatie van het toegepaste authenticatiemiddel, het uitgifteproces, de wijze waarop het beheer en intrekken plaatsvinden en het eigenlijke authenticatieproces. Ook het sterkste authenticatiemiddel levert bij een zwak beheer of gebrekkige verificatie niet meer dan een zwak resultaat.

Iedere zorginstelling (de zogenoemde 'Verantwoordelijke') die gegevens beschikbaar stelt via een IHE-XDS infrastructuur, is zelf verantwoordelijk voor het verplicht uitvoeren van een privacy en security risicoanalyse en het documenteren van de resultaten hiervan in een PIA. De eisen m.b.t. het betrouwbaarheidsniveau van de authenticatie maken hier deel van uit.

7.2.2 Eenmalig inloggen (Single Sign On)

Met eenmalig inloggen hoeven gebruikers van ICT-diensten (applicaties, websites) niet opnieuw in te loggen als ze in dezelfde gebruikers- of browsersessie naar een andere dienst of website navigeren. Eenmalig inloggen wordt Single Sign On (SSO) genoemd. De gebruiker kan dan volstaan met inloggen bij de eerste dienst en hoeft daarna niet steeds opnieuw zijn identiteit te bevestigen. SSO is mogelijk binnen één organisatie of domein en over organisatiegrenzen en domeinen heen. In dat laatste geval spreekt men over federatieve authenticatie.

Nauw verbonden met eenmalig inloggen is eenmalig uitloggen (Single Sign Off). Dit moet zekerheid geven dat de openstaande sessies en toegang tot de diensten in één handeling worden beëindigd na het uitloggen van de gebruiker.

Zoals eerder opgemerkt kunnen gebruikers bij zorginstellingen vaak in hun eigen dossiersysteem inloggen met gebruikersnaam en wachtwoord, als zij zich fysiek binnen de muren van de eigen organisatie bevinden. Via deze methode van inloggen en SSO kan men documenten raadplegen op het eigen IHE-XDS Affinity Domain of op een ander gekoppeld Affinity Domain. Dit vraagt van de dienstaanbieder dat hij er op vertrouwt dat de aangesloten organisatie de beveiliging op orde heeft en betrouwbare authenticatiemiddelen uitgeeft aan zijn gebruikers via een gecontroleerd uitgifteproces.

In de praktijk wordt SSO door de verschillende Affinity Domains en regio's, verschillend toegepast. Sommige Affinity Domains/regio's staan SSO toe als de IHE-XDS Consumer wordt aangeroepen vanuit het EPD van de gebruiker, andere Affinity Domains/regio's eisen dat de gebruiker zich aanvullend authenticeert met de UZI-pas. Het is gewenst hierover in Nederland een eensluidend beleid vast te stellen.

7.3 Autorisatie van gebruikers

Als gebruikers eenmaal toegang hebben tot de XDS-infrastructuur via een juiste authenticatie is het van belang dat ze alleen die gegevens van patiënten kunnen inzien waar ze op basis van hun rol toegang toe hebben en waar de patiënt toestemming voor heeft gegeven.

7.3.1 Autorisatiebeleid

De volgende uitgangspunten worden gehanteerd ten behoeve van autorisatie:

- Alleen een zorgverlener met een behandelrelatie heeft toegang tot de relevante gegevens;
- Bij het autoriseren vindt het principe van dataminimalisatie plaats: er wordt niet meer dan noodzakelijk voor de behandeling, ter beschikking gesteld aan de zorgverlener;
- Alle handelingen m.b.t. autorisatie worden gelogd en periodiek gecontroleerd (zie hoofdstuk 6 over logging)

De volgende onderwerpen vallen onder autorisatie en worden verder uitgewerkt.

- Autorisatie in samenhang met toestemming patiënt;
- Bevoegdheden van gebruikers;
- Toegangscontrole op basis van behandelrelatie;
- Breaking the glass toegang

7.3.2 Autorisatie in samenhang met toestemming patiënt

Bij uitwisseling van medische gegevens tussen zorginstellingen, is het verplicht om de toestemming van een patiënt voor het delen van zijn/haar informatie met andere zorginstellingen vast te leggen. In deze toestemming is onder andere vastgelegd wie de gegevens mag raadplegen zoals vastgelegd in toestemmingsregels, de zogenoemde *privacy policies*. (Zie: Nictiz White Paper “https://www.nictiz.nl/guidelines/richtlijn-voor-implementatie-van-toestemmingsprofielen-binnen-xds-netwerken/”). Deze privacy policies zijn geldend binnen het Affinity Domain en moeten ook afgestemd worden tussen Affinity Domains. Implementaties met BPPC kunnen plaatsvinden samen met op rollen gebaseerde toegangscontrole mechanismen zoals Role Based Acces Control (RBAC) of Policy Based Access Control (PBAC).

De toestemming wordt vastgelegd in een BPPC document en geeft in digitale vorm aan welke ‘consent policy of policies’ door een patiënt zijn vastgelegd. Door na het inloggen van een gebruiker, zijn of haar rol, organisatie en functie met de vastgelegde consent policies te vergelijken, worden gegevens wel of niet beschikbaar gesteld aan de opvrager. De mogelijke consent policies en wat een gebruiker, met een bepaalde rol, organisatie en functie, wel of niet mag is vastgelegd en ingericht op basis van afspraken die gemaakt zijn binnen het Affinity Domain en tussen Affinity Domains. De controle moet plaatsvinden op het niveau van de Registry. In dit geval forceert het Affinity Domain de vastgelegde toestemming van de patiënt bij het opvragen door een IHE-XDS consumer.

Voor toegang tot de Registry wordt gewerkt met een rollen- en rechtenstructuur waarmee de geautoriseerde gebruiker uitsluitend toegang krijgt tot functionaliteit en gegevenscategorieën waar hij/zij toe geautoriseerd is. Het advies is om hier de UZI-rollen voor te gebruiken zoals deze ook voor het LSP worden gebruikt. De gebruiker kan, ook al is deze bevoegd, gegevens alleen inzien als de patiënt daarvoor toestemming heeft gegeven. Toegang tot gegevens is hiermee een combinatie van gebruikersautorisatie en toestemming patiënt.

7.3.3 Bevoegdheden en autorisatie gebruikers

Iedere zorginstelling heeft een autorisatie matrix waarin een relatie wordt gelegd tussen de functie (samengevat in een rol) en de bijbehorende bevoegdheden. Bij de implementatie van een IHE-XDS infrastructuur dient daar de autorisatie voor de IHE-XDS consumer(s) aan te worden toegevoegd. Vervolgens dienen de lokale rollen te worden gemapt naar rollen van het Affinity Domain.

De LSP-rolcodes zijn afgeleid uit het BIG-register en daarnaast is er een aantal rolcodes die niet in het BIG voorkomen, die laatste worden ook wel de toegevoegde rolcodes genoemd.
De lijst van rolcodes is te vinden in de IHE-XDS metadataset (zie hoofdstuk 5).

Autorisatie van de patiënt voor toegang tot zijn/haar dossier is ook onderdeel van de autorisatiematrix. Aanvullend op het (eenmalig) inrichten van de rollen, dienen er regionale afspraken gemaakt worden over de mutaties in het personeelsbestand van de zorginstellingen. Bij mutaties in de rol of vertrek van een zorgverlener, dient de autorisatie direct te worden aangepast c.q. verwijderd.

Bij een nieuwe use case zal per instelling moeten worden bekeken welke organisatierollen van de gebruikers toegang nodig hebben en hoe deze moeten worden gemapt op de rollen in de IHE-XDS omgeving. Indien het gewenst is om een toevoeging te doen aan de rollen, dan kan daarin worden voorzien middels de volgende procedure:

- Mocht een UZI pas-rol onbekend zijn voor de IHE-XDS architectuur, dan dient de rol bekend gemaakt te worden via bestaande beheerafspraken zoals vastgelegd in een SLA, DAP of DVO;
- Change management zal in overleg met de leverancier de mapping tabel aanpassen.

7.3.4 Toegangscontrole o.b.v. behandelrelatie

Alleen een zorgverlener met een behandelrelatie krijgt toegang tot het dossier van de patiënt. Doorgaans wordt deze behandelrelatie getoetst door het EPD bij het openen van het dossier van de patiënt. Als de XDS-consumer wordt gestart vanuit het geopende dossier van de patiënt, dwingt het EPD dus af dat de behandelrelatie gecontroleerd is. Patiënt selectie in de IHE-XDS consumer is dan uitgeschakeld. EPD's met een ingebouwde IHE-XDS consumer, dwingen de controle op behandelrelatie dus automatisch af. Indien een zorgverlener de IHE-XDS consumer buiten het EPD om kan opstarten, dan is geen controle op behandelrelatie mogelijk. Het advies is in dat geval door periodieke audits op de logging de behandelrelatie handmatig te controleren. De patiënt kan hierin een rol spelen, door hem/haar inzage te geven in de logging.

7.3.5 Breaking the glass toegang

In situaties van acute zorg, is het wenselijk dat een medische samenvatting en/of recente medische beelden/gegevens van de patiënt beschikbaar zijn, ook in het geval dat een patiënt (nog) geen toestemming heeft gegeven voor het delen van gegevens. Via een Breaking the Glass procedure kan de zorgverlener toegang krijgen tot deze gegevens, zonder dat de patiënt vooraf toestemming heeft gegeven.
Het gebruik van de Breaking the Glass procedure en alle transacties die daarbinnen vervolgens plaatsvinden, wordt door ATNA gelogd.

Indien een patiënt ook bezwaar maakt voor het delen van medische gegevens in noodsituaties, zal een gebruiker geen gegevens te zien krijgen na het bevragen van een registry, ook niet via Breaking the Glass.

7.4 Adviezen

Zowel op het gebied van authenticatie als autorisatie zijn afspraken noodzakelijk. Een verdere invulling is nodig in overleg met juridische experts over de authenticatiemiddelen.

7.4.1 Adviezen Authenticatie

- Het is verplicht om een privacy en security risicoanalyse uit te voeren en de resultaten te documenteren in een PIA. Hiervan maken de eisen m.b.t. het betrouwbaarheidsniveau van de authenticatie deel uit;
- Het te koppelen IHE-XDS Affinity Domain ondersteunt het XUA-profiel voor single-sign-on authenticatie van gebruikers en het doorgeven van de autorisatierol conform de hiervoor landelijk vastgestelde standaard;
- Authenticatie van gebruikers voldoet aan het landelijk overeengekomen betrouwbaarheidsniveau (nog vast te stellen);
- Vanuit de IHE-XDS consumer dient de User identiteit via het XUA profiel doorgegeven te worden met minimaal de volgende gegevens (attributen):
    - UserID (BIGcode of Naam verplicht)
    - Zorgverlenertype (RoleCodeNL staat in de XDS metadataset)
    - Institution Name (URA)
    - De autorisatierol (= zorgverlenerstype) van de gebruiker is een rol uit de landelijk vastgestelde rollenmodel (nog vast te stellen);
- Iedere autorisatierol (RBAC) is gekoppeld aan een landelijk overeengekomen set permissies (nog vast te stellen).

7.4.2 Adviezen Autorisatie

- BPPC-enforcement moet plaatvinden op niveau van de Registry;
- Er is een mapping tabel beschikbaar tussen rollen binnen de zorginstelling en de rollen binnen het Affinity Domain. Geadviseerd wordt om de UZI-rollen en rechten voor autorisaties te gebruiken;
- Er is een procedure beschikbaar bij mutaties in het personeelsbestand;
- Op termijn moet een rol beschikbaar zijn waarin de autorisatie van de patiënt is beschreven;
- Er is een proces beschikbaar (als onderdeel van de beheerafspraken) voor het muteren van autorisatierollen;
- Bij gebruik van de IHE-XDS consumer met mogelijkheid tot patiëntselectie vinden periodieke audits plaats op controle behandelrelatie;
- Er is een toestemming patiënt beschikbaar waarbij de zorgverlener in gevallen van acute zorg toegang kan krijgen tot de gegevens;
- Er vinden periodieke audits plaats op het rechtmatig gebruik van de breaking the glass procedure.

8 Applicaties - koppelingen

Op de applicatielaag van het interoperabiliteitsmodel worden 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 gemaakt over systeemconfiguraties en over eisen ten aanzien van de user interface. Voor elke digitale uitwisseling van zorggegevens is het nodig dat er koppelingen worden gelegd met lokale ICT-zorgsystemen. In de ideale situatie zijn alle zorgsystemen van de diverse ICT-leveranciers aan elkaar te koppelen op basis van IHE profielen en zijn gegevens beschikbaar zodra er een toestemming van de patiënt is vastgelegd. In de praktijk blijkt dit echter niet het geval en is het koppelen van systemen en het daadwerkelijk uitwisselen van gegevens niet altijd direct haalbaar. Dit hoofdstuk geeft een overzicht van medische gegevens die worden uitgewisseld, de benodigde koppelingen en hoe hiermee te starten in de vorm van een roadmap.

