Onderzoeksrapport LSP

Privacy en security in het Landelijk Schakelpunt

Opleiding	System and Network Engineering
Student	Niels Sijm
Begeleider	Guido van 't Noordende
Project	RP1
Datum	30 juni 2008

Inhoudsopgave

1 Inleiding

De zorg in Nederland werkt toe naar digitalisering van patiëntinformatie: het Elektronisch Patiënten Dossier (EPD). Onderdelen hiervan zijn het Elektronisch Medicatie Dossier (EMD) en het Waarneem Dossier Huisartsen (WDH).

Om het EPD mogelijk te maken, is een landelijk aanspreekpunt nodig. Dit aanspreekpunt is door het Nationaal ICT Instituut in de Zorg (Nictiz) ontworpen en draagt de naam Landelijk Schakelpunt (LSP).

Bij het ontwerpen van het LSP is bestaande wetgeving leidend geweest. Zo is er de Wet op de Geneeskundige Behandelingsovereenkomst en de Wet Bescherming Persoonsgegevens waaraan voldaan moet worden. Deze wetgeving legt de relatie tussen zorgverlener en patiënt vast, en waarborgt de privacy van burgers in het algemeen.

Dit onderzoek kijkt naar de manier waarop privacy (en daarmee samenhangend security) in de ontwerpbeslissingen van het LSP zijn gewaarborgd. De documentatie van het Nictiz dient hierbij als uitgangspunt.

Hoofdstuk 2 definieert het onderzoek zoals uitgevoerd. Hoofdstuk 3 geeft een overzicht van de basale architectuur waarin de belangrijkst entiteiten worden benoemd. Hoofdstuk 4 is de uitwerking van het onderzoek naar de ontwerpbeslissingen van het LSP. Hoofdstuk 5 bevat een aanzet tot discussie naar aanleiding van het onderzoek, samen met aanbevelingen voor verder onderzoek.

2 Onderzoeksdefinitie

Door de grote hoeveelheid en het gevoelige karakter van de informatie die door het LSP wordt doorverwezen, dient goed te zijn nagedacht over de bescherming van privacy van patiënten. Dit komt naar voren in de architectuur en ontwerpbeslissingen van het LSP.

Dit project is bedoeld als verkenning van de architectuur en ontwerpbeslissingen van het LSP. De nadruk ligt op de privacyaspecten van het LSP. Dit komt op twee plaatsen naar voren.

1. Architectuur en ontwerpbeslissingen LSP
2. Functionele en technische specificaties LSP

Het onderzoek naar het LSP kent twee concrete onderzoeksdoelen.

1. Het is kaart brengen van de architectuur en ontwerpbeslissingen in het Landelijk Schakelpunt op basis van publiek beschikbare specificaties van Nictiz.

2. Toetsen van een deel van de functionele en technische specificaties aan de ontwerpbeslissingen op het gebied van privacy en security.

Het eerste deel van het onderzoek bestaat uit het in kaart brengen van de architectuur en ontwerpbeslissingen van het LSP. Aspecten die weinig met privacy te maken hebben en geen sleutelrol spelen in de structuur van het LSP worden buiten beschouwing gelaten of geabstraheerd. Vragen die centraal staan zijn onder andere: wie beheert de patiëntinformatie, hoe verloopt authenticatie en autorisatie, welke informatie passeert het LSP?

Voor het tweede deel van het onderzoek wordt de verwijsindex (VWI) van het LSP nader onderzocht. In de verwijsindex worden patiënten middels hun burgerservicenummer (BSN) gekoppeld aan dossiers bij zorgaanbieder. Hierbij wordt ingezoomd op de functionele en technische specificaties met betrekking tot privacy van patiënten.

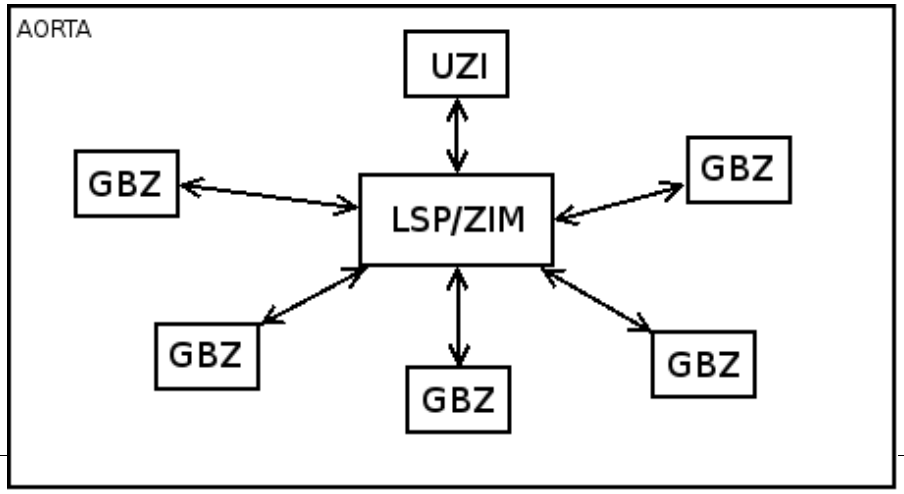
Centraal staat de vraag welke informatie precies in het LSP wordt bijgehouden en hoe deze informatie ontsloten wordt. Tevens wordt gekeken naar de consequenties van de genomen beslissingen voor de privacy van patiënten.

3 Basale architectuur

Het Nederlandse zorglandschap bestaat uit diverse entiteiten. Onderstaande tabel behandelt kort hun rol en samenhang.

Entiteit	Beschrijving
Nictiz	**Nationaal ICT Instituut in de Zorg**. Het Nictiz is het nationale knooppunt en kenniscentrum voor ICT en innovatie in de zorg. Het Nictiz heeft in opdracht van het Ministerie van Volksgezondheid, Welzijn en Sport het LSP ontwikkelt.
AORTA	AORTA is de naam van de ICT-basisinfrastructuur, gedefinieerd door Nictiz, die elektronisch berichtenverkeer tussen zorgpartijen mogelijk maakt.
ZIM	**Zorginformatiemakelaar**. De ZIM is het schakelpunt binnen AORTA. Het ZIM maakt het mogelijk landelijk medische informatie uit te wisselen. Binnen een infrastructuur kunnen meerdere ZIM's actief zijn.
LSP	**Landelijk Schakelpunt**. Het LSP in de Nederlandse zorginformatiemakelaar. Binnen AORTA is het LSP de enige ZIM. De belangrijkste taak van het LSP is het koppelen van patiënten aan dossiers bij zorgaanbieders.
GBZ	**Goedbeheerd Zorgsysteem**. Een GBZ is een informatiesysteem van zorgverleners en zorgverzekeraars dat voldoet aan duidelijke omschreven kwaliteitseisen op het gebied van berichtenstandaarden, beveiliging, performance en beschikbaarheid.
UZI	**Unieke Zorgverleners Identificatie**. Het UZI houdt een register bij met zorgverleners. Het UZI-register wordt gebruikt bij identificatie, authenticatie en autorisatie van zorgverleners.

Onderstaand schema (figuur 1) geeft kort de relaties tussen de verschillende entiteiten weer.



Figuur 1: Samenhang entiteiten AORTA

4 Ontwerpbeslissingen LSP

Dit hoofdstuk is een beknopte samenvatting van de ontwerpbeslissingen van het LSP, gedestilleerd uit de documentatie van het Nictiz (release mei 2007)[1]. Bij het in kaart brengen van de ontwerpbeslissingen van het LSP is nadruk gelegd op de privacyaspecten met betrekking tot patiëntgegevens.

In de eerste paragraaf wordt een inleiding gegeven tot het LSP. In de tweede paragraaf wordt kort uitgelegd wat AORTA is. In paragraaf drie wordt uitgelegd wat de taken en verantwoordelijkheden van het LSP zijn. In de daarop volgende paragrafen worden de uitgangspunten van AORTA genoemd en wordt verder ingegaan op de taken en verantwoordelijkheden van het LSP.

4.1 Inleiding Landelijk Schakelpunt

Met het LSP kunnen zorgverleners landelijk actuele patiëntinformatie opvragen uit de systemen van diverse ziekenhuizen, apotheken en huisartsen. Een goed functionerend LSP is een noodzakelijke voorwaarde voor de landelijke invoering van het Elektronisch Medicatie Dossier (EMD) en het Elektronische Waarneem Dossier Huisartsen (WDH), de eerste concrete componenten van een landelijk Elektronisch Patiënten Dossier.

Het Nictiz werkt aan de ontwikkeling van een landelijke basisinfrastructuur in de zorg, AORTA genaamd, die mogelijk moet maken dat zorgaanbieders, en later ook zorgverzekeraars en patiënten, ten behoeve van verschillende zorgtoepassingen op landelijke schaal patiëntgegevens kunnen uitwisselen.

Centraal in AORTA staat de zorginformatiemakelaar (ZIM). De rol van ZIM wordt in AORTA ingevuld door het LSP. Daarop kunnen zorgaanbieders hun bestaande zorginformatiesystemen aansluiten, mits zij voldoen aan de eisen van een goed beheerd zorgsysteem (GBZ). Die aansluiting vindt plaats via datacommunicatienetwerken (DCN), die worden geëxploiteerd door zorgserviceproviders (ZSP).

Voor het uniek identificeren van patiënten, zorgaanbieders, zorgverzekeraars en zorgsystemen wordt gebruik gemaakt van landelijke registers: het UZI–register (Unieke Zorgverleners Identificatie), de SBV-Z (Sectorale BerichtenVoorziening in de Zorg van het BSN-stelsel) en het UZOVI-register (Uniek Zorgverzekeraars Identificatie).