8.1 Medische gegevens

Bij voorkeur worden alle deelsystemen in alle zorginstellingen op dezelfde wijze ontsloten en worden medische gegevens zoveel mogelijk met dezelfde inhoud tussen deze instellingen uitgewisseld, waarbij zorgverleners maximaal worden ondersteund in hun werkzaamheden.

8.1.1 Relevante medische gegevens

Medische gegevens worden uitgewisseld bij een verwijzing van een patiënt, een overdracht naar een andere zorginstelling, voor intercollegiale consultatie, om onderzoeken uit te besteden en voor multidisciplinaire overleggen.

Hierbij is het van belang om alle relevante medische gegevens uit te kunnen wisselen, waarbij gegevens ontsloten dienen te worden uit de diverse systemen en het EPD het startpunt is. Voor wat betreft de relevante medische gegevens moet per use case worden afgestemd welke gegevens gedeeld moeten worden.

8.1.2 Zorginformatie bouwstenen EPD's

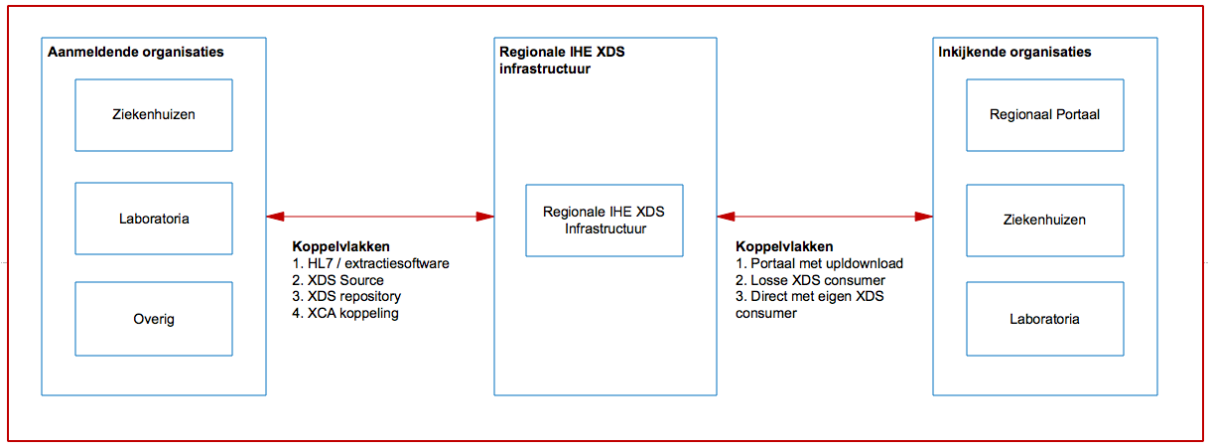
Op termijn zullen EPD's in staat zijn gegevens op een gestructureerde manier te ontsluiten op basis van zorginformatiebouwstenen (ZIB's), waarbij deze ook gestructureerd overgenomen kunnen worden in EPD's van een andere leverancier. Sommige EPD-systemen ondersteunen reeds een koppeling op basis van IHE-profielen, maar nog geen ontsluiting op basis van ZIB's. De meeste leveranciers hebben dit op hun ontwikkelagenda staan voor de komende jaren. Het is aan te raden om het EPD ook geschikt te maken om ZIB's uit te kunnen wisselen via IHE standaarden.

8.1.3 Overige gegevens

Naast de uitwisseling van een gestructureerde basisset aan gegevens o.b.v. ZIB's, bestaat er een noodzaak om alle overige relevante gegevens uit het EPD te delen. Denk hierbij aan brieven en verslagen van diagnostisch onderzoek: lab, pathologie, radiologie en beelden. Daarnaast zijn de relevante gegevens niet altijd in het EPD beschikbaar, maar te vinden in andere deelsystemen. Zorginstellingen maken daarnaast steeds meer gebruik van een Vendor Neutral Archive (VNA) voor beelden, waarbij het in de randvoorwaarden is opgenomen dat deze ook gekoppeld kunnen worden met een IHE-XDS infrastructuur. Door de inzet van een VNA als IHE-XDS repository hoeft een zorginstelling maar één component voor beelden te ontsluiten, in plaats van meerdere archieven zoals een radiologie PACS, cardiologie PACS en een beeldopslagsysteem voor de oogheelkunde.

8.1.4 Advies

Het doel zou moeten zijn om medische gegevens in regionaal verband zoveel mogelijk te ontsluiten via een regionale IHE-XDS infrastructuur. De manier waarop ontsloten wordt, is een keuze van de betrokken zorginstellingen, waarbij gekozen kan worden uit verschillende koppelvlakken (figuur 8.1). Inzage binnen zorginstellingen kan plaatsvinden via een eigen IHE-XDS consumer, al dan niet geïntegreerd in het EPD van de instelling. In de regio kan ook gebruik gemaakt worden van een centrale viewer via een regionaal portaal.



Figuur 8.1: Voorstel regio-architectuur

De categorie overig bij aanmeldende organisaties is niet gedefinieerd, maar hier vallen in ieder geval huisartsen, apotheken en VVT instellingen onder die ook medische gegevens kunnen gaan aanleveren. Waar ze in zullen verschillen t.o.v. ziekenhuizen, is dat ze vermoedelijk niet een eigen oplossing kiezen om aan te sluiten, maar dat ze gebruik zullen maken van één gemeenschappelijke regionale oplossing. Het verzoek van deze partijen kan dan ook zijn om met één oplossing te komen, in plaats van verschillende.

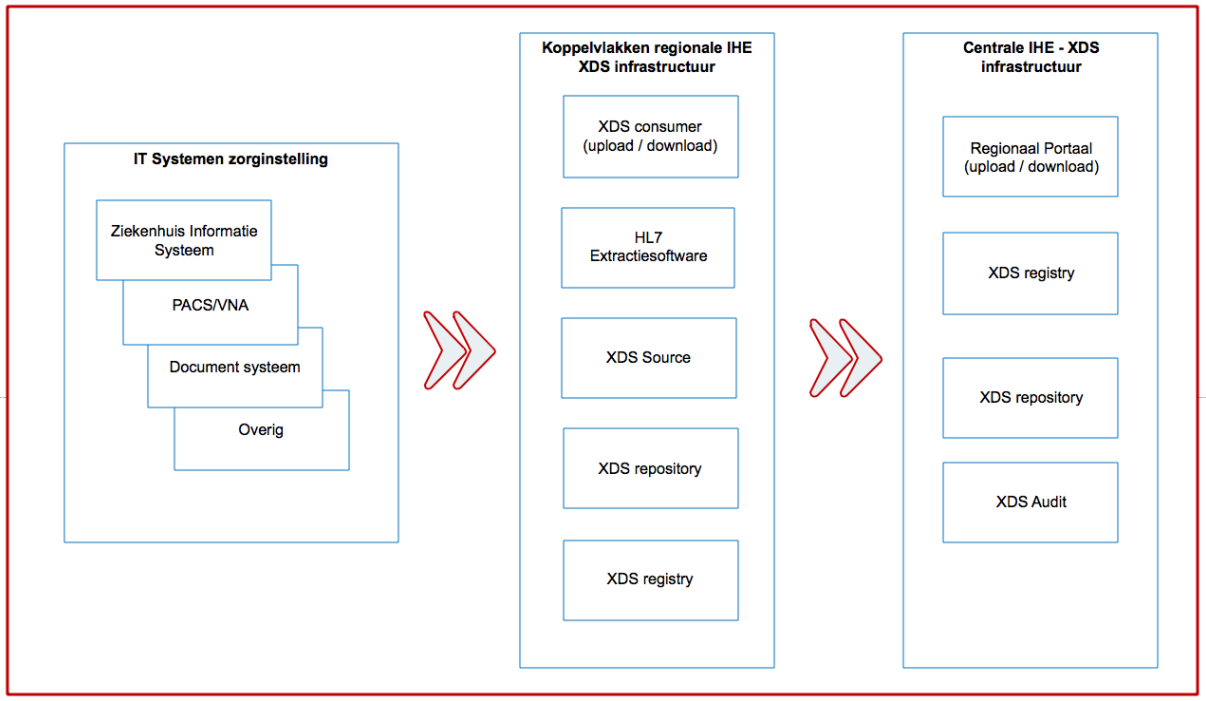
8.2 Koppelvlakken

De diverse ICT-systemen binnen een zorginstelling kunnen op meerdere manieren worden aangesloten op een IHE infrastructuur voor zowel ontsluiting van medische gegevens als inzage functionaliteit. De IHE infrastructuur kan centraal in een regio zijn ingericht of binnen een zorginstelling zelf. Er is een aantal mogelijke koppelvlakken om ICT-systemen van een zorgaanbieder te ontsluiten (figuur 8.2).

- **Handmatig**
  Hierbij is er geen directe digitale koppeling, maar wordt een portaal of viewer gebruikt waarmee de gebruiker documenten kan uploaden naar-, of downloaden vanuit de XDS-infrastructuur. Het portaal kan dan zowel de XDS-consumer (inzien en downloaden) als XDS-source (uploaden) functie vervullen.
- **XDS Adaptors o.b.v. HL7-berichten en/of extractiesoftware**
  Als een bronsysteem zelf geen mogelijkheden biedt om op XDS aan te sluiten, kan gezocht worden naar een optie om dat te doen via HL7- of DICOM-koppelingen of door gebruik te maken van extractiesoftware. In dat geval worden de documenten via de koppeling of extractie uit het bronsysteem gehaald en in een XDS Repository geplaatst die ze vervolgens aanmeldt op de (centrale) Registry.
- **XDS-Source intern, Repository en Registry extern**

Als een applicatie, bijvoorbeeld een PACS, zelf als XDS(-i) source kan functioneren, dan kan deze nieuw beschikbaar gekomen documenten direct in een (regionale) XDS Repository plaatsen en aanmelden op de Registry.

- **Repository intern**
  Sommige XDS implementaties maken gebruik van een centrale regionale Registry terwijl de aangesloten zorgorganisaties hun documenten opslaan in een eigen interne Repository. Het koppelvlak vanuit de zorgorganisatie is dan de Repository die de documenten aanmeldt op de externe centrale Registry.
- **Registry en repository intern (eigen AD)**
  Ziekenhuizen vormen soms ook een eigen XDS Affinity Domain en hebben dus hun eigen Repository en Registry die via XCA aan de buitenwereld zijn gekoppeld.



Figuur 8.2: Mogelijkheden tot ontsluiting binnen een zorginstelling.

8.3 Aanmelden van medische gegevens

Naast ziekenhuizen, zijn ook laboratoria belangrijke organisaties waar gegevens mee uitgewisseld worden.

8.3.1 Ziekenhuizen

Ziekenhuizen die zijn aangesloten op een regionale IHE-XDS infrastructuur starten vaak met het uitwisselen van beeldmateriaal van diagnostisch onderzoek. Overige gegevens en documenten kunnen via papier, post of fax gedeeld worden, maar een DVD/CD-rom is niet te faxen. Het is gewenst om op termijn de digitale uitwisseling van alle soorten zorggegevens via XDS mogelijk te maken zodat een volledig digitale workflow ontstaat om de zorgverlener te ondersteunen in zijn dagelijkse activiteiten.

Dit streven heeft een aantal redenen:

- Gegevens hoeven maar een keer ontsloten te worden en kunnen daarna, na toestemming van de patiënt, door andere aangesloten instellingen ingezien worden. Zowel het delen van gegevens met

andere instellingen als het inkijken en eventueel exporteren/overdragen van gegevens, vindt dan op een eenduidige manier plaats;
- Door implementatie van een regionale XDS-infrastructuur, hoeven zorgverleners niet per ziekenhuis op een ander portaal in te loggen;
- Daarnaast is het op termijn eenvoudig om tot een landelijke dekking te komen. Regionale indexen kunnen op basis van IHE -profielen (XCA / XUA) aan elkaar gekoppeld worden, waar de toestemming ook weer specifiek op is in te richten.