4.2 Uitgangspunten AORTA

AORTA vormt de basis voor het EPD en het LSP. Bij het ontwikkelen van AORTA zijn de volgende uitgangspunten gedefinieerd.[2]

- Bij het ontwerp van de architectuur is uitgegaan van de bestaande wet- en regelgeving, zoals de

1 http://www.nictiz.nl/
2 Bron: Architectuurvisie AORTA v5.0, § 3.3

Wet op de Geneeskundige Behandelingsovereenkomst[3] (WGBO) en de Wet Bescherming Persoonsgegevens (WBP).

- Er wordt gestreefd naar oplossingen die op draagvlak in het veld kunnen rekenen. Daarom is het ontwerp van de architectuur primair gebaseerd op een samen met het veld ontwikkeld vertrouwensmodel[4], gebaseerd op de bestaande vertrouwensstructuren, autonomie en verantwoordelijkheden van patiënten, betrokken zorgverleners, organisaties en instellingen. Ook is draagvlak vanuit politiek en samenleving van belang.

- De zorgverlener kan, binnen bepaalde randvoorwaarden m.b.t. de beveiliging, zijn ICT-voorzieningen naar eigen inzicht kan organiseren en blijft zelf verantwoordelijk voor het waarborgen van de integriteit en privacy van patiëntgegevens.

- De eigen rol en verantwoordelijkheid van de leveranciers van systemen en softwarepakketten blijft gehandhaafd. Het streven is om oplossingen te zoeken waarbij de marktwerking niet wordt beperkt.

Bijlage A bevat de hoofdlijnen van de architectuurprincipes van AORTA.

4.3 Taken en verantwoordelijkheden LSP

Het LSP heeft de volgende taken en verantwoordelijkheden.

- Authenticeren van zorgverleners, zorgsystemen en het LSP
- Autoriseren van zorgverleners
- Bijhouden en ontsluiten van een VWI
- Doorgegeven van medische gegevens
- Bijhouden van een toegangslog

De volgende paragrafen gaan in op elke van deze taken en verantwoordelijkheden,

4.4 Authenticatie

Een zorgverlener authenticeert zich door de UZI-pas in een card reader te steken en een pincode in te voeren. De aangesloten zorgsystemen kunnen nu de UZI-pas gebruiken om de gebruiker te authenticeren. (Zie paragraaf 4.4.1 voor meer informatie over de UZI-pas.)

Alle entiteiten (zorgverleners, zorgsystemen en het LSP) maken gebruik van X.509-certificaten voor authenticatie. De X.509-certificaten zijn opgeslagen in de UZI-pas.

Communicatie met het LSP verloopt via web services, en daarom via HTTP. Deze HTTP-communicatie

3 http://wetten.overheid.nl/cgi-bin/deeplink/law1/title=WGBO, http://www.hulpgids.nl/wetten/wgbo.htm
4 Zie Bijlage F voor het vertrouwensmodel volgens Nictiz.

loopt over een SSL-verbinding; het wordt dan HTTPS (HTTP Secure). Bij het opzetten van een SSL-verbinding stuurt het LSP een certificaat mee dat ondertekend is door een Certificate Authority (CA) van het UZI-register. Hierdoor weet de partij die contact zoekt met het LSP dat de tegenpartij ook echt het LSP is, en niet een applicatie dan derden.

4.4.1 De UZI-pas

UZI staat voor Unieke Zorgverlener Identificatie. Een UZI-pas is een pas waarmee zorgverleners zich kunnen authenticeren. De pas kan met behulp van een card reader worden gebruikt. Een pincode is verplicht om de identiteit van de gebruiker te controleren.

Er zijn vier verschillende soorten UZI-passen.

- Zorgverlenerspas
- Medewerkerpas op naam
- Medewerkerpas niet op naam
- Servicespas

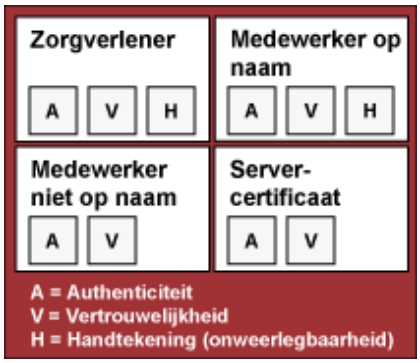
De passen worden als volgt uitgegeven.

Zorgverlenerspas	Voor een beroepsbeoefenaar als bedoeld in de artikelen 3 en 34 van de Wet BIG werkzaam in een zorginstelling.
Medewerkerpas op naam	Een medewerker van een zorginstelling of die door een individuele zorgverlener is aangewezen als hulppersoon.
Medewerkerpas niet op naam	Voor medewerkers van een zorginstelling of die door een individuele zorgverlener zijn aangewezen.
Servicespas	Voor services (systemen, websites, gegevensverzamelingen, servers etc.) in een zorginstelling of van een individuele zorgverlener.

De UZI-pas biedt drie diensten aan; Authenticiteit, Vertrouwelijkheid en Handtekening. Figuur 2 geeft aan welke functionaliteit elke passoort biedt.

Authenticiteit: Authenticatie d.m.v. een X.509-certificaat
Vertrouwelijkheid: Versleuteling d.m.v. een X.509-certificaat
Handtekening: Een cryptografische handtekening

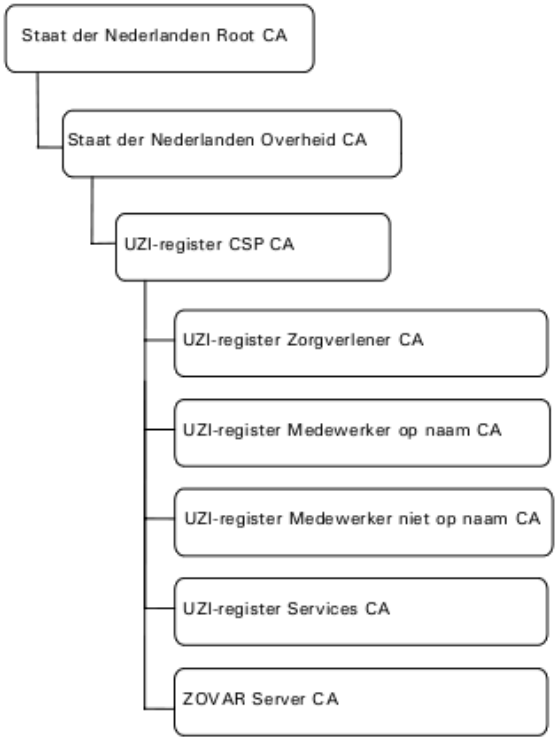
Voor elke functionaliteit zijn eigen sleutelparen beschikbaar. Hiervoor is vermoedelijk gekozen om de gevolgen van het gecompromitteerd raken van één van de sleutels beperkt te houden tot de betreffende functionaliteit.



Figuur 2: Functionaliteit UZI-passen

Omwille van onweerlegbaarheid is het mogelijk een cryptografische handtekening te zetten. De status van de digitale handtekening is gelijk aan die van de papieren (natte) handtekening. Ook hiervoor wordt een apart certificaat op de UZI-pas gebruikt.

De publieke sleutels van de certificaten van de UZI-pas zijn opgeslagen in LDAP. Deze directory wordt bijgehouden door het UZI-register[5]. Indien communicatie met LDAP over SSL plaatsvindt, kunnen certificaten betrouwbaar worden opgevraagd.



Figuur 3: Certificate Chain UZI-passen

Elke passoort heeft zijn eigen CA. De certificate chain is als beschreven in figuur 3.

4.5 Autorisatie van zorgverleners

Autorisatie wordt deels door het LSP en deels door de zorgaanbieders geregeld. Het LSP autoriseert zorgverleners aan de hand van hun beroepsfunctie:

> Bij het landelijk schakelpunt (LSP) krijgen zorgverleners op basis van hun beroep (rol) per zorgtoepassing (te beginnen met EMD en WDH) toegang tot een gespecificeerde set van zorggegevens. Voor het EMD zijn dit in eerste instantie artsen en apothekers. Voor

5 https://www.uzi-register.nl/ldapsearch/LDAPUserServlet

> het waarneemdossier zijn dit huisartsen en waarnemend huisartsen.[6]

In het autorisatie*protocol* wordt vastgelegd welke informatie door welke beroepsfunctie opvraagbaar is. Ook wordt bij elke informatiesoort een vertrouwensniveau vermeld. Het vertrouwensniveau kan hoog, midden of laag zijn. De vereisten voor verschillende vertrouwensniveaus zijn als volgt.

Vertrouwensniveau	Vereisten
Hoog	Versleuteling en elektronische handtekening op berichtniveau via XML-encryption en XML-signature, met behulp van de sleutels van UZI-passen.
Midden	Versleuteling en authenticatie op transportniveau via SSL/TLS, met behulp van de sleutels van persoonlijke UZI-passen en/of UZI- servercertificaten.
Laag	Versleuteling en authenticatie op netwerkniveau door aansluiting van het GBZ op een VPN met bijv. IPsec of SSL met behulp van de sleutels van UZI-servercertificaten.

Bij berichtenverkeer met vertrouwensniveau hoog authenticeren zorgaanbieders elkaar met behulp van elektronische handtekeningen. Bij de vertrouwensniveaus midden en laag verloopt de communicatie via het LSP en authenticeren de zorgaanbieders elkaar niet; zij vertrouwen het LSP als Trusted Third Party.[7]

Het autorisatieprotocol wordt beheerd door het LSP. Het LSP maakt gebruik van het autorisatieprotocol om toegang tot medische gegevens te verlenen danwel af te wijzen.

Het Nictiz meldt over het autorisatieprotocol het volgende.