8.3.2 Laboratoria

Naast de ziekenhuizen wisselen ook laboratoria gegevens uit met andere zorginstellingen. Lab uitslagen worden via Edifact berichtenverkeer teruggestuurd naar de 1e lijn en via HL7-berichten naar de ziekenhuizen. Binnen ziekenhuizen is de behoefte aanwezig om de uitslagen van de 1e lijn in te kunnen zien en bij de 1e lijn is de wens om de gegevens van ziekenhuizen in te kunnen zien. Dit geldt zowel voor de klinisch chemische laboratoria, maar ook voor medische microbiologie en pathologie.

Voor de 1e lijn hebben laboratoria vaak eigen portalen en deze voldoen. Om aansluiting te krijgen met regionale en landelijke infrastructuren is het aan te raden om gegevens via een regionale IHE-XDS te ontsluiten. Ook hier geldt, dat in ieder geval een aansluiting bij een centrale IHE-XDS infrastructuur voorwaarde is, zodat er een overzicht van de medische historie van een patiënt ontstaat.

8.3.3 Overige zorginstellingen

Overige instellingen, zoals bijvoorbeeld diagnostische centra, maar ook VVT-instellingen, huisartsen en apothekers, zullen om uitwisseling met andere zorginstellingen mogelijk te maken aan kunnen sluiten bij een regionale IHE-XDS infrastructuur. Als die aansluiting wordt gerealiseerd via een regionale samenwerkingsorganisatie, kan een eenduidige oplossing worden geboden die voor alle zorgorganisaties qua techniek en governance transparant is.

8.4 Inzage van medische gegevens

8.4.1 Ziekenhuizen en laboratoria

Ziekenhuizen en laboratoria zullen meestal een directe aansluiting op een IHE-XDS infrastructuur realiseren. Voor inzage van gegevens maken zij gebruik van een eigen XDS consumer. Dit kan in eerste instantie een losse XDS consumer zijn die aan gebruikers beschikbaar wordt gesteld via een losstaande webapplicatie. Hierop moeten gebruikers dan apart inloggen en de gewenste patiënt selecteren. Het heeft veel voordelen om de XDS-consumer in het EPD te integreren. Dit biedt de mogelijkheid om SSO in te loggen en, omdat de patiënt al in het EPD is geselecteerd, hoeft de gebruiker dat niet meer apart in de viewer te doen. De XDS-consumer kan ook een PACS/VNA viewer zijn, mits die de juiste IHE profielen kan ondersteunen.

8.4.2 Overige zorginstellingen via centrale viewers

Doordat ziekenhuizen en andere zorginstellingen hun gegevens ontsluiten via een regionale IHE-XDS infrastructuur ontstaat er een regionaal koppelvlak, waar zorgverleners terecht kunnen voor hun gegevens. Niet alle zorginstellingen zullen zelf medische gegevens aanleveren, maar alle zorgverleners zullen wel behoefte hebben aan een inkijkfunctie. Deze inkijkfunctie kan worden ingevuld door het inrichten van een regionale IHE-XDS consumer, die bij voorkeur geïntegreerd vanuit het eigen EPD- of HIS-systeem wordt aangeroepen. Een andere optie is het aanbieden van een inzage portaal. Er zijn meerdere partijen op de markt die de gewenste functionaliteit bieden, waarbij sommige een zorgverlenersportaal hebben met veel

extra functionaliteiten en andere een eenvoudige inkijkfunctie met upload en download mogelijkheden. Een voorwaarde is dat de leverancier alle relevante IHE profielen ondersteunt, zodat op termijn gegevens uit andere gekoppelde regio's via hetzelfde portaal ontsloten kunnen worden. Afhankelijk van de mogelijkheden kunnen er een of meerdere regionale viewers ingezet worden.

8.5 Roadmap XDS koppelvlakken

Om als regio te starten met XDS is het aan te raden klein te beginnen en vanuit daar de IHE-XDS infrastructuur uit te bouwen.

8.5.1 IHE-koppelvlakken korte termijn (1 tot 3 jaar)

Ontsluiting van gegevens (Integratie XDS-sources)

De ontsluiting van gegevens op korte termijn zal zoveel mogelijk via standaard IHE-XDS profielen plaatsvinden. Waar mogelijk kan gestructureerde data ontsloten worden (o.b.v. ZIB's en HL7 CDA), maar als dat niet mogelijk is kunnen documenten ook als PDF, Word of in andere formaten beschikbaar worden gesteld. Voor radiologiebeelden is DICOM het standaard formaat, maar ook daar zijn andere formaten mogelijk, bijvoorbeeld .jpg.

Te ontsluiten medische gegevens worden of automatisch aangemeld op de XDS Registry of via handmatige acties aangemeld. In het uiterste geval kunnen documenten door middel van een handmatige upload worden gedeeld. Dit is geen ideale oplossing, maar als het alternatief is dat er geprint wordt en gefaxt, is het nog steeds eenvoudiger om gegevens eenmalig in IHE-XDS te zetten, waarna deze door meerdere partijen ingezien kunnen worden.

Een verdere uitwerking van de koppelvlakken voor ontsluiting van gegevens uit bronsystemen is te vinden in de bijlage 8.

Inzage van gegevens (Gebruik IHE-XDS consumer)

Voor het kunnen inkijken van gegevens binnen de ziekenhuizen zal de komende jaren veelal nog gebruik worden gemaakt van een XDS consumer die bij voorkeur met de patiëntcontext via single sign on (SSO) vanuit het EPD opgestart kan worden, waarbij het selecteren van een patiënt uitgeschakeld is binnen de XDS consumer. Zo nodig kan de consumer ook onafhankelijk van het EPD gebruikt worden. Sommige EPD's hebben al XDS consumer functionaliteit in zich en kunnen in dat geval rechtstreeks op een regionale XDS infrastructuur worden aangesloten.

Voor de inzage door derde partijen, die geen volledige aansluiting hebben, kan gebruik worden gemaakt van regionale viewers die via het internet beschikbaar kunnen worden gesteld, waarbij gegevens gedownload kunnen worden en indien nodig, geüpload kunnen worden. Bij inzage door externe partijen wordt een sterkere identificatie en authenticatie gevraagd.

Procesondersteuning middels XDW

Voor procesondersteuning tussen organisaties zal gebruik kunnen worden gemaakt van XDW (cross-enterprise document workflow) als IHE-standaard over de organisaties heen. Voor de korte termijn zullen deze XDW-processen gestart kunnen worden vanuit een losse XDS consumer, waarbij de processen zo eenvoudig mogelijk moeten worden gehouden.

8.5.2 IHE-koppelvlakken middellange termijn (3 tot 5 jaar)

Voor de middellange termijn zal worden uitgegaan van meer standaardisatie en ondersteuning van IHE profielen om gegevens te ontsluiten en te kunnen inzien.

Ontsluiting van gegevens (Integratie XDS-sources)

Op de langere termijn zullen zoveel mogelijk gegevens gestructureerd, bij voorkeur op basis van ZIB's, worden ontsloten en is het gewenst ook andere gegevens zoals verslagen niet langer als een digitale 'blob' te verzenden, maar als (semi) gestructureerde (CDA) documenten, zodat ontvangende systemen deze kunnen interpreteren en verwerken.

Inzage van gegevens (Gebruik IHE-XDS consumer)

Voor het inzien van gegevens binnen zorginstellingen zal er bij voorkeur geen gebruik meer worden gemaakt van een losse XDS consumer, maar zal het EPD de volledige XDS consumer functionaliteit bieden als native EPD-component of als geïntegreerde viewer.

Voor inzage door andere zorginstellingen dan ziekenhuizen en laboratoria, kan een regionale viewer gebruikt worden. Het streven zou echter moeten zijn om ook deze zorginstellingen op termijn direct aan te sluiten op een regionale XDS infrastructuur. Daarnaast kan gedacht worden aan toegang voor patiënten om hun toestemming aan te passen, hun eigen gegevens in te kunnen zien en in te kunnen zien wie inzage hebben gehad in hun gegevens.

Procesondersteuning (bijv. via XDW)

Naast het inkijken van gegevens binnen het EPD zal ook de procesondersteuning volledig geïntegreerd binnen het EPD plaatsvinden, waarbij HL7 orders een transmurale XDW-workflow kunnen starten. De order komt door middel van een HL7-bericht automatisch binnen bij het ontvangende EPD en is bijv. gekoppeld aan "Whatsnew" berichten. Hierdoor maakt het voor specialisten dan niet meer uit of ze onderzoeken binnen de eigen organisatie laten uitvoeren of dat deze elders plaatsvinden. De handelingen om deze onderzoeken aan te vragen is hetzelfde voor zowel intern als extern.

Formulier standaardisatie

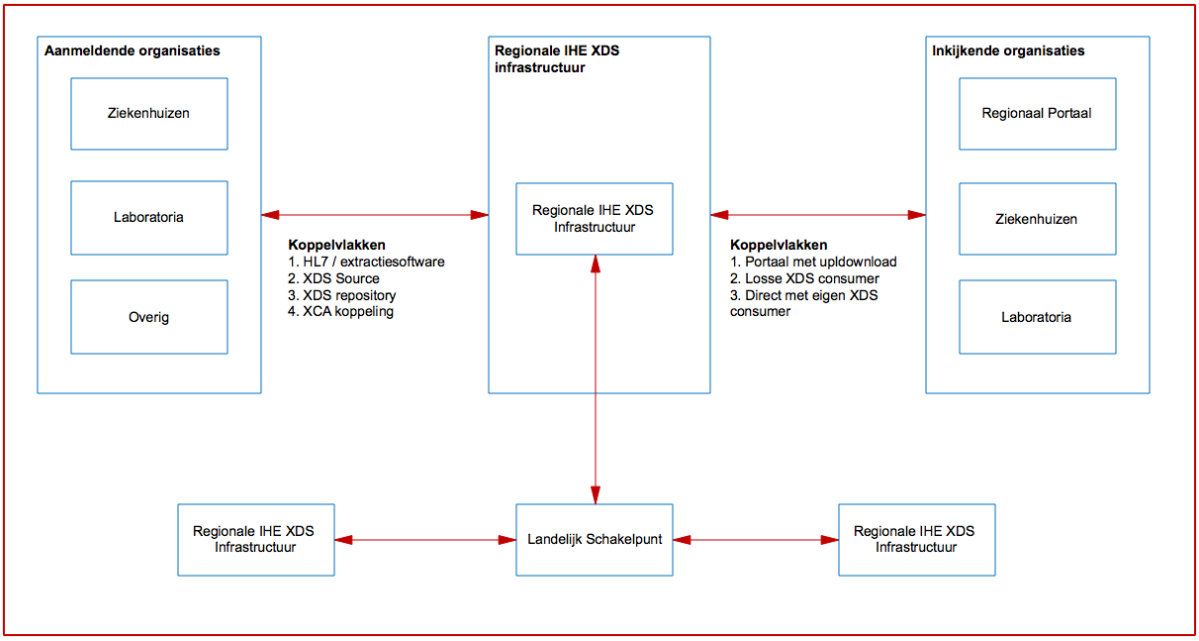
Er zijn diverse MDO-bespreekformulieren, verschillend per afdeling en per ziekenhuis. Daarnaast zijn de checklists waarop aangegeven is welke informatie nodig is bij welke verwijzing of overdracht niet hetzelfde en ontwikkeld vanuit specifieke specialismes. Bij het inrichten van nieuwe use cases op basis van XDS en XDW zal voor de diverse specialismes (bijvoorbeeld cardiologie) zoveel mogelijk vast worden gehouden aan standaard formulieren, waarbij eventuele uitzonderingen als aparte velden kunnen worden toegevoegd.

Proces standaardisatie

Tijdens DVD/CD-uitfaseringsprojecten blijkt vaak dat de huidige processen rondom uitwisselingen nu plaats vinden via formele en informele stappen en afspraken, waarbij er tussen afdelingen en andere organisaties per proces andere stappen en afspraken zijn gemaakt. Door gebruik te maken van procesondersteuning via XDW kunnen processen meer gestandaardiseerd worden en zijn ze ook beter te monitoren en te verbeteren.

8.6 Landelijke opschaling

In een samenwerking tussen VZVZ en RSO NL wordt in overleg met XDS-regio's gewerkt aan een koppeling tussen de diverse infrastructuren. Of dit een koppeling wordt tussen alle regio's onderling of dat er een landelijke infrastructuur komt, wordt steeds duidelijker (zie ook figuur 8.3). Het LSP zou een kandidaat voor een landelijk koppelingspunt kunnen zijn, maar ook de diverse XDS leveranciers streven dit na door een cloud-oplossing aan te bieden.



Figuur 8.3: koppelvlakken voor landelijke opschaling

Naast koppelingen tussen regionale Affinity Domains onderling, komt er dan ook een koppeling met het LSP.