> Samenwerkende zorgaanbieders die willen aansluiten op hetzelfde schakelpunt moeten akkoord gaan met het autorisatieprotocol en verklaren dat zij patiëntgegevens alleen zullen opvragen in het kader van een behandelrelatie.[8]

In het autorisatie*profiel* wordt bijgehouden welke patiëntgegevens opvraagbaar zijn. Patiënten kunnen zelf hun autorisatieprofiel beheren. Ook kunnen patiënten aangeven welke zorgaanbieders geen toegang mogen krijgen tot hun patiëntgegevens. Per zorgaanbieder kan worden ingesteld welke patiëntgegevens opvraagbaar zijn.

Het autorisatieprofiel wordt door het LSP beheerd. Bij het autoriseren van zorgverleners raadpleegt het LSP het autorisatieprofiel. Heeft de patiënt in diens autorisatieprofiel uitwisseling van medische gegevens verboden, dan wijst het LSP toegang tot diens gegevens af.

6 Architectuurvisie AORTA v5.0, § 3.5
7 Bron: Technische architectuur AORTA v3.0, § 7.1
8 Bron: Bedrijfsarchitectuur AORTA v3.0, § 9.2

Toegang tot informatie door zorgaanbieders wordt gegeven aan de hand van de volgende parameters[9].

- Functie zorgverlener (gecontroleerd door LSP)
- Behandelrelatie zorgaanbieder en patiënt
- Autorisatieprofiel patiënt (gecontroleerd door LSP)
- Noodzaak tot inzage patiëntgegevens
- Is er sprake van een noodsituatie

Om het systeem werkbaar te houden, moeten de meeste van deze gegevens vooraf worden vastgelegd. De zorgaanbieder dient de benodigde gegevens te verzamelen. Het LSP fungeert hierin slechts als VWI met beperkte (niet-fijnmazige) autorisatie.

Het is aan de opvragende zorgverlener om aan te geven of het een noodsituatie betreft. Indien dit het geval is, krijgt de zorgverlener toegang tot de medische gegevens. Het toegangslog kan worden gebruikt om misbruik van deze functionaliteit te reconstrueren.

Zie Bijlage B voor meer informatie over autorisatie en de rol van het LSP daarin.

Een zorgaanbieder kan bepaalde taken delegeren aan zijn medebehandelaren en medewerkers. Dit zijn de zogenaamde “voorbehouden handelingen” (ook wel “verlengde arm” genoemd). Die taken omvatten zowel zorgtaken als ondersteunende taken, waaronder het vastleggen, beheren en uitwisselen van patiëntgegevens. De hoofdbehandelaar blijft echter verantwoordelijk.

Voor het delegeren kan de zorginstelling een mandateringstabel aanleggen. Hierin wordt vastgelegd aan wie bepaalde taken zijn gedelegeerd. De mandateringstabel wordt niet door het LSP bijgehouden, maar door de zorgaanbieder.

Het Nictiz meldt het volgende over autorisatie m.b.t. de mandateringstabel.

> Voor het landelijk uitwisselen van patiëntgegevens geldt het landelijke autorisatieprotocol. Daarin worden medebehandelaren met wettelijk beschermde beroepstitels (bijv. verpleegkundige, verloskundige, etc.) geautoriseerd op basis van hun functie. Daarentegen worden medewerkers zonder beschermde beroepstitel (bijv. co-assistent, doktersassistent, etc.) niet genoemd in het landelijke autorisatieprotocol.[10]

Zie Bijlage C voor een schematisch overzicht met uitleg van het mandateringsmechanisme.

4.6 Bijhouden en ontsluiten van verwijsindex

Het LSP houdt zelf geen medische gegevens bij, maar verwijst naar autonome systemen van zorgaanbieders. De VWI koppelt dossiers van zorgaanbieder aan patiënten. Ter identificatie van de

9 Bedrijfsarchitectuur AORTA, v3.0, § 9.2
10 Bron: Bedrijfsarchitectuur AORTA v3.0, § 9.4

patiënt wordt gebruikt gemaakt van het burgerservicenummer (BSN). De VWI slaat alleen verwijzingen op naar dossiers, en bevat zelf geen medische gegevens.

De VWI slaat geen verwijzingen op van patiënten die bezwaar hebben gemaakt tegen het elektronisch uitwisselen van hun patiëntgegevens.

De VWI biedt de volgende diensten aan.

- Opvragen van verwijzingen (index)
- Toevoegen verwijzing (aanmelden)
- Wijzigen verwijzing (heraanmelden)
- Verwijderen verwijzing (afmelden)
- Ophogen foutenteller

De foutenteller wordt gebruikt om het aantal foutieve verwijzingen bij te houden.

4.6.1 Structuur verwijsindex

Bron: Informatiesysteemarchitectuur AORTA v3.0, bijlage C.

Attribuut	Verplicht	Wijzigbaar
Patient-id (BSN)	Ja	Nee
Applicatie-id	Ja	Ja
Beheerverantwoordelijke • Zorgaanbieder-id • Zorgverleners-id • Zorgverlener-functie	 Ja Ja ja	 Nee Ja Ja
Inhoudverantwoordelijke • Zorgaanbieder-id • Zorgverleners-id • Zorgverlener-functie	 Ja Ja Ja	 Nee Ja Ja
Gegevenssoort	Ja	Nee
Patientgegevens-id	Ja	Nee (uniek)
Actualiteit • Begintijd • Eindtijd	 Nee Nee	 Ja Ja
Foutenteller	(verborgen)	(verborgen)

De inhoudverantwoordelijke is verantwoordelijk voor de juistheid van de medische inhoud van de patiëntgegevens. De beheerverantwoordelijke is verantwoordelijk is voor het bewaren van bepaalde

patiëntgegevens en het zonodig ter beschikking stellen daarvan aan anderen.

De attributen hebben de volgende betekenis.

Atttribuut	Betekenis
Patient-id	Unieke sleutel bestaande uit het BSN (burgerservicenummer). Het BSN is het nummer dat elke Nederlander naar de overheid toe identificeert.
Applicatie-id	Applicatie die het betreffende dossier ontsluit[11]. Elke applicatie die als onderdeel van het LSP dossiers ontsluit, heeft een unieke applicatie-id toegewezen gekregen.
Zorgaanbieder-id	Het zorgaanbieder-id is een nummer dat een zorgaanbieder binnen Nederland uniek identificeert.
Zorgverlener-id	Het zorgverlener-id is een nummer dat een zorgverlener binnen Nederland uniek identificeert. Zorgverleners-id's worden uitgegeven door het UZI en opgeslagen in het UZI-register.[12]
Zorgverlener-functie	Het beroep met één of meer gerelateerde specialismen dat een zorgverlener daadwerkelijk uitoefent .[13] (Zie Bijlage D voor een lijst met zorgverlenersfuncties.)
Gegevenssoort	Voorbeelden gegevenssoorten: adresgegevens, diagnose, labuitslag, factuur[14], index, medicatievoorschrift, medicatieverstrekking, eerstelijnsdossier[15]. (Zie Bijlage E voor meer informatie over de gegevenssoortentabel.)
Patiëntgegevens-id	Unieke sleutel aan de hand waarvan een stuk patiëntinformatie kan worden geïdentificeerd.
Begintijd	Tijdstip waarop informatie geactualiseerd is.
Eindtijd	Tijdstip waarop informatie als niet actueel moet worden beschouwd.
Foutenteller	Een teller die door het LSP wordt opgehoogd indien een verwijzing niet blijkt te kloppen. De foutenteller is door gebruikers niet aan te passen.

De applicatie-id koppelt een beheerverantwoordelijke aan een patiënt. Het patiëntgegevens-id is nodig om te differentiëren tussen verschillende dossiers bij dezelfde zorgaanbieder of tussen verschillende delen van dossiers.

Het veld Gegevenssoort classificeert elke verwijzing. De complete tabel met gegevenssoorten is in de documentatie van het Nictiz niet teruggevonden. Een gegevenssoort is niet te wijzigen, maar wel te

11 Bron: Informatiesysteemarchitectuur AORTA v3.0, § 5.3
12 Bron: Informatiesysteemarchitectuur AORTA v3.0, § 5.11
13 Bron: Bedrijfsarchitectuur AORTA v3.0, § 3.4
14 Bron: Systeemarchitectuur AORTA v3.0, § 6.3
15 Bron: Informatiesysteemarchitectuur AORTA v3.0, § 5.4

verbijzonderen.

Een aangemelde verwijzing kan niet worden gewijzigd door een andere zorgaanbieder. Het overnemen van verwijzingen is dus niet mogelijk. Indien de patiënt van zorgaanbieder wisselt, worden de gegevens door de oude zorgaanbieder afgemeld en door de nieuwe zorgaanbieder weer aangemeld.

4.6.2 Ontsluiting via web services

De VWI is onderdeel van het LSP. Het LSP biedt haar diensten, waaronder de VWI, aan via web services[16]. De web service doet dienst als Remote Procedure Call (RPC) mechanisme. De HL7v3-berichten die over deze web services verstuurt worden bevatten de medische gegevens.

Het Nictiz heeft een testtool[17] gebouwd waarmee zorgsystemen hun HL7v3-berichten kunnen valideren. Hiermee wordt zowel syntax van de SOAP-berichten als de inhoud van de HL7v3-berichten gevalideerd.

De testtool biedt webservices aan op drie gebieden: Zorginformatiemakelaar (LSP), Medicatiedossier (EMD) en Waarneemdossier Huisartsen (WHD). Zie onderstaande tabel voor bijbehorende web services en interacties.

Gebied	Web service	Operatie
WHD	Waarneming	QueryResponse
		VersturenVerslagDWH
EMD	Voorschriftbericht	ActiveerMedicatievoorschrift
	Verstrekkingsquery	QueryResponse
		ContinuationCancelResponse
LSP	AanmeldenGegevens	AanmeldenNieuweGegevens
		WijzigenAangemeldeGegevens
		LatenVervallenAangemeldeGegevens
	OpvragenMetagegevens	QueryResponse
		ContinuationCancelResponse
	BsnOpvraagVerificatie	GetBSNInfo

Van bovenstaande web services zijn de WSDL's en XML Schema's beschikbaar. Dit zijn XML-documenten die op technische niveau de web services beschrijven.

16 http://en.wikipedia.org/wiki/Web_service
17 Http://www.testtool.nl/

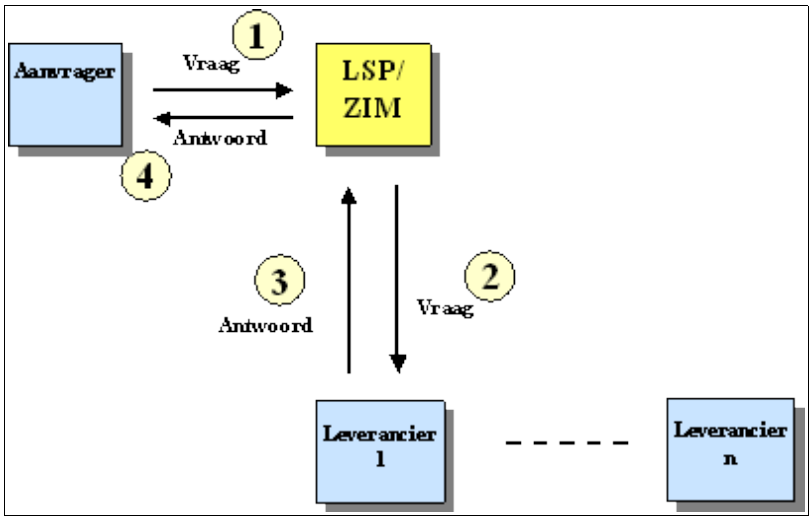
4.7 Doorgegeven van medische gegevens

Het LSP kan medische gegevens op twee manieren aanleveren.

1. Via het LSP (indirect, figuur 4)
2. Tussen zorgaanbieders onderling (direct, figuur 5)

Bij uitwisseling via het LSP zou het model gecentraliseerd worden. Wisselen zorgaanbieders onderling gegevens uit, dan is het model meer gedecentraliseerd.

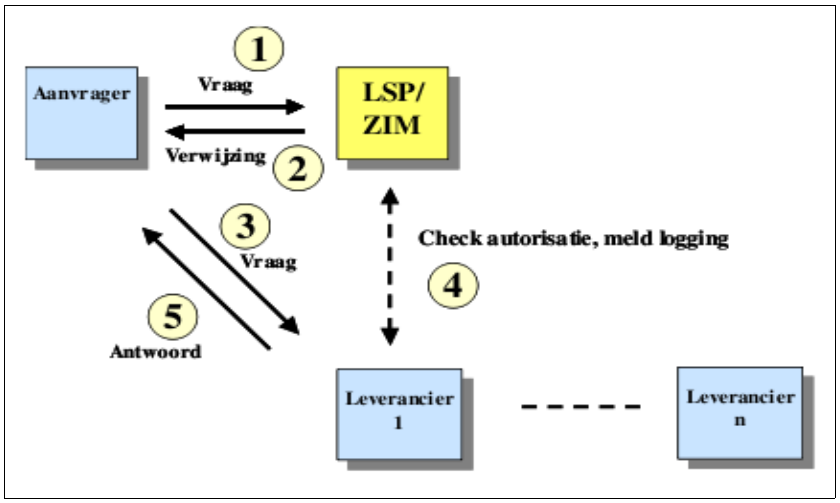
Bij het indirect uitwisselen van medische gegevens fungeert het LSP als doorgeefluik; de medische gegevens komen eerst bij het LSP terecht.



Figuur 4: Direct uitwisselen van medische gegevens via het LSP

Bij het direct uitwisselen van medische gegevens krijgt het LSP de medische gegevens niet in handen. Het LSP geeft een token uit waarmee de opvrager bij de betreffende zorgaanbieder informatie kan opvragen. De techniek die hiervoor gebruikt wordt is SAML[18] (Security Assertion Markup Language). SAML is een XML-dialect waarmee authenticatie- en autorisatieinformatie kan worden doorgegeven.

18 http://en.wikipedia.org/wiki/SAML



Figuur 5: Uitwisseling van medische gegevens tussen zorgverleners onderling

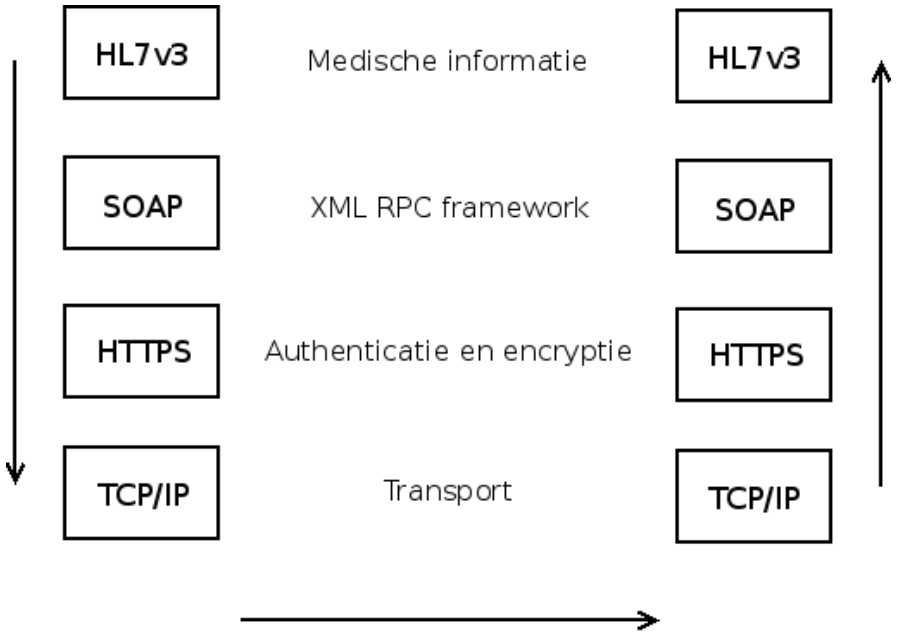
Bij het indirect uitwisselen van medische gegevens kan de informatie op meerdere manieren worden versleuteld.

1. Versleuteling met het LSP als Man in the Middle
2. End-to-end encryption tussen verstrekker en ontvanger

Versleuteling met het LSP als Man in the Middle betekent dat medische informatie onversleuteld in handen van het LSP terecht komt. End-to-end encrpytion betekent dat de informatie door de verstrekker met de publieke sleutel van de ontvanger wordt versleuteld, waardoor het LSP geen inzicht krijgt in de medische gegevens.

Het LSP is benaderbaar via web services. Web services communiceren door middel van SOAP[19]. SOAP is een op XML gebaseerd basic messaging framework. Het wordt vooral gebruikt voor Remote Procedure Calls (RPC). SOAP maakt gebruik van HTTP/HTTPS als transportmiddel. De berichten die uitgewisseld worden zijn dus XML-berichten over een HTTP(S)-verbinding. Figuur 6 toont de samenhang tussen deze technieken.