8.6.1 LSP IHE koppeling

Het Landelijk Schakelpunt (LSP) is, zowel technisch als organisatorisch, landelijk ingericht. Het LSP wordt nu gebruikt voor de uitwisseling van medicatiegegevens en huisartsen samenvattingen. De medicatiegegevens worden zowel uitgewisseld tussen huisartsen en apothekers, maar ook tussen de 1e en 2e lijn voor het actuele medicatiedossier. Voor gegevens, zoals beelden, verslagen, specialistenbrieven en lab uitslagen wordt het LSP nu (nog) niet ingezet.

Er is een succesvolle proef geweest met een koppeling tussen XDS en het LSP om met een XDS viewer het LSP te bevragen en andersom. Daarbij kunnen twee situaties worden onderscheiden:

- het verschaffen van medicatiegegevens uit het LSP, via een XDS infrastructuur;
- het verschaffen van labuitslagen uit een XDS affinity domain, via het LSP.

Zie bijlage 9 voor meer details over de koppeling tussen XDS en het LSP.

8.7 Adviezen

- Het is aan te raden eerst de aandacht te richten op het ontsluiten van bronsystemen (sources) en pas later te investeren in workflow ondersteuning en uitgebreidere viewing;
- Per use case moeten eindgebruikers aangeven welke gegevens klinisch relevant zijn voor delen via XDS;
- Volg de landelijke ontwikkelingen op het gebied van standaardisatie van gegevens;
- Ontsluit medische gegevens in regionaal verband indien mogelijk via een regionale XDS infrastructuur;
- Maak en volg een roadmap, waarbij een IHE-XDS infrastructuur stap voor stap wordt opgebouwd en opgeschaald
    - Breng in eerste instantie alleen die koppelingen tot stand die noodzakelijk zijn om het systeem te gebruiken;
    - Voeg daar vervolgens koppelingen aan toe die de bestaande situatie telkens iets dichter bij de ideale situatie brengt.

9 IT-Infrastructuur - Servers, netwerken en security

Een technische infrastructuur bepaalt op welke manier de betrokken informatiesystemen gegevens uitwisselen. De infrastructuur is nodig voor de daadwerkelijke digitale gegevensoverdracht tussen de systemen in zorginstellingen. Op dit niveau worden afspraken vastgelegd over ontwerp en inrichting van servers, netwerken, IP-nummers, SAML tokens, certificaten en andere onderdelen die de systemen technisch met elkaar verbinden.

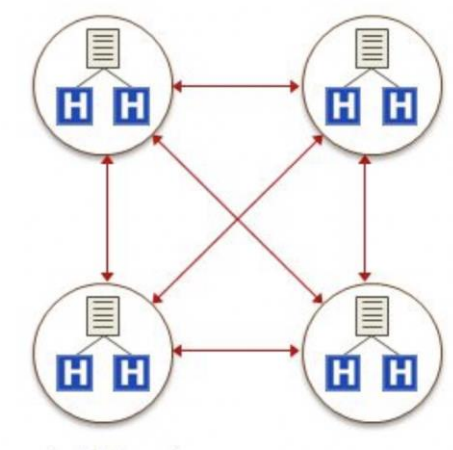
Dit hoofdstuk start met een overzicht van de mogelijkheden om Affinity Domains aan elkaar te koppelen op basis van het IHE XCA-profiel. Vervolgens wordt ingegaan op de architectuur en de basiseisen die gelden binnen een Affinity Domain en tussen Affinity Domains.

9.1 Architectuur Affinity Domains

Voor het koppelen van Affinity Domains met behulp van IHE XCA zijn verschillende architecturen ofwel topologieën, mogelijk. De keuze voor een architectuur is afhankelijk van strategische keuzes van zorginstellingen en RSO's en wordt daarnaast beïnvloed door reeds bestaande infrastructuren of initiatieven.

9.1.1 Bilaterale koppeling tussen Affinity Domains

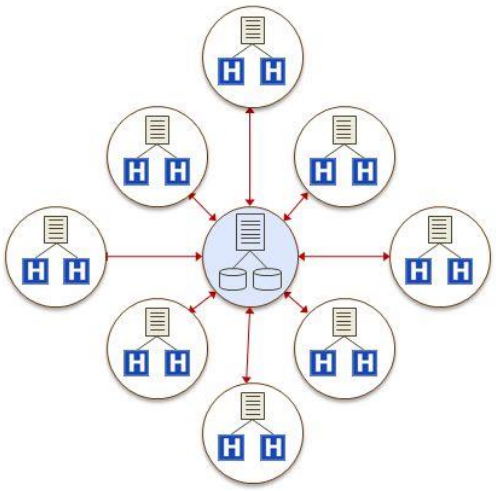
Het bilaterale model (figuur 9.1) gaat uit van een point-to-point configuratie tussen de verschillende IHE-XDS Affinity Domains. Elk Affinity Domain heeft een lijst met andere Affinity Domains en kan deze via een onderliggende netwerk infrastructuur bereiken. De 'cirkels' in de schema's vertegenwoordigen XDS Affinity Domains, waarin schematisch één Registry (lijst) en twee zorginstellingen(H) zijn weergegeven. Per Affinity Domain kunnen meer dan twee zorginstellingen zijn aangesloten.



Figuur 9.1: Bilaterale koppeling van Affinity Domains

9.1.2 Stervorm van Affinity Domains

De stervorm is een model, waarbij een centrale Responding Gateway wordt ingericht, die een verbinding legt met andere Affinity Domains (figuur 9.2). In dit model sluiten alle Affinity Domains aan op één centrale 'hub'. Een voordeel is, dat elk Affinity Domain slechts één verbinding naar buiten heeft. De centrale hub kan daarnaast specifieke extra taken gaan vervullen, zoals services op het gebied van landelijke lijsten, een hoge kwaliteit authenticatie, autorisatie, en andere diensten. Een nadeel is de afhankelijkheid van één centrale hub en het aantal verbindingen dat vanuit één hub moeten worden bediend. Daarnaast zijn er juridische en organisatorische vraagstukken die tussen twee zorginstellingen vaak eenvoudiger zijn te organiseren en af te stemmen.



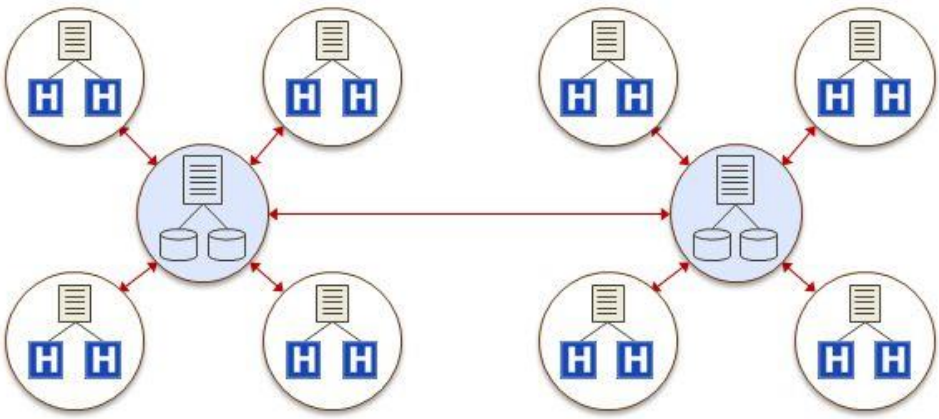
Figuur 9.2: Affinity Domains gekoppeld via stervorm

9.1.3 Multi-ster vorm

In zowel het bilaterale model als de stervorm worden gegevens uitgewisseld binnen het eigen Affinity Domain en via verbindingen tussen Affinity Domains. De optimale architectuur, bilateraal, stervorm of een combinatie, hangt af van het aantal aan te sluiten Affinity Domains. Wanneer er slechts twee Affinity Domains zijn, lijkt een XCA gateway tussen twee Affinity Domains de meest logische optie. Naarmate het aantal Affinity Domains stijgt, neemt het beheer toe van het bilaterale model vanwege de lange lijst van Affinity Domains die per Affinity Domain moeten worden bijgehouden.

Daarnaast is er een ontwikkeling gaande dat steeds meer zorginstellingen kiezen voor een eigen individueel Affinity Domain, waarbij de uitwisseling van gegevens plaatsvindt door te koppelen met Affinity domains van andere zorginstellingen en regio's. De infrastructuur wordt gezien als onderdeel van de eigen zorginstelling, waardoor alle eigen medische gegevens onder de verantwoordelijkheid van de zorginstelling geregistreerd kunnen worden en niet opvraagbaar zijn door andere zorginstellingen. Dit registreren kan plaatsvinden zonder dat patiënt toestemming heeft gegeven om die met anderen te delen. Als de trend van een Affinity Domain per zorginstelling doorzet, zal het aantal Affinity Domains dusdanig toenemen dat een stervorm van alle 50 tot 60 Affinity Domains op nationale schaal nodig is. Het inzetten van een lokalisatie service zal dan nodig zijn, om te voorkomen dat per uitwisseling elke keer alle Affinity Domains worden bevraagd . De lokalisatie service legt vast welke Affinity Domains informatie van een bepaalde patiënt hebben, zodat bij het opvragen van gegevens van een patiënt alleen die Affinity Domains bevraagd worden, waar de patiënt bekend is.

Naast het bilaterale model en het stermodel, zou het bij het grote aantal Affinity Domains verstandig zijn om meerdere regionale sterren van Affinity Domains in te richten die onderling zijn verbonden, waarbij meerdere centrale Affinity Domains ontstaan (figuur 9.3).



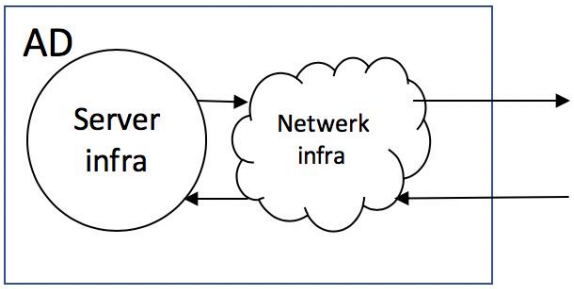
Figuur 9.3 - Multi-ster model van Affinity Domains

Het voordeel is dat dit een flexibel model is dat kan worden opgebouwd met behoud van de momenteel aanwezige Affinity Domains. Het principe is, dat een aantal Affinity Domains in een wat grotere regio aansluiten bij een (super-) regionaal Affinity Domain. Dit Affinity Domain vormt het schakelpunt naar andere Affinity Domains. Het kan een nadeel zijn dat deze Affinity Domains dan volledig interoperabel moeten zijn en er geen centraal punt is van waaruit extra services kunnen worden geleverd. Daar staat tegenover dat meerdere hubs elkaars functionaliteit en data kunnen dupliceren waardoor ze elkaars functie in het geval van storingen kunnen overnemen.

De keuze voor een bepaalde topologie en de beschikbaarheid van bepaalde componenten zal vastgesteld moeten worden in overleg met architecten van zorginstellingen, regio's en landelijke partijen.

9.2 Technische gegevens per Affinity Domain

De technische infrastructuur van een Affinity Domain bestaat uit servers die via een netwerk aan elkaar gekoppeld zijn (figuur 9.4).



Figuur 9.4: Koppeling Affinity Domain via netwerk

Dit is een eenvoudige weergave van de werkelijkheid, waarbij het Affinity Domain zelf ook weer een complexe IT-infrastructuur kan hebben. Deze is echter voor het uitwisselen van gegevens tussen Affinity Domains niet relevant, aangezien de afspraken gelden voor de koppelvlakken waarop Affinity Domains met elkaar communiceren. Per IT-component binnen de server-infrastructuur moet goed gedocumenteerd worden wat de gegevens zijn van elke component en waar deze mee gekoppeld is. (Zie bijlage 10 voor een voorbeeld).

9.2.1 Eisen aan het individuele Affinity Domain

- De verantwoordelijk voor het beheer van de server- en netwerkinfrastructuur kan bij verschillende partijen liggen. Voor deze beheerorganisatie(s) geldt dat zij ISO 27001:2013 gecertificeerd moeten zijn

voor alle componenten en organisatieonderdelen die betrokken zijn bij het beleid en beheer van het Affinity Domain;
- De beheerpartij voor de server infra moet NEN7510 gecertificeerd zijn;
- Te overwegen valt om de serverinfra ook te toetsen aan de relevante GBX eisen (GBX, 2018), en de netwerkinfra aan de relevante GZN (GZN, 2018) eisen;
- Zowel voor het inkomende als uitgaande verkeer beschikt het Affinity Domain over een gegarandeerde bandbreedte van 50Mb. Gelet op de praktijk is dit een minimum. Studies worden steeds groter en een minimale bandbreedte van 1Gb of hoger is op termijn wenselijk;
- De performance van een Affinity Domain moet voldoen aan de binnen dat domein geformuleerde performance eisen;
- Een Affinity Domain maakt gebruik van publiek IP.

9.2.2 Eisen gerelateerd aan de community van Affinity Domains

- Landelijk wordt minimaal één keer per jaar een hack en pentest op de deelnemende Affinity Domains uitgevoerd door een onafhankelijke partij. Binnen de netwerken (Affinity Domains) zelf is dit een verantwoordelijkheid van het netwerk zelf;
- Afhankelijk van de SLA, is de verbinding tussen Affinity Domains redundant uitgevoerd;
- Tussen Affinity Domains is een minimum SLA afgesproken waarin is opgenomen:
    - Beschikbaarheid
    - Bereikbaarheid serviceorganisatie tijdens kantooruren
    - Bereikbaarheid serviceorganisatie buiten kantooruren;
- Tussen de diverse deelnemers is een IP plan afgestemd. Dit om te voorkomen dat hierin conflicten ontstaan. Dit IP plan is voor alle deelnemers inzichtelijk. Afhankelijk van de gebruikte techniek is een algemeen BGP nummerplan, dan wel routerplan beschikbaar;
- Het is aan te raden om een (centrale) DNS infrastructuur in te richten, inclusief een DNS naamgevingsconventie;
- Bij het gebruik van certificaten geldt een minimale sleutelsterkte. Deze wordt jaarlijks door de deelnemers beoordeeld en zo nodig aangepast;
- Wijzigingen in de infrastructuur worden door deelnemers binnen een periode van één jaar gerealiseerd;
- Er is een landelijk OID-plan voor alle IHE-XDS componenten, waarvan de basis OID's door NICTIZ worden beheerd;
- Er is een landelijk uniform overzicht van rollen die binnen de Affinity Domains dezelfde autorisaties kennen;
- Communicatie protocollen en het berichtenverkeer tussen Affinity Domains moeten gedocumenteerd zijn.

9.3 Adviezen

- Maak een keuze hoe Affinity Domains in de regio en landelijk gekoppeld gaan worden;
- De keuze voor een bepaalde topologie en de beschikbaarheid van bepaalde componenten zal vastgesteld moeten worden in overleg met architecten van zorginstellingen, regio's en landelijke partijen;
- Documenteer alle IT-componenten en hun onderlinge verbanden in een technisch overzicht.

10 Testmanagement

Dit hoofdstuk gaat over het testen van de interoperabiliteit binnen een regio en tussen regio's. Er wordt gestart met een lijst van randvoorwaarden om goed testmanagement uit te voeren. Vervolgens wordt ingegaan op de verschillende testen en het belang van een testset. Dit hoofdstuk eindigt met de wens voor een landelijke testomgeving, waar de verschillende use cases tegenaan getest kunnen worden.

10.1 Randvoorwaarden testmanagement

10.1.1 OTAP-omgeving

Bij het ontwikkelen van software is het toepassen van de OTAP-methode (Ontwikkeling, Test, Acceptatie en Productie) een gemeengoed. Ook bij RSO's en zorginstellingen is dit een relevante methodiek voor de ontwikkeling/implementatie van infrastructuren voor gegevensuitwisseling. Doel van deze methode is om de software in een bepaald stadium te bevriezen en die daarna over te zetten naar de hogere laag binnen dit model, bijvoorbeeld van Test naar Acceptatie. Dit voorkomt het opnieuw ontwikkelen en testen van configuraties die in de vorige laag reeds zijn uitgewerkt. Het uiteindelijke doel is het realiseren van een goed functionerende Productieomgeving.

Ontwikkeling van softwarecomponenten vindt vaak plaats bij de leverancier, die over een Ontwikkel- en Testomgeving beschikt. Daarna wordt de configuratie overgezet naar een Test-/Acceptatieomgeving bij een RSO of zorginstelling. In veel gevallen, om complexiteit en kosten te reduceren, beschikt de zorgorganisatie of de RSO alleen over een Acceptatieomgeving en Productieomgeving. Hoewel het samenvoegen van een Test- en Acceptatieomgeving op de korte termijn handig of goedkoper lijkt, kan dit ook veel extra werk met zich meebrengen. In de praktijk gebeurt het vaak dat op de samengevoegde Test-/Acceptatieomgeving nog veel ontwikkeling en configuratie plaatsvindt. Gevolg is dat de Acceptatieomgeving niet stabiel is, door het steeds wijzigen van de opbouw/configuratie, waardoor testen steeds opnieuw uitgevoerd moeten worden omdat eerder geteste onderdelen niet meer werken. Op de lange termijn brengt dit extra ontwikkelwerk (van de leverancier) met zich mee evenals het testen van de componenten.

Het advies vanuit RSO Nederland is om zowel een Test- als een Acceptatieomgeving te hebben. Zowel binnen een zorginstelling als binnen een centrale RSO-omgeving.

In de praktijk blijkt dat een Productieomgeving, van RSO's of zorginstellingen, niet altijd 100% gelijk is aan een Acceptatieomgeving. Dit geldt zowel voor de softwareconfiguraties die van elkaar verschillen, maar ook voor de hardware waarop de diverse softwarecomponenten zijn geïnstalleerd. Een acceptatieomgeving wordt vaak op één serveromgeving geïnstalleerd om kosten te besparen, terwijl deze op productie over meerdere servercomponenten verdeeld is. Een voorbeeld hiervan is het inzetten van een redundante omgeving, een registry met bijbehorende componenten zoals een BPPC repository en ATNA repository, op een Productieomgeving. In deze redundante configuratie zorgt een load balancer voor het routeren van binnenkomend verkeer. Doordat een acceptatieomgeving vaak enkel is uitgevoerd, zonder load balancer, kan het testen van de load balancer alleen op productie plaatsvinden. Dit is ongewenst, omdat elke test op productie afgestemd moet zijn met alle betrokken partijen, dit vaak in de avonduren moet plaatsvinden en er een roll-back mogelijk moet zijn die grote gevolgen kan hebben.

RSO Nederland adviseert om de Acceptatieomgeving als een exacte kopie van de Productieomgeving neer te zetten.

Daarnaast adviseert RSO Nederland om de gelijke inrichting van beide omgevingen (Acceptatie en Productie) mee te nemen in het contract als de software wordt aangekocht, zodat de leverancier daarvoor geen meerkosten in rekening brengt.

10.1.2 Testplan/script, testscenario's, test-sets

Voorafgaand aan het testen is het wenselijk om een goed uitgewerkt testscript te hebben. Een testscript geeft inzicht in onder andere de volgende activiteiten:

- Wat zijn de handelingen/transacties om te testen;
- Welke componenten zijn betrokken en hebben gezamenlijke transacties;
- Wat zijn de verwachte resultaten van de test;
- Wat zijn de behaalde resultaten van de test;
- Wat zijn de acties naar aanleiding van de bevindingen.

En groot voordeel van het hebben van een vooraf uitgewerkt testscript is dat een test na afloop goed gedocumenteerd is. Daarnaast zijn bevindingen de volgende keer makkelijker opnieuw te testen onder dezelfde condities.

Een testscript kent een aantal hoofdonderdelen. Dat zijn:

- Verbindingen/configuratie: bij dit onderdeel staat het testen van de verbinding centraal, kortom hebben de partijen connectie met elkaar (bijvoorbeeld door ping en telnet testen);
- Aanmelden (source kant): de aanmeldende partij test een aantal keren het aanmelden van gegevens, zoals een consent-document, verwijsbrieven, onderzoeksverslagen. Tevens valt het aanmelden van beelden onder dit onderdeel. Het soort beelden (echo, MRI, CT-scan) en documenten is afhankelijk van hetgeen de betrokken partijen met elkaar willen testen (de use case);
- Opvragen (consumer kant): De opvragende partij zal bij dit onderdeel de eerder aangemelde beelden en documenten, welke door de aanmeldende partij zijn uitgevoerd, ophalen. Van belang is of alle gegevens zonder kwaliteitsverlies aan de andere kant beschikbaar zijn;
- Registry en Logging: vanuit een centraal punt, bijvoorbeeld de RSO, is het mogelijk om zaken als metadata en ATNA-log gegevens te beoordelen. Deze gegevens dienen conform de geldende aansluitvoorwaarden beschikbaar te zijn;
- Aanvullende testen: dit zijn zaken die te maken kunnen hebben met gebruikte servercertificaten, URA-namen, performance testen.

Vervolgstap is om het testscript aan te laten sluiten op de te testen use-case(s), bijvoorbeeld het traject verwijzing kinderorthopedie of longgeneeskunde.

In het testscript moeten go/nogo momenten aanwezig zijn. Dit kan alleen als vooraf heldere testdoelen opgesteld zijn waarbij de use case en het testproces zijn bepaald.

Qua volgordelijkheid is het advies om eerst binnen de eigen organisatie een testscript op te stellen en uit te voeren voor alle "interne" verbindingen en systemen om vervolgens een testscript te doorlopen met een externe partij.

10.2 Update & Upgrade planning (releasemanagement)

De softwarecomponenten van RSO's dienen ook met enige regelmaat een update te krijgen. Aan de ene kant voor nieuwe functionaliteiten en aan de andere kant voor noodzakelijke (beveiligings-) updates. Ook hier geldt dat de aangesloten zorginstellingen deze nieuwe software moeten testen.

Een RSO kan zelf bepalen hoeveel keer per jaar een update/upgrade noodzakelijk is. Deze upgrade planning moet een RSO afstemmen met de aangesloten zorginstellingen.

De eerste stap is om de update/upgrade uit te voeren op de acceptatieomgeving. En vier tot zes weken later op de productieomgeving.

Iedere aangesloten zorginstelling heeft twee weken de tijd om te testen op de acceptatieomgeving. Eventuele bevindingen zullen de twee weken erna door de leverancier opgelost moeten worden. Waarna weer twee weken beschikbaar zijn om de oplossingen te testen.

De nieuwe release wordt voorzien van een:

- impactanalyse van de leveranciers van de centrale infrastructuur;
- release notes.

In het geval van incidenten, grote bugs en/of nieuwe functionaliteiten kan dit leiden tot extra/spoed updates en/of "hotfixes". Indien dit het geval is zal afstemming met de aangesloten zorginstellingen plaatsvinden om de uitvoering zo snel mogelijk te realiseren.

10.3 Technische-, Functionele-, Keten- en Acceptatietests

Een risico bij het testen is dat te veel zaken tegelijk in één test gedaan worden. Bijvoorbeeld een test van aanmelden van een document tot en met het inzien ervan door een andere zorginstelling. Gevolg hiervan is dat als zich een probleem voordoet, het vaak moeilijk is te achterhalen wat de oorzaak is. Winst is te behalen als testscripts worden uitgewerkt voor afzonderlijke transacties. Hierbij is het voordeel dat als er iets misgaat, het zoeken naar de oorzaak meer gericht is dan bij het testen van een groter proces van meerdere transacties.

10.3.1 Technisch testen

De eerste stap in het testen, de technische test, is een testscript dat bestaat uit afzonderlijk te testen transacties. Een afzonderlijke transactie is hierbij de gegevensoverdracht tussen twee systemen, er is geen sprake van een keten van gegevensoverdracht. Een transactie is bijvoorbeeld het aanmelden van een consentdocument tussen een bronsysteem en een repository of het registreren van een document vanaf de repository naar een registry.

Voordat gestart wordt met functionele- of ketentesten, is het noodzakelijk dat alle technische testen met goed resultaat zijn afgerond.

10.3.2 Functionele Testen

Na afronden van de technische testen volgen de functionele testen. De focus hierbij is of de software doet wat het moet doen. Is bijvoorbeeld toegang tot de IHE-XDS consumer alleen mogelijk via de afgesproken manier van authenticatie? Of is het mogelijk om een opgevraagd document op te slaan in een EPD?

Aan de andere kant moet ook controle plaatsvinden dat de software niet doet wat het niet moet doen. Denk hierbij aan het intrekken van een consent dat moet leiden tot het niet langer kunnen inzien van gerelateerde documenten. Wenselijk is het om bij de functionele testen ook een superuser, één van de eindgebruikers, betrokken te hebben. De samenstelling van een testteam is weergegeven in tabel 10.1.