19 http://www.w3.org/TR/soap/



Figuur 6: Samenhang tussen technieken voor uitwisselen HL7v3-berichten

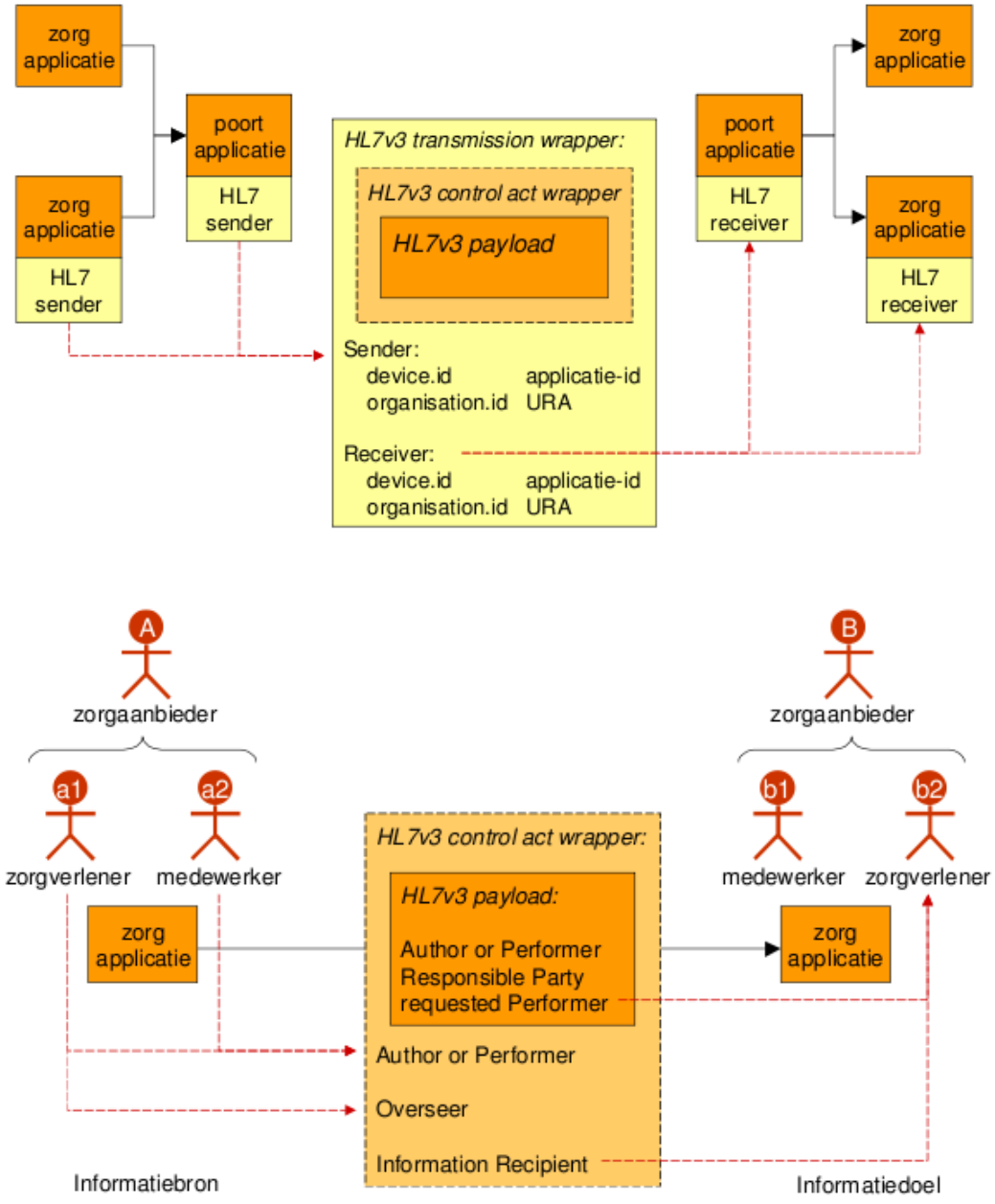
4.7.1 HL7v3-berichten

HL7v3-berichten bestaan uit een aantal lagen.[20]

- Transmission Wrapper
  - Control Act Wrapper
    - Payload

De **Transmission Wrapper** adresseert de zorgaanbieder en de applicatie van de zorgaanbieder. De **Control Act Wrapper** onderscheidt Author/Performer, Overseer en Information Recipient van elkaar. De **Payload** bevat medische informatie. Zie figuur 7 voor een schematische weergave.

20 Bron: Technische architectuur AORTA v3.0, Bijlage B



Figuur 7: Inhoud en encapsulatie van HL7v3-pakketten

Uit de Transmission Wrapper valt niet op te maken welke zorgverleners betrokken zijn. Uit de Control Act Wrapper valt dat wel op te maken.

Over de manier van versleuteling van medische gegevens zegt het Nictiz het volgende (Technische architectuur AORTA v3.0, paragraaf 7.2):

> De interne beveiliging van de ZIM is van groot belang omdat in principe alle landelijk

> uitgewisselde patiëntgegevens via de ZIM lopen. Echter, de ZIM is slechts een schakelpunt voor gegevensstromen. De ZIM kijkt in principe niet in de HL7 Payload met patiëntgegevens van de uitgewisselde HL7-berichten. **De ZIM kijkt wel in de HL7 Transport Wrapper en de HL7 Control Act Wrapper, maar die bevatten geen patiëntgegevens.** Daarmee is de interne beveiliging van de ZIM vooral een zaak van fysieke toegangscontrole, betrouwbare beheerprocedures, betrouwbaar personeel, etc.

Hieruit blijkt dat de HL7v3-berichten voor het LSP in geheel leesbare vorm voorbijkomen. Dit kan niet het geval zijn indien end-to-end encryption wordt gebruikt. Het LSP zal dus twee SSL-verbindingen opzetten; één met elke zorgaanbieder.

In de toekomst wordt de mogelijkheid geboden medische informatie op applicatie-niveau te versleutelen. En wordt dan gebruik gemaakt van XML Encyption, waarbij de payload van HL7v3-berichten wordt versleuteld. Hierbij kan gebruik worden gemaakt van de publieke sleutels van zorgverleners die via LDAP zijn op te vragen bij het UZI-register.

4.8 Bijhouden van een toegangslog

Omwille van onweerlegbaarheid wordt een toegangslog bijgehouden. Hierin worden alle transacties (opvraag- en mutatiegegevens) bijgehouden. Het toegangslog kan gebruikt worden om na te gaan wie welke informatie op welk moment heeft opgevraagd of gemuteerd. Hiermee is een soort van notarisfunctie in de infrastructuur ingebakken.

Het toegangslog legt gegevens vast, maar speelt geen rol bij het autorisatieproces. Het toegangslog kan gebruikt worden om achteraf te controleren of bijvoorbeeld het beroepsgeheim is geschonden. Het actief voorkomen van misbruik van patiëntgegevens is niet het doel van het toegangslog.

De volgende gebruikersinteracties worden gelogd[21].

1. Inloggen en uitloggen van gebruikers
2. Opvragen en versturen van patiëntgegevens
3. Opvragen index van gegevenssoorten
4. Aanmelden en afmelden van gegevenssoorten

Punt 1 en 2 hebben betrekking op het LSP als geheel. Punt 3 en 4 hebben betrekking op de VWI als onderdeel van het LSP. Het document “Informatiesysteemarchitectuur AORTA v3.0” noemt in paragraaf 5.8 de attributen die per transactie gelogd worden.

In het toegangslog komen geen medische gegevens te staan. Doordat patiëntgegevens tot een bepaalde datum moeten kunnen zijn te reconstrueren[22], is dit ook niet nodig. De informatie in het toegangslog zijn dus metagegevens.

21 Bron: Informatiesysteemarchitectuur AORTA v3.0, § 5.8
22 Bron: Informatiesysteemarchitectuur AORTA v3.0, § 4.9 (OPV.B03)

4.9 Connectiviteit

> Een DataCommunicatieNetwerk (DCN) is een gemeenschappelijke ICT-voorziening die nodig is om de [Goed Beheerde Zorgsysemen] (GBZ'en) van verschillende zorgpartijen (zorgaanbieders, zorgverzekeraars, etc.) te kunnen aansluiten op de ZIM. Zo'n DCN kan een [Virtual Private Network] (VPN) of een [Value Added Network] (VAN) zijn, zolang deze voldoet aan de gestelde eisen m.b.t. beveiliging en dienstverlening.[23]

Om een DCN te mogen aansluiten op het LSP zal de netwerkdienstverlener ondersteunende diensten moeten bieden aan zorgaanbieders die hun systemen willen aansluiten:

- **De uitgifte van hostnamen en IP-adressen aan GBZ'en op basis van een IP-adresblok toegekend door het LSP**
- De aanlevering van routeringsgegevens aan het LSP voor uitgegeven IP-adressen
- Hulp aan zorgaanbieders bij het aansluiten van hun GBZ'en
- De eerste-lijns hulp aan zorgaanbieders bij incidenten
- De bewaking van de prestaties van het Data Communicatie Netwerk (DCN)

Alle zorgsystemen die communiceren met het LSP maken dus deel uit van hetzelfde VPN. Zorgverleners zelf kunnen geen toegang krijgen tot het VPN; dit is voorbehouden aan geauthenticeerde zorgsystemen waarop zorgverleners eventueel kunnen inloggen.

23 Bron: Technische structuur AORTA v3.0, § 3.7

5 Discussie en verder onderzoek

Een punt van discussie is autorisatie door het LSP op basis van wettelijk beschermde beroepstitels. Medewerkers zonder een wettelijk beschermde beroepstitel kunnen dus niet bij het LSP geautoriseerd worden. Dit probleem wordt opgelost door gebruik van mandateringstabellen of andere voorzieningen buiten het LSP om. Autorisatie van zorgverleners zonder wettelijk beschermde beroepstitel wordt bij de zorgaanbieders zelf geregeld. De vraag is waarom het LSP niet voorziet in dergelijke functionaliteit.

Bij het doorgeven van medische gegevens worden de HL7v3-berichten geheel leesbaar door het LSP ontvangen. Versleuteling van de HL7v3-payload is mogelijk, maar staat gepland voor de toekomst. Het Nictiz concludeert “[...] is de interne beveiliging van de ZIM vooral een zaak van fysieke toegangscontrole, betrouwbare beheerprocedures, betrouwbaar personeel, etc.”. Dit is op te vatten als een understatement, omdat medische informatie onversleuteld door het LSP wordt geleid. Hiermee wordt de impact van compromitatie van het LSP gebagatelliseerd.

Het Nictiz pleit ervoor informatie bij voorkeur via het LSP uit te wisselen. Het LSP fungeert dan als Man in the Middle, hetgeen het model centraliseert. Afgevraagd kan worden of dat een gewenste situatie is, zeker uit het oogpunt van privacy; gecentraliseerde medische informatie uitwisselen verhoogt de impact van compromitering van het LSP. End-to-end encryption zou medische informatie beschermen tegen inzage door onbevoegden, maar de informatiestromen zouden nog steeds duidelijke zichtbaar zijn.

De precieze structuur van het VPN waar GBZ'en op moeten aansluiten voor connectiviteit met het LSP, is in dit onderzoek niet duidelijk naar voren gekomen. Kunnen zorgverleners met behulp van hun UZI-pas verbinding maken met het LSP, of kunnen alleen geautoriseerde zorgsystemen dat? Wordt gebruik van encryptie (bijvoorbeeld SSL) verplicht gesteld bij deelname aan het VPN?