10.3.3 Ketentesten

Als deze twee testonderdelen zijn afgerond, kan een ketentest plaats vinden. De gedachte hierachter is om de gehele use case te testen zoals die ook in de praktijk plaats zal vinden. Bijvoorbeeld het gehele proces

van het verwijzen van een longpatiënt naar een andere zorginstelling voor verdere behandeling waarbij het mogelijk is relevante documenten zoals de verwijsbrief en beelden zoals CT's uit te wisselen. Als de technische- en functionele testen met goed resultaat zijn afgerond, is te verwachten dat de ketentest zonder al te veel problemen uit te voeren is.

10.3.4 Acceptatietesten

Het laatste onderdeel van testen omvat de acceptatie van de oplossing door gebruikers, dit zijn de zorgverleners die daadwerkelijk met de software aan de slag gaan. De focus van deze test is of een gebruiker goed kan werken met de aangeboden oplossing. Idealiter zijn gebruikers of superusers eerder in het proces al betrokken geweest om hier feedback op te geven. De acceptatiecriteria en testdoelen dienen van tevoren vastgelegd te zijn.

Door het volgen van deze vier teststappen is te verwachten dat de totale testinspanning, en het aantal adhoc testen, lager is dan zonder het volgen van deze structuur.

Advies is dan ook om deze vier teststappen vooraf uit te werken en in te laten vullen door de juiste personen.

10.4 Samenstelling test team

Bij de samenstelling van het testteam in tabel 10.1, is een onderverdeling gemaakt in de vier teststappen van: technisch-, functioneel-, keten- en acceptatietest. Afhankelijk van het soort test en de use case is de samenstelling van dit team naar eigen inzicht in te vullen. De tabel is zowel voor interne als externe testen toe te passen.

Teststap Testrol	Technisch	Functioneel	Keten	Acceptatie
Zorginstelling testmanager	x	x	x	x
Zorginstelling projectleider	(x)	(x)	x	x
Zorginstelling netwerkbeheer	x	(x)	(x)	(x)
PACS/VNA-beheerder	x	x	x	x
EPD-beheerder	x	x	x	x
Super-user	-	x	x	(x)
Gebruiker	-	-	x	x
Leverancier	(x)	(x)	(x)	(x)
RSO testmanager	(x)	(x)	(x)	(x)

Tabel 10.1: Samenstelling testteam. Legenda: x, dient aanwezig te zijn. (x), optionele aanwezigheid.

10.4.1 Melden bevindingen testen aan RSO

Testen op het niveau van Techniek en/of Functionaliteit om informatiedeling over de RSO-infrastructuur mogelijk te maken, is de verantwoordelijkheid van de aangesloten zorginstellingen, tenzij anders is afgesproken. Hierbij is het noodzakelijk dat het testen plaatsvindt met een andere zorgpartij binnen de RSO of daarbuiten in het geval van bovenregionale uitwisseling. RSO's hebben over het algemeen geen faciliteiten beschikbaar om een externe zorginstelling te simuleren.

Mochten er bij het testen issues gevonden worden, dan zijn de zorgpartijen eerst zelf aan zet om het probleem (eventueel met de eigen leverancier) op te lossen. Als blijkt dat het probleem centraal bij de RSO ligt, dan kan deze daar gemeld worden.

Bij het melden van issues (zowel op Acceptatie als Productie) moeten de volgende zaken gedocumenteerd zijn zodat de RSO het issue snel kan oppakken:

- Functionele beschrijving van het onderdeel dat is getest en dat een issue oplevert;
- Beschrijving van het eigenlijk verwacht resultaat van het geteste onderdeel;
- Welke systemen/componenten zijn hierbij betrokken;
- Beschrijving van de acties die zijn uitgevoerd om het issue aan te pakken.

Ontbreken van eigenaarschap van het issue dient voorkomen te worden.

Het is aan te raden om vanuit de regio een testmanager aan te stellen die de gehele coördinatie op zich neemt en zowel medewerkers van zorginstellingen en leveranciers er actief bij betrekt.

10.5 Testpatiënten

Binnen een Affinity Domain zijn de verschillende zorginstellingen vaak actief bezig met configuraties en het testen van gegevensuitwisseling. Dit kan bijvoorbeeld het geval zijn bij het in gebruik nemen van nieuwe versies/releases van een PACS of EPD of wanneer een nieuwe use case wordt geïmplementeerd. Testen van alle componenten voor gegevensuitwisseling is ook dan noodzakelijk.

Om gegevensuitwisseling te testen met een andere zorginstelling, is het gewenst een goede set testpatiënten met gedeelde testdocumenten en beelden beschikbaar te hebben. Een zorginstelling wil soms tussendoor één of twee dingen testen en daarbij moet een afhankelijkheid van aanwezige personen uit een andere zorginstelling die testgegevens klaar moeten zetten, voorkomen worden. Die afhankelijkheid vraagt namelijk extra inspanning en kan zorgen voor vertraging bij het testen. Daarnaast biedt het hebben van vaste testpatiënten en testdata ook voor demo doeleinden grote voordelen.

Iedere aangesloten zorginstelling moet er daarom voor zorgen een set van testpatiënten gereed te hebben met daaraan gekoppelde testdata. Advies is om per instelling altijd minimaal zes testpatiënten beschikbaar te hebben, waarvan drie vaste en drie variabele testpatiënten. Dit geldt zowel voor de Acceptatie- als voor de Productieomgeving.

10.5.1 “Vaste” testpatiënten

Elke zorginstelling heeft altijd minimaal drie vaste testpatiënten beschikbaar waarbij:

- Twee testpatiënten met consent voor het delen van medische informatie en één testpatiënt zonder consent (bezwaar voor delen medische informatie);
- De vaste testpatiënten met consent hebben een voor de instelling representatieve gepubliceerde set documenten en beelden beschikbaar voor het delen met andere zorginstellingen. Deze set is afhankelijk van de use case(s);
- De vaste testpatiënten worden nooit geschoond, uit de source/repository bij de zorginstelling;
- De vaste testpatiënten worden nooit geschoond, uit de registry, bij de RSO;
- De vaste testpatiënten zijn altijd beschikbaar voor eigen testen en testen vanuit andere zorginstellingen;

- Om vervuiling van de gegevens set van vaste testpatiënten tegen te gaan, is het niet toegestaan om beelden of documenten toe te voegen of te verwijderen;
- De aanwezige set van beelden en documenten zijn bekend bij de zorginstellingen waarmee uitwisseling plaatsvindt;
- Er zijn CIBG (VZVZ) testpatiënten beschikbaar en in de regio dienen er afspraken gemaakt te worden, zodat er geen onduidelijkheid ontstaat over gebruik door meerdere instellingen van dezelfde patiënt.

10.5.2 "Variabele" testpatiënten

Elke zorginstelling heeft altijd minimaal drie variabele testpatiënten beschikbaar waarbij:

- Consent voor het delen van medische informatie wel of niet aanwezig mag zijn;
- Geen verplichting is met betrekking tot gekoppelde beelden en/of documenten aan een testpatiënt. Dit is per test te bepalen of af te stemmen;
- De data van de variabele testpatiënten mag geschoond worden bij een zorginstelling en/of een RSO. Wel moet dit bij de andere testpartners en/of RSO bekend zijn gemaakt (informatieplicht);
- De variabele testpatiënten zijn altijd beschikbaar, de achterliggende data kunnen echter variëren;
- Aanwezige beelden en documenten hebben een wisselend karakter en hoeven niet bekend te zijn bij andere instellingen;
- De noodzaak van variabele testpatiënten ligt vooral bij het uitvoeren van "technische" testen. Dit omdat de te testen beelden en/of documenten bij een specifieke transactie kunnen plaatsvinden.

10.5.3 Aanvullende voorwaarden testpatiënten

- Dit geldt zowel voor Acceptatie- als Productieomgeving. Voor beide omgevingen dient een vaste en variabele set van testpatiënten aanwezig te zijn;
- De BSN's zijn bekend bij de instellingen waarmee uitwisseling plaatsvindt;
- Testpatiënten hebben geldige fictieve BSN's (fBSN), zoals uitgegeven door vZVZ. (NB. Sommige systemen kunnen niet goed met fictieve BSN's overweg);
- Zorginstellingen bieden zelf het overzicht van de beschikbare testpatiënten en beschikbare testbeelden en documenten;
- Een RSO kan de taak op zich nemen om dit overzicht voor alle aangesloten partijen bij te houden en te delen.

10.6 Landelijke testvoorziening

In deze handreiking staat een aantal adviezen en afspraken waaraan RSO's zich moeten houden om binnen de regio en buiten de regio op elkaar aan te kunnen sluiten. Een landelijke voorziening waar use cases getest kunnen worden om de naleving van deze (technische) afspraken te toetsen kan hieraan een bijdrage leveren.

10.7 Adviezen

- Zet zowel een Test- als een Acceptatieomgeving op. Zowel binnen een zorginstelling als binnen een centrale RSO-omgeving;
- Zorg dat de Acceptatieomgeving altijd identiek is aan de Productieomgeving. Elke wijziging wordt eerst op acceptatie uitgevoerd en na validatie overgezet op productie;

- Neem de inrichting van beide omgevingen (Acceptatie en Productie) mee bij de aankoop van de software en implementatie, zodat de leverancier daar achteraf geen meerkosten voor in rekening brengt;
- Stel eerst een testscript op voor het testen van alle interne systemen en verbindingen in de eigen zorginstellingen en vervolgens een testscript om te testen met een externe partij;
- Volg de vier teststappen: technisch-, functioneel-, keten- en acceptatietesten. Werk deze vooraf uit en stel de juiste personen op binnen het testteam;
- Stel een testteam samen volgens de richtlijnen in dit hoofdstuk;
- Elke zorginstelling biedt minimaal drie vaste en drie variabele testpatiënten en zet deze ook klaar binnen de eigen zorginstelling;

11 Toetsingskader handreiking Interoperabiliteit

In dit hoofdstuk is een toetsingskader beschreven om een samenwerkingsverband of een zorginstelling die gebruik maakt van IHE-XDS in staat te stellen de eigen Affinity Domain inrichting met bijbehorende processen en afspraken te kunnen toetsen tegen de handreiking interoperabiliteit.

11.1 Toelichting

- Het toetsingskader kan gebruikt worden om bestaande Affinity Domains te toetsen, maar ook voor de aansluiting van een nieuwe Affinity Domain en kan zowel ingezet worden voor een specifieke use case als voor alle use cases die reeds in gebruik zijn;
- De toetsingselementen beschrijven criteria voor de beoordeling van een (te koppelen) Affinity Domain of een zorgorganisatie binnen een Affinity Domain. De toetsingscriteria beschrijven de eisen en aansluitvoorwaarden waaraan een Affinity Domain moet voldoen om te kunnen koppelen aan andere Affinity Domains;
- De toetsingselementen zijn beschreven vanuit het perspectief van een toetser/auditor in zo concreet mogelijke, meetbare criteria die meestal met een 'Ja' of 'Nee' beantwoord kunnen worden. Bijvoorbeeld: "Het Affinity Domain maakt gebruik van …".

De toetsingscriteria kunnen in principe opgedeeld worden in twee categorieën:

1. Algemene criteria voor gegevensuitwisseling in de zorg;
2. IHE-XDS Affinity Domain specifieke criteria.

De algemene criteria zijn niet specifiek voor IHE interoperabiliteit maar generiek voor alle vormen van gegevensuitwisseling in de zorg. Dit betreft bijvoorbeeld criteria voortkomend uit wet- en regelgeving. Deze algemene criteria zijn niet opgenomen in dit toetsingskader voor IHE Interoperabiliteit. In plaats daarvan wordt verwezen naar bestaande criteria op dit gebied, bijvoorbeeld de NFU-criteria.

Alleen de IHE specifieke criteria zijn onderwerp van het toetsingskader in deze Handreiking.

11.2 Toetsingskader IHE Interoperabiliteit

11.2.1 Algemene IHE-gerelateerde eisen

13. Het IHE-XDS Affinity Domain maakt gebruik van de open internationale IHE standaarden en profielen. De leverancier van de IHE-XDS infrastructuur kan hiervan de certificaten overleggen.
14. Het IHE-XDS Affinity Domain beschikt over een actueel overzicht van ondersteunde standaarden en profielen.
15. Het IHE-XDS Affinity Domain ondersteunt tenminste de volgende profielen:
    a. XCA – Cross Community Access;
    b. XCA-I (Cross community Acces for Imaging;
    c. XDS -Cross Enterprise Document Sharing;
    d. XDS-I Cross Enterprise Document Sharing for Imaging;
    e. XDW – Cross Enterprise Document Workflow (optioneel);
    f. XUA - Cross-enterprise User Assertion;
    g. BPPC – Basic Patient Privacy Consent;
    h. ATNA - Audit Trail and Node Authentication;
    i. CT - Consistent Time;

j. XCPD - Cross Community Patient Discovery.

11.2.2 Wet en Regelgeving

16. Zorgaanbieders die gegevens van hun patiënten delen via een XDS-infrastructuur, hebben een Verwerkersovereenkomst gesloten met de RSO die deze dienst beschikbaar stelt of rechtstreeks met de XDS-leverancier.
17. Indien er sprake is van een RSO die de IHE-XDS diensten zelf weer afneemt van een IHE-XDS leverancier, dan heeft de RSO subverwerkersovereenkomsten afgesloten met de IHE-XDS leverancier.
18. De verwerkersovereenkomsten voldoen aan het model van de Branche Organisaties Zorg.

11.2.3 Gebruik van metadata

19. Het gebruik van metadata door het Affinity Domain moet voldoen aan de vigerende versie van de standaard IHE-XDS metadata op de Nictiz website (https://www.nictiz.nl/XDSmetadata).
20. Het Affinity Domain houdt een Spreadsheet bij ('XDS Metadatacode Set') met een actuele beschrijving van de set in gebruik zijnde metadata elementen met hun toegestane waardenlijsten, zoals die zijn geconfigureerd in de IHE-XDS Registry.
21. Binnen het Affinity Domain is een procedure ingericht die ervoor zorgt dat alle organisaties in het domein dezelfde en meest recente versie van de standaard metadata gebruiken, en aanpassingen in de XDS metadataset binnen een afgesproken termijn worden doorgevoerd.
22. Nieuwe participanten kunnen alleen bij een Affinity Domain aansluiten als het gebruik van de XDS metadata voldoet aan de standaard XDS metadata (aansluitvoorwaarde).
23. Het Affinity Domain maakt gebruik van het landelijke OID-plan. Gebruik van eigen OID's is niet toegestaan om verwarring te voorkomen. NICTIZ beheert de root OID's per AD.
24. De inrichting en het beheer van het IHE-XDS Affinity Domain en het dagelijks gebruik van de IHE-XDS functionaliteit, voldoen aan wet- en regelgeving en de professionele normen voor ICT in de zorg, zie hiervoor separate toetsingskaders. Het gaat om:
    a. AVG;
    b. Wet Cliëntenrechten bij elektronische verwerking van gegevens;
    c. Wabvpz - Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg;
    d. WGBO;
    e. Richtlijn EGiZ-2016;
    f. NEN7510, 7512, 7513

25. De samenwerkende organisaties binnen een Affinity Domain, hebben een samenwerkingsconvenant getekend waarin afspraken zijn vastgelegd over o.m.: rollen, verantwoordelijkheden, omgang met privacy en security, beheer, financiële- en juridische aspecten.

11.2.4 Eisen gerelateerd aan de community van Affinity Domains

26. Het Affinity Domain laat minimaal één keer per jaar een hack en penetratietest op de infrastructuur uitvoeren door een onafhankelijke partij. Het Affinity Domain neemt de verplichting op zich om geconstateerde onvolkomenheden binnen een, met de samenwerkingspartners overeengekomen termijn te herstellen. Het hack en pentestrapport is voor alle samenwerkingspartners in te zien.
27. Het Affinity Domain laat één keer per twee jaar een IT-audit op de infrastructuur uitvoeren door een onafhankelijk partij. De scope van de IT-audit is de keten bestaande uit de Registry, de koppelingen van zorginstellingen met de Registry, en de gateways tussen de Affinity Domains. Het IT-audit rapport is voor alle samenwerkingspartners in te zien.

28. Afhankelijk van de SLA, is de verbinding tussen Affinity Domains redundant uitgevoerd.
29. Tussen de Affinity Domains is een SLA afgesproken waarin tenminste de volgende aspecten zijn opgenomen:
    a. Beschikbaarheid;
    b. Bereikbaarheid serviceorganisatie tijdens kantooruren;
    c. Bereikbaarheid serviceorganisatie buiten kantooruren.
30. Tussen de diverse deelnemers is een IP plan afgestemd. Dit om te voorkomen dat hierin conflicten ontstaan. Dit IP plan is voor alle deelnemers beschikbaar. Afhankelijk van de gebruikte techniek is een algemeen BGP nummerplan, dan wel routerplan beschikbaar.
31. Het Affinity Domain maakt gebruik van een (centrale) DNS infrastructuur, inclusief een DNS naamgevingsconventie.
32. Bij het gebruik van certificaten geldt een minimale sleutelsterkte. Deze wordt jaarlijks door de deelnemers beoordeeld en zo nodig aangepast.
33. Overeengekomen wijzigingen in de infrastructuur worden door deelnemers binnen een periode van een jaar gerealiseerd.
34. Communicatie protocollen tussen Affinity Domains worden volgens een vast schema bijgehouden en zijn verplicht voor alle gelegde connecties.

11.2.5 Identificatie, Authenticatie en Autorisatie

35. Veilige toegang tot de IHE-XDS infrastructuur voor zorgprofessionals, vindt plaats op één van de volgende manieren:
    a. Via single sign on (SSO) openen van de IHE-XDS consumer vanuit het geopende dossier van een patiënt in het EPD-systeem. Hierbij is de patiënt al geselecteerd en de behandelrelatie gecontroleerd. Authenticatie van de gebruiker (in dit geval meestal via gebruikersnaam en wachtwoord) valt onder de verantwoordelijkheid van de zorginstelling en toegang tot de XDS-infrastructuur is gebaseerd op de onderlinge vertrouwensrelatie tussen de samenwerkende partners in het Affinity Domain.
    b. Door het stand-alone opstarten van de IHE-XDS consumer na sterke authenticatie van de gebruiker (met UZI-pas of vergelijkbaar sterk authenticatiemiddel).
36. Iedere zorgorganisatie binnen het Affinity Domain verplicht zijn medewerkers met een eigen unieke gebruikersaccount in te loggen op de IHE-XDS infrastructuur, zodat op individueel niveau herleidbaar is wie de gegevens heeft geraadpleegd. Het gebruik van functionele of groepsaccounts is niet toegestaan.
37. Iedere zorgorganisatie binnen het Affinity Domain (de brondossierhouders), is verantwoordelijk voor het uitgeven en beheren van rollen en rechten aan de eigen medewerkers, zodat deze beschikken over de juiste autorisaties en alleen toegang krijgen tot gegevens indien sprake is van een behandelrelatie met de patiënt.
38. Iedere zorgorganisatie binnen het Affinity Domain beschikt over een autorisatiematrix die de relatie weergeeft tussen de functie van gebruikers (samengevat in een organisatierol) en de autorisatierol binnen het IHE-XDS Affinity Domain.
39. Het Affinity Domain maakt gebruik van de landelijk gedefinieerde autorisatierollen. Deze autorisatierollen bepalen welke rechten een ingelogde gebruiker op de IHE-XDS infrastructuur heeft.
40. Het Affinity Domain heeft het XUA profiel geïmplementeerd.

11.2.6 Patiënttoestemming

41. Het Affinity Domain waarborgt dat patiëntgegevens pas via IHE-XDS (pull-verkeer) ingezien of uitgewisseld kunnen worden nadat de patiënt daarvoor uitdrukkelijk toestemming heeft gegeven. Hierbij dient sprake te zijn van ‘Informed Consent’ conform de EGiZ gedragscode.

42. Het Affinity Domain heeft werkprocedures geïmplementeerd die de patiënt de mogelijkheid geven toestemming vast te (laten) leggen, wijzigen en/of in te trekken.
43. Het Affinity Domain heeft een werkprocedure geïmplementeerd die de patiënt de mogelijkheid geeft (al dan niet digitaal) inzage te krijgen in een overzicht van de door hem of haar gegeven toestemmingen voor gegevensuitwisseling. Dit overzicht vermeldt zowel voor welke (soorten) gegevens toestemming is gegeven als de zorgorganisaties waarmee deze gegevens gedeeld mogen worden.
44. Iedere zorgorganisatie binnen het Affinity Domain, heeft een werkproces voor het vastleggen van de patiënttoestemming geïmplementeerd die het voor controle doeleinden mogelijk maakt achteraf aan te tonen dat de patiënt inderdaad toestemming heeft gegeven. Dit kan bijvoorbeeld door een ingescand toestemmingsformulier met de handtekening van de patiënt of een elektronisch formulier met de elektronische handtekening van de patiënt; het kan echter ook via een aantekening in het dossier van de patiënt.
45. Voor het afdwingen van de patiënttoestemming heeft het Affinity Domain het BPPC-profiel geïmplementeerd, met tenminste de volgende landelijk gedefinieerde toestemmingspolicies (zie: Nictiz White Paper “Richtlijn voor implementatie van toestemmingsprofielen binnen XDS-netwerken”):
    a. Uitdrukkelijk toestemming voor het Affinity Domain;
    b. Uitdrukkelijk toestemming voor Nederland;
    c. Breaking the glass voor noodsituaties;
    d. Generiek bezwaar.

11.2.7 Logging en auditing

46. Het Affinity Domain heeft het ATNA-profiel geïmplementeerd voor logging van alle transacties die plaats vinden op het IHE-XDS Affinity Domain. De implementatie van het ATNA-profiel moet, indien technisch mogelijk, voldoen aan de NEN7513.
47. Het Affinity Domain heeft een procedure geïmplementeerd waarmee patiënten hun recht op inzage in de loggegevens kunnen uitoefenen, zowel voor inzage in de metadata als in de berichtinhoud. De loggegevens moeten voldoende informatie bevatten om de patiënt inzicht te geven in welke zorgorganisaties welke gegevens heeft verstrekt aan welke andere zorgorganisaties en welke zorgverleners die gegevens hebben ingezien.
48. De samenwerkende Affinity Domains hebben onderling afspraken gemaakt over welke transacties en welke metadata wordt vastgelegd in de logbestanden. Voor het loggen van de metadata is de laatste versie van de Nictiz XDS metadataset leidend.
49. Iedere zorgorganisatie binnen het Affinity Domain is verplicht zelf een eigen logging van ‘lokale’ (niet IHE) transacties bij te houden. (Zie EGiZ gedragscode artikel 10: logging). Dit zijn transacties op de diverse zorgsystemen die binnen de zorgorganisatie draaien.
50. Binnen het Affinity Domain zijn afspraken vastgelegd wie toegang moeten hebben tot de (centrale) logbestanden.
51. Het Affinity Domain heeft een procedure ingericht voor de periodieke (steekproefsgewijze) audits van de logbestanden.
52. Het Affinity Domain heeft een procedure ingericht voor het aanvragen van inzicht in de loggegevens. Hierin is onder meer vastgelegd wie inzage kunnen aanvragen, hoe en waar dit aangevraagd moet worden en welke reactietermijnen worden gehanteerd. In deze procedure is ten minste ook inzage in de loggegevens door de patiënt geregeld.
53. Het Affinity Domain heeft sanctiebeleid geformuleerd voor gevallen waarbij misbruik van de IHE-XDS infrastructuur wordt geconstateerd door medewerkers van één van de samenwerkende organisaties.