De manier waarop het LSP medische informatie doorgeeft is in dit onderzoek vrij duidelijk naar voren gebracht. Minder diepgaand is onderzocht hoe het uitwisselen van medische informatie bij zorgaanbieders onderling precies in zijn werk gaat. Welke informatie kan een zorgaanbieder verkrijgen aan de hand van het door het LSP uitgeschreven token? Wordt een zorgaanbieder met token alsnog geauthenticeerd, of neemt de dossier-ontsluitende zorgaanbieder genoegen met een token? Wie is er verantwoordelijk voor logging van directe uitwisseling van medische gegevens?

Het door het LSP bijgehouden toegangslog bevat informatie die de privacy van patiënten in gevaar kan brengen. Aan de hand van een gelogde aanvraag van een zorgaanbieder of zorgverlener kan worden afgeleid welke zorg een patiënt behoeft. Inzage in het toegangslog kan voor zorgverzekeraars reden zijn patiënten te weigeren op grond van hun (vermeende) medische historisch. Het bieden van inzage in het toegangslog, zoals het LSP wil realiseren, behoeft grote zorgvuldigheid.

In het ideale geval kan alleen de zorgverlener die een verwijzing in de VWI plaats, deze wijzigen of

verwijderen. Om praktische redenen is besloten dit te verruimen tot de zorgaanbieder onder wie de zorgverlener de verwijzing heeft aangemeld. Dit betekent dat, zeker bij grote zorgaanbieder, veel zorgverleners toegang hebben tot en invloed hebben op de verwijzingen in de VWI. Privacy van patiënten is in dit geval afhankelijk van de zorgaanbieder. Deze kan toegang tot de VWI softwarematig beperken of zich beroepen op het beroepsgeheim. De vraag is, of deze situatie wenselijk is.

Tijdens dit onderzoek is niet gekeken naar de samenstelling van de sleutels in de VWI. De vraag is of uit deze sleutels informatie af te leiden is, bijvoorbeeld over welk zorgsysteem bij welke zorgaanbieder hoort. Bij de patiëntgegevens-id is interessant of uit de sleutel valt op te maken bij welke patiënt een patiëntgegevens-id hoort. Indien sleutels worden samengesteld uit andere gegevens kan dit gevaar opleveren voor de privacy van patiënten.

Bijlage A: Architectuurprincipes AORTA

(Bron: Architectuurvisie AORTA v5.0, § 3.6)

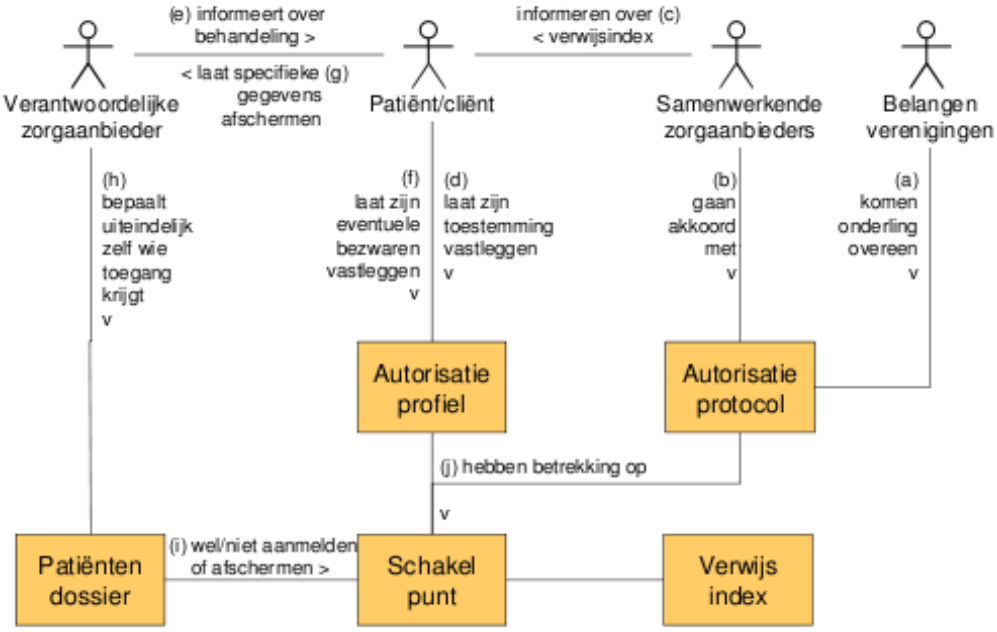
1. Waar mogelijk, is en blijft de opslag van patiëntgegevens in het bronsysteem van de verantwoordelijke zorgverlener. Daarmee kan de integriteit en actualiteit van de gegevens worden gerealiseerd en blijft de verantwoordelijkheid voor de gegevens waar die moet zijn: bij de bron.
2. De basisinfrastructuur biedt generiek functies om zorginformatiesystemen te kunnen aansluiten en informatie-uitwisseling mogelijk te maken, maar doet zo weinig mogelijk uitspraken over de interne werking van zorginformatiesystemen.
3. Voor het opzoeken en opslaan van patiëntinformatie wordt gebruik gemaakt van een unieke patiënt identificatie door middel van het landelijke Burger Service Nummer (BSN).
4. De basisinfrastructuur biedt mogelijkheden om:
   a. Patiënten te identificeren via een landelijk register de SBV-Z;
   b. Zorgverleners, zorgverzekeraars en zorginformatiesystemen te identificeren en authenticeren via landelijke registers;
   c. Patiëntgegevens op te vragen en te versturen;
   d. Te abonneren op patiëntgegevens.
5. In de basisinfrastructuur wordt voor de uitwisseling van patiëntgegevens tussen GBZ'en in principe gebruik gemaakt van een landelijk schakelpunt.
6. Voor het snel en efficiënt vinden en toegankelijk maken van de gezochte informatie wordt in een landelijk schakelpunt gebruik gemaakt van een verwijsindex (een verwijsindex geeft aan waar bepaalde informatie ligt opgeslagen). Aan deze verwijsindex zijn de volgende functies gekoppeld:
   a. authenticatie van de aanvragende zorgverlener, om te kunnen bepalen of hij daadwerkelijk degene is die hij beweert te zijn;
   b. autoriseren van toegang tot de patiëntgegevens;
   c. loggen van de aanvragen en antwoorden om de rechtmatigheid van aanvragen achteraf te kunnen controleren.
7. De basisinfrastructuur geeft zorgverleners toegang tot patiëntgegevens op basis van generieke autorisatie gericht op de rol van de zorgverlener (autorisatieprotocol), rekening houdend met eventueel vastgelegde wensen van de patiënt (autorisatieprofiel); autorisatieprotocollen en –profielen worden landelijk beheerd.
8. De basisinfrastructuur biedt verschillende beveiligingsniveaus voor beschikbaarheid, vertrouwelijkheid en onweerlegbaarheid en één niveau voor de integriteit van patiëntgegevens.
9. Aangesloten zorginformatiesystemen moeten aan specifieke eisen voldoen ten aanzien van beveiliging en beheer. Deze eisen hebben betrekking op het zorgdragen voor integere, actuele, volledige patiëntgegevens die 7 dagen per week en 24 uur per dag beschikbaar zijn. Een dergelijk systeem wordt aangeduid met de term GoedBeheerd Zorgsysteem (GBZ).
10. Zorg Service Providers (ZSP's) zorgen ervoor dat de systemen van zorgpartijen aangesloten zijn

op de ZIM. Naast communicatiediensten voor toegang tot de ZIM kunnen partijen aanvullende diensten bieden zoals bijvoorbeeld specifieke content etc.

11. Uitgave, beheer en valideren van identiteitcertificaten van de zorgverleners en zorgsystemen vindt plaats met behulp van een landelijk centraal Unieke Zorgverleners Identificatie (UZI) -register. Als vertrouwensmiddel maken zorgverleners en hun systemen gebruik van UZI-passen.
12. Op technisch niveau zijn keuzen gemaakt die aansluiten bij bestaande praktijken voor uitwisseling van medische gegevens tussen zorgverleners. Daarbij wordt gekozen voor berichtuitwisseling op basis van HL7 versie 3 vanwege de groeimogelijkheden richting een EPD en de aansluiting bij internationale ontwikkelingen.
13. De uitwisseling van patiëntgegevens tussen GBZ'en en basisinfrastructuur geschiedt via Web Service Messaging, en internetprotocollen. Het op deze wijze uitwisselen van berichten met behulp van Internettechnologie, is gestandaardiseerd door het internationale standaardisatie-instituut W3C en wordt door alle grote leveranciers en systeemhuizen in de markt ondersteund.
14. De uitwisseling van patiëntgegevens wordt op transportniveau beveiligd met SSL/TLS en Virtual Private Networks (VPN).

Bijlage B: Autorisatiemechanisme AORTA

(Bron: Bedrijfsarchitectuur AORTA, v3.0, § 9.2)



De bovenstaande figuur toont het autorisatiemechanisme in een UML collaboration diagram.

a. Beroepsverenigingen van zorgaanbieders formuleren in overleg met belangenverenigingen van patiënten/cliënten een autorisatieprotocol, waarin staat wélke soorten patiëntgegevens een zorgaanbieder, op grond van zijn functie, nodig kan hebben voor een adequate behandeling.
b. Samenwerkende zorgaanbieders die willen aansluiten op hetzelfde schakelpunt moeten akkoord gaan met het autorisatieprotocol en verklaren dat zij patiëntgegevens alleen zullen opvragen in het kader van een behandelrelatie.
c. Samenwerkende zorgaanbieders die hun patiëntdossiers hebben aangesloten op hetzelfde schakelpunt, informeren hun patiënten/cliënten wanneer zij hun patiëntgegevens aanmelden bij de verwijsindex.
d. Patiënten/cliënten kunnen het al of niet akkoord gaan met elektronische uitwisseling van hun patiënt-/cliëntgegevens, centraal (laten) vastleggen in een autorisatieprofiel.
e. Bij iedere zorgvraag informeert de verantwoordelijke zorgaanbieder zijn patiënt/cliënt over welke andere zorgaanbieders in het kader van de behandeling toegang tot zijn patiëntgegevens zullen krijgen.
f. Patiënten/cliënten kunnen wensen of bezwaren m.b.t. bepaalde zorgaanbieders die wel of geen toegang mogen krijgen, centraal (laten) vastleggen in het autorisatieprofiel.
g. Patiënten/cliënten kunnen specifieke patiëntgegevens laten afschermen door de zorgaanbieder

zelf.

h. De verantwoordelijke zorgaanbieder blijft aanspreekbaar op zijn beroepsgeheim. Daarom moet hij ongeacht het autorisatieprotocol en het autorisatieprofiel uiteindelijk zelf kunnen bepalen welke gegevens opvraagbaar zijn.
i. Dit kan de zorgaanbieder bepalen door het wel of niet aanmelden van patiëntgegevens bij de verwijsindex in combinatie met het vrijgeven of afschermen van specifieke gegevens voor opvraag door andere zorgaanbieders.
j. Het autorisatieprotocol en de autorisatieprofielen hebben betrekking op alle patiëntdossiers die zijn aangesloten op het schakelpunt, behalve dat ieder autorisatieprofiel betrekking heeft op de patiëntdossiers van één patiënt/cliënt.
k. In gevallen waarvoor dit autorisatiemechanisme niet werkt, zal het bij het opvragen van patiëntgegevens mogelijk moeten zijn expliciete toestemming van de verantwoordelijke zorgaanbieder te vragen.

Opmerkingen:

- Ad (a) de invulling van het autorisatieprotocol is geen sinecure. Het kan enige tijd duren voordat de koepelverenigingen hierover volledige overeenstemming bereiken, daarom wordt het protocol incrementeel ingevuld naar de behoefte van de landelijke toepassingen, te beginnen met EMD en WDH, zie [EMD-autorisatie] en [WDH-autorisatie].
- Ad (a) een strak autorisatieprotocol heeft het nadeel dat een zorgverlener in onvoorziene omstandigheden geen toegang tot patiëntgegevens kan krijgen, terwijl dat toch noodzakelijk is, bijv. in levensbedreigende gevallen. Voor dergelijke noodsituaties moet er de mogelijkheid zijn het autorisatieprotocol te doorbreken.
- Bij (b) is het wenselijk dat zorgaanbieders ervoor tekenen dat degenen die patiëntgegevens opvragen zich aansprakelijk stellen voor eventueel misbruik, opdat de verantwoordelijke zorgaanbieder zoveel mogelijk wordt gevrijwaard van aanspraken op zijn beroepsgeheim. Zonder deze waarborg zullen zorgaanbieders hun patiëntdossiers minder gauw willen aansluiten op het schakelpunt.
- Met (b) wordt tevens het probleem omzeild dat alle behandelrelaties met een patiënt/cliënt niet tijdig vooraf vastgelegd kunnen worden. Overigens speelt dit probleem op kleinere schaal ook binnen ziekenhuizen. Daar worden vaak slimme oplossingen gebruikt, bijv. door een elektronisch vastgelegde afspraak van een patiënt/cliënt met een zorgverlener te beschouwen als blijk van een behandelrelatie. Die afspraak moet dan wel door een onafhankelijke, bevoegde partij worden vastgelegd. Op landelijke schaal is deze oplossing vrijwel niet haalbaar.
- Bij (b) zal het autorisatieprotocol alleen betrekking hebben op zorgverleners en niet op hun medewerkers. In paragraaf 9.4 wordt beschreven hoe ook medewerkers als “verlengde arm” van een zorgverlener kunnen optreden.
- Bij (c) is het informeren van patiënten/cliënten noodzakelijk op grond van de [WBP], omdat de inhoud van de verwijsindex als persoonsgegevens kan worden aangemerkt. Bij voorkeur doen alle zorgaanbieders in een regio dit gecoördineerd en sturen zij gezamenlijk één brief per patiënt/cliënt, eventueel gecombineerd met de uitgifte van een landelijk of regionaal

patiëntnummer, zie paragraaf 10.2. In theorie zou dit aanmelden bij de verwijsindex, en dus ook het informeren van de patiënt/cliënt, kunnen wachten tot de eerstvolgende keer dat de patiënt/cliënt naar een zorgaanbieder gaat. Echter, dit zou voor vele patiënten/cliënten betekenen dat, in afwachting van die eerstvolgende keer, hun patiëntgegevens in noodgevallen niet kunnen worden opgevraagd.

- Bij (d) kan met de juiste voorlichting goedkeuring worden verondersteld, tenzij een patiënt/cliënt bezwaar maakt. Deze aanpak is doeltreffender dan andersom, want vele patiënten/ cliënten zullen het nalaten om te reageren.
- Bij (e) zou de zorgaanbieder zijn patiënt/cliënt idealiter moeten informeren over:
  - Welke andere zorgaanbieders kunnen worden betrokken bij de behandeling,
  - Welke zorgaanbieders onderling elektronische patiëntgegevens kunnen uitwisselen en wat daarvan de voordelen zijn,
  - Welke soorten gegevens die andere zorgaanbieders op grond van hun rol dan mogen inzien, onder verwijzing naar het autorisatieprotocol,
  - Welke keuzemogelijkheden de patiënt/cliënt hierin heeft,
  - Welke verdere technische voorzieningen (beveiliging, logging) worden gebruikt om de privacy van de patiënt/cliënt te waarborgen,
  - Welke controle-, bezwaar- en beroepsmogelijkheden de patiënt/cliënt heeft.

  In de praktijk heeft een zorgverlener helemaal geen tijd om dit expliciet met iedere patiënt/cliënt door te nemen. In plaats daarvan kan hij zijn patiënten/cliënten impliciet informeren via een folder en/of affiche in de wachtkamer.
- Bij (f) kan het autorisatieprofiel door de zorgaanbieder worden vastgelegd, maar in de praktijk zal die daar geen tijd voor hebben. Daarom is er een andere partij nodig die dit voor de patiënten/cliënten vastlegt, want dan is een patiënt/cliënt niet afhankelijk van een drukke zorgaanbieder om eenmaal gegeven toestemming weer te kunnen intrekken. Als in de toekomst de e-NIK beschikaar is, kunnen patiënten/cliënten zelf hun wensen via het internet vastleggen.
- Bij (f) is het goed denkbaar dat een patiënt/cliënt alleen de hem bekende of behandelende zorgverleners toegang wil geven. Op het moment dat hij onverwacht een nieuwe zorgverlener bezoekt, blijkt dat die zorgverlener zijn patiëntgegevens niet kan inzien. De patiënt/cliënt wil die zorgverlener alsnog toegang geven, maar kan dat ter plekke niet, want daarvoor moet hij eerst terug naar de beheerder van het autorisatieprofiel. Wanneer de e-NIK is ingevoerd komen er mogelijkheden voor de patiënt/cliënt om ter plekke een zorgverlener toestemming te geven.
- Bij (f) kan de patiënt/cliënt bijvoorbeeld wensen dat hij niet wil dat een bepaalde zorgaanbieder (bijv. een buurman die toevallig zorgverlener is) inzage krijgt in zijn patïentgegevens. Dit is een alles-of-niets kwestie: hij kan níet selectief aangeven dat voor die zorgverlener alleen gevoelige patiëntgegevens (bijv. mbt. psychiatrie, HIV-besmetting, abortus) worden uitgesloten.
- Bij (g) kan de patiënt/cliënt onder begeleiding van de zorgaanbieder wél selectief aangeven dat hij bepaalde gevoelige patiëntgegevens wil laten afschermen, maar dan voor alle andere zorgaanbieders. De zorgaanbieder kan de patiënt/cliënt dan wijzen op de consequenties, bijvoorbeeld dat een opvragende zorgaanbieder zou worden geconfronteerd met onvolledige patiëntgegevens, terwijl juist de gevoelige gegevens vaak cruciaal zijn voor andere

zorgaanbieders.