11.2.8 Infrastructuur, netwerken en servers

54. Het Affinity Domain maakt gebruik van een uniek HomeCommunityID, uitgegeven door Nictiz (valt onder OID plan).
55. Per Affinity Domain is er een configuratiedocument waarin de volgende gegevens zijn vastgelegd:
    a. IP-adressen (IP-configuraties van alle aangesloten zorgorganisaties);
    b. Poortnummers;
    c. AE titles;
    d. (WADO) URL;
    e. OID's;
    f. Firewall configuratie instellingen.
56. Het Affinity Domain maakt gebruik van extern benaderbare IP-adressen.
57. Het Affinity Domain maakt gebruik van de volgende firewall configuratie:
    a. IP adres filtering: Het configureren van IP-adressen van de RSO en de aangesloten zorginstellingen binnen het Affinity Domain vindt plaats in de desbetreffende firewalls. Dat betekent blokkering bij communicatie vanuit een onbekend IP-adres. Voor gebruik binnen het Affinity Domain leveren zorginstellingen IP configuraties aan. Deze gegevens zijn centraal in een lijst beschikbaar voor de andere zorginstellingen. (zie hoofdstuk 3.6.5);
    b. Voor toegang tot de Registry is maar één enkel toegangspunt ('chokepoint') beschikbaar;
    c. Redundantie ('Defense in Depth');
    d. Het gebruik van verschillende soorten van beveiligingsmiddelen ('Diversity of Defense');
    e. Wanneer één beveiligingsmiddel faalt, zal geen toegang worden verleend ('Failure Mode');
    f. 'Stateful inspection': die de toegang tot bepaalde onderdelen van het systeem beperkt.
58. De beheerorganisatie(s) die betrokken zijn bij het beheer van het Affinity Domain en de server infrastructuur, zijn ISO 27001 en/of NEN7510 gecertificeerd voor alle componenten en organisatieonderdelen.
59. Het Affinity Domain heeft een procedure om beveiligingsupdates van alle IHE-XDS software componenten en besturingssystemen zo snel mogelijk te installeren.
60. De serverinfrastructuur van het Affinity Domain voldoet aan de GBX eisen.
61. De netwerkinfrastructuur voldoet aan de GZN eisen.
62. Systemen die behoren tot het Affinity Domain, communiceren met andere systemen door middel van beveiligde TLS-verbindingen op basis van servercertificaten. Deze servercertificaten worden uitgegeven door het UZI-register of andere vertrouwde partijen zoals Comodo. Op productieomgevingen is het niet toegestaan om "self-signed" certificaten te gebruiken. (De specificaties m.b.t. de TLS verbindingen staan uitgewerkt in het ATNA profiel van IHE).
63. Zowel voor het inkomende als uitgaande verkeer beschikt het AD over een gegarandeerde bandbreedte van 50Mb. Gelet op de praktijk is dit een minimum. Studies worden steeds groter en een minimale bandbreedte van 1Gb of hoger is op termijn wenselijk.
64. De performance van het Affinity Domain is zodanig dat studies binnen een volgens de zorgverleners acceptabele tijd overgehaald (geëxporteerd vanuit de 'centrale IHE-XDS infra') kunnen worden. Deze doorlooptijd geldt bij een normale bedrijfsvoering.

11.2.9 Testmanagement

65. (Het Affinity Domain beschikt, naast de productie omgeving, over een aparte test-/acceptatieomgeving voor het doorontwikkelen en testen van nieuwe versies/releases en upgrades van de IHE-XDS functionaliteit.

66. Het Affinity Domain beschikt over een goed uitgewerkt testscript dat doorlopen moet worden voor het in productie nemen van nieuwe versies/releases en upgrades van de IHE-XDS functionaliteit. Het testscript bevat tenminste een beschrijving van:
    a. De te testen componenten;
    b. De te testen handelingen/transacties;
    c. De verwachte resultaten van de test;
    d. De behaalde resultaten van de test;
    e. De acties naar aanleiding van de bevindingen.
67. Iedere zorgorganisatie binnen het Affinity Domain beschikt over een set van ten minste zes testpatiënten met een geldig fictief BSN. Voor een beschrijving van de testpatiënten zie paragraaf 10.5.

11.2.10 Beheer

68. Het Affinity Domain beschikt over een SLA met zowel de leverancier van de IHE-XDS infrastructuur als met de aangesloten zorgorganisaties, waarin de afspraken zijn vastgelegd betreffende het melden en afhandelen van incidenten, storingen en geconstateerde fouten in zowel de productieomgeving als tijdens testen in de test-/acceptatieomgeving.

12 Bijlages (zie separaat document)

1 Interoperabiliteitsmodel
2 Convenant Uitwisseling Persoonsgegevens in de zorg
3 Template gecombineerde DVO en DAP
4 Voorbeeld Aansluit document
5 Voorbeeld aanpak XDS-project
6 Voorbeeld IHE Use Case beschrijving
7 Stappenplan realisatie Use case
8 IHE koppelvlakken met bronsystemen
9 Technische uitwerking koppeling LSP-IHE
10 Templates Equipmentlist voor een Affinity Domain

13 Afkortingen & begrippenlijst

- AORTA. Zorginfrastructuur LSP. https://www.vzvz.nl/ict-dienstverleners/aorta-standaardisatie
- AD Affinity Domain
- ATNA. Audit Trail & Node Authentication
- AVG. Algemene Verordening Gegevensbescherming
- BPPC Basic Patient Privacy Consent (patiënt toestemming)
- BGZ Basis Gegevensset Zorg. https://www.nictiz.nl/standaarden/basisgegevensset-zorg/
- CDA Clinical Document Architecture. https://en.wikipedia.org/wiki/Clinical_Document_Architecture
- DAP Dossier Afspraken en Procedures
- EGIZ Gedragscode Elektronische Gegevensuitwisseling in de Zorg
- EPD Elektronisch Patiënten Dossier
- FG Functionaris Gegevensbescherming
- FO Functioneel Ontwerp
- GBX Goed beheerd zorgsysteem
- GEB Gegevensbescherming effectbeoordeling
- GTS Gespecificeerde Toestemming Structureel.
- GZN Goed Beheerd Zorg Netwerk
- IHE Integrating the Healthcare Enterprise
- LSP Landelijk Schakel Punt. https://www.volgjezorg.nl/het-lsp
- MDO Multi Disciplinair Overleg. https://www.nivel.nl/nl/dossier/multidisciplinair-overleg
- NICTIZ Nationaal Instituut in de Zorg. https://www.nictiz.nl
- OTAP Ontwikkeling, Test, Acceptatie en Productie
- PGO Persoonlijke Gezondheids Omgeving. https://www.patientenfederatie.nl/themas/persoonlijke-gezondheidsomgeving/
- PIA Privacy Impact Assessment
- RBAC Role Based Access Control
- RNI Register Niet Ingezetenen
- RSO Regionale Samenwerkingsorganisatie. https://www.rsonl.nl\
- RSO NL Regionale Samenwerkingsorganisatie Nederland. De overkoepelende vereniging van alle regionale samenwerkingsorganisaties (RSO's) in Nederland. https://www.rsonl.nl\

- SLA Service Level Agreement
- SSO Single Sign On
- TO Technisch Ontwerp
- UZI Unieke Zorgverlener Identificatie
- VWS Ministerie van volksgezondheid, Welzijn en Sport. https://www.rijksoverheid.nl/ministeries/ministerie-van-volksgezondheid-welzijn-en-sport
- VZVZ Vereniging van Zorgaanbieders voor Zorgcommunicatie. https://www.vzvz.nl
- WAbvpz Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
- WBGO Wet op de geneeskundige behandelingsovereenkomst.
- Wbp Wet bescherming persoonsgegevens
- Wmg Wet marktordening gezondheidszorg
- XDS Cross-enterprise Document Sharing
- XUA Cross User Assertion
- ZIB Zorginformatie Bouwstenen
- Zvw Zorgverzekeringswet.

14 Referenties

- AP. (2011). Advies conceptwijziging Besluit gebruik BSN in de zorg. https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/adv/z2011-00063.pdf
- AP. (2010).Advies wetsvoorstel gebruik burgerservicenummer in de jeugdzorg.
- https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/adv/z2010-01343.pdf
- AP (2018). Recht op dataportabiliteit. https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/recht-op-dataportabiliteit
- AVG (2018). AVG. https://www.rijksoverheid.nl/ministeries/ministerie-van-volksgezondheid-welzijn-en-sport/avg/documenten.
- EGIZ (2014). Gedragscode Elektronische Gegevensuitwisseling in de Zorg – EGiZ. https://www.nictiz.nl/overig/gedragscode-elektronische-gegevensuitwisseling-in-de-zorg-egiz/ [gezien 25-11-2018]
- EGIZ (2016). Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGiZ) Samenvatting. https://www.knmg.nl/zoekresultaten.htm?keyword=egiz&start=0&show_pdf_files=true&facet_creation_date=all-data&facet_creation_date_from=&facet_creation_date_to= [gezien 25-11-2018]
- GERRIT (2017). Beleidskader uitwisseling patiëntgegevens XDS Gerrit V1-2
- GERRIT (2017). Juridisch Kader XDS-Gerrit 0.8.pdf
- GERRIT (2017). Beleidskader uitwisseling patiëntgegevens XDS Gerrit V1-2 (Wet Cliëntenrechten)
- GBX (2018). Programma van Eisen GBx. Goed beheerd systeem. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwilkf2Ay-_eAhXK3KQKHbiLAaIQFjAAegQIBRAC&url=https%3A%2F%2Fwww.vzvz.nl%2Fmedia%2F541%2Fdownload&usg=AOvVaw3itwcQvTiI73iytZruIpZi [gezien 25-11-2018]
- GZN (2018). Programma van Eisen GZN. https://www.vzvz.nl/cookies?return_path=%252Fmedia%252Fdownloads%252Fprogramma-van-eisen-goedbeheerd-zorgnetwerk-v8020%252Fdownload [gezien 25-11-2018]
- IHE (2017). XDS metadata for exchange medical documents and images guideline. https://www.ihe-europe.net/node/162 [gezien 25-11-2018]
- IHE. (2018). Integrating the healthcare enterprise. Wat is IHE? https://nl.wikipedia.org/wiki/IHE [gezien 25-11-2018]

- IHE. (2018). Document Sharing metadata handbook. https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Handbook_Metadata_Rev1-1_Pub_2018-08-20.pdf [gezien 25-11-2018]
- IHE (2017). IHE perspective on the European Union GDPR
- https://www.ihe-europe.net/sites/default/files/2018-05/IHE-Europe-GDPR%20White%20Paper-2018.pdf?utm_source=IHE-Europe+Newsletter&utm_campaign=12b8fc149f-EPR-Projectathon-Progresses-Swiss+Federal-Electro_&utm_medium=email&utm_term=0_cf01e2ec3a-12b8fc149f-448674193 [gezien 25-11-2018]
- KNMG (2018). Wet cliëntenrechten bij elektronische verwerking van gegevens. https://www.knmg.nl/web/file?uuid=0024843f-c4dc-4287-98dc-e32a18b64c71&owner=5c945405-d6ca-4deb-aa16-7af2088aa173&contentid=67601 [gezien 25-11-2018]
- Medmij. (2018). Informatiestandaarden. https://www.medmij.nl/informatiestandaarden/ [gezien 25-11-2018]
- NEN. (2015). NEN 7512:2015 https://www.werkenmetnen7510.nl/publicaties/nen-7512-2015 [gezien 25-11-2018]
- NEN. (2017). NEN 7510-1:2017 https://www.werkenmetnen7510.nl/publicaties/nen-7510-1-2017/sec_0 [gezien 25-11-2018]
- NEN. (2018). NEN 7513:2018 https://www.werkenmetnen7510.nl/publicaties/nen-7513-2018 [gezien 25-11-2018]
- Nictiz (2012). Richtlijn voor Implementatie van toestemmingsprofielen binnen XDS-netwerken, https://www.nictiz.nl/wp-content/uploads/2018/04/richtlijn-voor-implementatie-van-toestemmingsprofielen-binne.pdf [gezien 25-11-2018]
- Nictiz. (2015). Handreiking Interoperabiliteit tussen XDS Affinity Domains 2015. https://www.nictiz.nl/wp-content/uploads/2018/03/Handreiking_interoperabiliteit_tussen_XDS_Affinity_Domains_2015.pdf [gezien 25-11-2018]
- Nictiz. (2018). Use Cases. https://www.nictiz.nl/Paginas/Use-case.aspx [gezien 25-10-2018]
- Nictiz. (2018). Interoperabiliteit. https://www.nictiz.nl/standaardisatie/interoperabiliteit/ [gezien 10-08-2018]
- NVZ. (2018). Model Verwerkersovereenkomst Branche Organisaties Zorg https://www.nvz-ziekenhuizen.nl/_library/38492/Verwerkersovereenkomst-BOZ_181217.pdf [gezien 25-10-2018]
- Overheid.nl (2008). Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg https://wetten.overheid.nl/BWBR0023864/2018-07-28 [gezien 25-11-2018]
- PALGA. (2018). PALGA: "Pathologisch-Anatomisch Landelijk Geautomatiseerd Archief. https://www.palga.nl [gezien 25-11-2018]
- RSONL. (2018).RSO NL. RSO's leveren een belangrijke bijdrage aan de zorgcommunicatie in Nederland. https://www.rsonl.nl [gezien 25-11-2018].
- UML (2018). Usecases. https://en.wikipedia.org/wiki/Use_case [gezien 25-10-2018]
- VWS (2017). FACTSHEET IDENTIFICATIE EN OPVRAGEN BSN. Ministerie van VWS. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/brochures/2007/04/10/factsheet-identificatie-en-opvragen-bsn/factsheet-identificatie-4.pdf
- VZVZ. (2018). PvE GBx Infrastructurele Systeemrollen. https://www.vzvz.nl/ict-dienstverleners/aorta-standaardisatie/aorta-documentatie [gezien 25-11-2018]
- Wikipedia. (2018).)Privacy Impact Assessment. https://en.wikipedia.org/wiki/Privacy_Impact_Assessment) [gezien 25-10-2018]