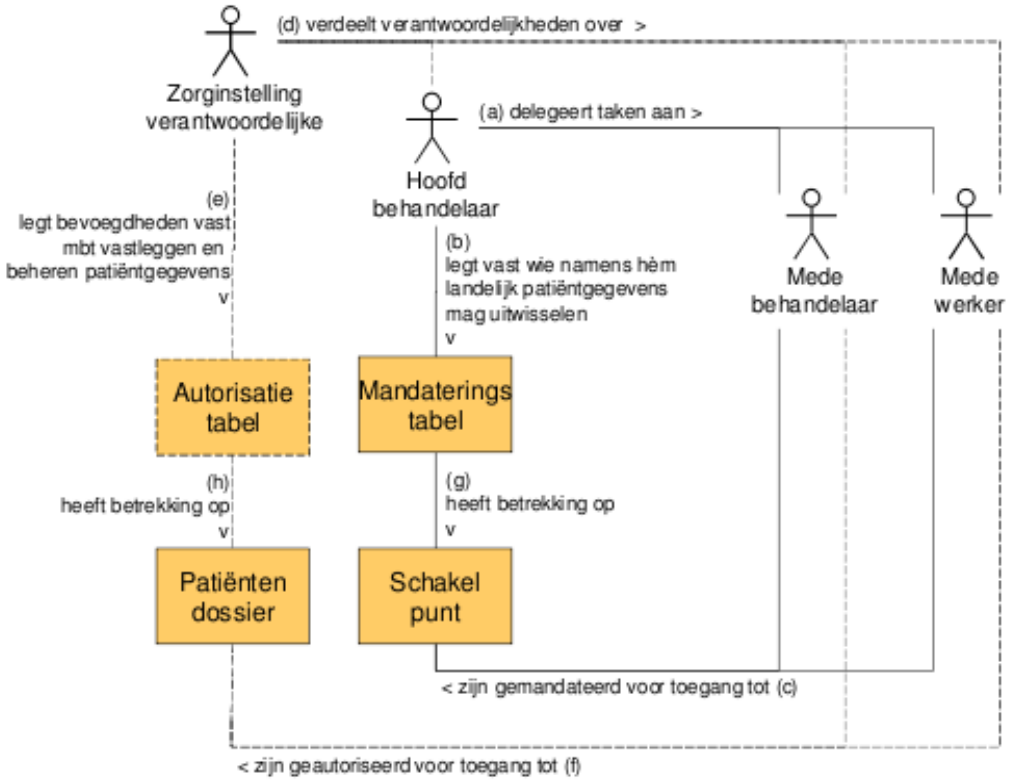
- Bij (h) kan een zorgaanbieder uiteindelijk zelf bepalen, in hoeverre hij tegemoet komt aan de wensen van een patiënt/cliënt. Desnoods kan hij een lastige patiënt/cliënt de simpele keuze voorleggen: wél of níet meedoen met elektronische uitwisseling van patiëntgegevens.
- Ad (i) het aanmelden van patiëntgegevens aan de verwijsindex is net zo gevoelig als het opvragen van patiëntgegevens. Ook deze handeling is voorbehouden aan de verantwoordelijke zorgverleners.
- Ad (j) het autorisatieprotocol en het autorisatieprofiel zijn slechts een hulpmiddel en hebben juridisch geen betekenis. De zorgaanbieder blijft verantwoordelijk om voor individuele gevallen te beoordelen. Het autorisatieprotocol is echter nodig als vertrouwenwekkende basis, opdat afzonderlijke zorgaanbieders bereid zullen zijn hun patiëntdossiers aan te sluiten op het schakelpunt. Evenzo is het autorisatieprofiel nodig om patiënten/cliënten te overtuigen dat ze akkoord kunnen gaan met elektronische uitwisseling van hun patiëntgegevens. Het alternatief zou zijn dat iedere zorgaanbieder zelf vastlegt welke andere zorgaanbieders toegang tot zijn dossier krijgen, zoals dit in sommige regionale toepassingen wordt geregeld. Op kleine schaal kan dat werken, maar op landelijke schaal wordt dit onbeheersbaar voor de zorgaanbieders en ondoorzichtig voor de patiënt/cliënt.
- Hoewel het hier beschreven autorisatiemechanisme vooral is bedoeld voor het opvragen van patiëntgegevens, kan dit mechanisme evengoed worden toegepast voor het versturen van patiëntgegevens.
- Hoewel het hier beschreven autorisatiemechanisme vooral is bedoeld voor de uitwisseling van medische gegevens, kan dit mechanisme evengoed worden gebruikt voor persoonlijke, logistieke en financiële gegevens.
- Het autorisatieprotocol en –profiel zijn in principe bedoeld voor de landelijke uitwisseling van patiëntgegevens. Echter, als landelijk verkregen patiëntgegevens lokaal worden opgeslagen binnen een zorginstelling, kunnen die gegevens alsnog in verkeerde handen vallen, bijv. als binnen de zorginstelling geen interne autorisatie is geregeld of als die interne autorisatie in strijd is met de landelijke autorisatie. Zie verder paragraaf 9.4.

Openstaande punten:

- Bij (b) kan het noodzakelijk zijn dat alle zorgverleners afzonderlijk moeten tekenen. Dit kan betekenen dat bij het schakelpunt moet worden vastgelegd welke zorgverleners hebben getekend en alleen dan deze zorgverleners met hun UZI-pas toegang tot het schakelpunt kunnen krijgen.

Bijlage C: Mandateringsmechanisme zorgaanbieder

(Bron: Bedrijfsarchitectuur AORTA, v3.0, § 9.4)



De bovenstaande figuur toont het delegatiemechanisme in een UML collaboration diagram.

a. De hoofdbehandelaar delegeert bepaalde taken aan zijn medebehandelaren en medewerkers.
b. De hoofdbehandelaar legt overeenkomstig in een mandateringstabel vast wie namens hèm landelijk patiëntgegevens mag uitwisselen.
c. Aldus worden medebehandelaren en medewerkers gemandateerd voor toegang tot het schakelpunt voor het uitwisselen van patiëntgegevens.
d. In geval van een zorginstelling worden zorgverleners aangesteld in een bepaalde functie en worden verantwoordelijkheden verdeeld over zorgverleners en medewerkers.
e. Overeenkomstig wordt in een interne autorisatietabel vastgelegd welke bevoegdheden zorgverleners en medewerkers krijgen m.b.t. de lokale patiëntdossiers.
f. Aldus worden zorgverleners en medewerkers geautoriseerd voor toegang tot de lokale patiëntdossiers.
g. De lokale mandateringstabel heeft betrekking op het landelijk schakelpunt.
h. De interne autorisatietabel, indien aanwezig, heeft betrekking op de lokale patiëntdossiers.

Opmerkingen:

- Ad (a) hoewel deze taakverdeling per zorgcontact anders kan zijn, zal in de praktijk vaak een karakteristiek samenwerkingspatroon ontstaan, bijv. in de vorm van behandelteams.
- Ad (b) deze mandateringstabel kan dus specifiek pèr zorgverlener (als hoofd- behandelaar) aangeven welke zorgverleners (als medebehandelaar) en medewerkers gemandateerd worden voor het uitwisselen van welke soorten patiëntgegevens.
- Ad (c) met deze mandatering kan een medebehandelaar of medewerker handelingen uitvoeren die anders zijn voorbehouden aan de hoofdbehandelaar.
- Ad (d) in een ziekenhuis is het vaak de medische directeur die, in overleg met een staf van specialisten, de bijbehorende bevoegdheden bepaalt.
- Ad (e) de invulling van de interne autorisatie is de verantwoordelijkheid van de zorginstelling en zal vaak wezenlijk verschillen van de landelijke autorisatie. Bijvoorbeeld omdat in een ziekenhuis aan de hand van de agenda of de dossiers kan worden gecontroleerd of een zorgverlener een behandelrelatie heeft met een patiënt/cliënt. Om te voorkomen dat landelijk uitgewisselde patiëntgegevens alsnog in verkeerde handen kunnen vallen, dient te worden gecontroleerd dat een zorginstelling adequate interne autorisatie heeft geregeld, maar is de wijze waarop niet belangrijk.
- Ad (g) ten behoeve van autorisatie en logging, zal een gemandateerde uitvoerder (binnen HL7v3 “author or performer” genoemd) altijd moeten aangeven namens welke mandaterende zorgverlener (binnen HL7v3 “overseer” genoemd) hij handelt. In geval van behandelteams moet dan wel duidelijk worden bepaald welke zorgverlener als hoofdbehandelaar optreedt.
- Ad (h) hoe de logging van toegang tot het lokale patiëntdossier wordt geregeld, is de verantwoordelijkheid van de zorginstelling.

Bijlage D: Overzicht zorgverlenerfuncties

(Bron: Bedrijfsarchitectuur AORTA v3.0, § 3.4)

Een zorgverlener is een natuurlijke persoon die beroepsmatig zorgdiensten verleent aan een patiënt/cliënt. Er zijn zorgverleners met zeer uiteenlopende beroepstitels.
Volgens de Wet BIG zijn bepaalde beroepstitels wettelijk beschermd:

- Arts
- Tandarts
- Apotheker
- Gezondheidspsycholoog
- Psychotherapeut
- Fysiotherapeut
- Verloskundige
- Verpleegkundige

Daarnaast laat Artikel 34 van de Wet BIG toe via een AmvB de volgende beroepstitels toe te voegen:

- Apothekersassistent
- Diëtist
- Ergotherapeut
- Huidtherapeut
- Logopedist
- Mondhygiënist
- Oefentherapeut (Mensendieck/Cesar)
- Optometrist
- Orthotpist
- Podotherapeut
- Radiodiagnostisch laborant
- Radiotherapeutisch laborant

Binnen sommige beroepstitels is sprake van vergaande specialisatie, zoals vastgesteld door de respectievelijke beroepsverenigingen, bijvoorbeeld:

- Arts
  - Allergologie
  - Anesthesiologie
  - Cardio-thoracale chirurgie
  - Cardiologie
  - Dermatologie en venerologie

    - Gastro-enterologie
    - Huisartsgeneeskunde
    - Etc.
- Tandarts
    - Dento-maxillaire orthopaedie
    - Mondziekten en kaakchirurgie

Men mag die beroepen met eventuele specialismen pas uitoefenen, als men daarvoor de benodigde kwalificaties heeft. Deze kwalificaties worden vastgelegd en bijgehouden in het BIG-register resp. het Kwaliteitsregister Paramedici. Het gaat hier om diploma's, maar ook om eventuele nascholing en in de toekomst misschien ook om tuchtrechtelijke zaken.

Aldus definiëren we het begrip zorgverlener-kwalificaties als de kwalificaties van een zorgverlener, zoals vastgelegd in het BIG-register of het Kwaliteitsregister Paramedici, die bepalen dat hij een bepaald beroep met eventuele specialismen mag uitoefenen.

Voor wat betreft de daadwerkelijke uitoefening geldt dat zorgverleners zelfstandig vanuit een eigen praktijk, binnen een zorginstelling, beide of helemaal niet werken:

- Individuele uitoefening is toegestaan voor bepaalde beroepen, voor sommige daarvan (bijvoorbeeld gezondheidspsychologen) geldt een vrije vestiging, voor andere gelden vestigingsvoorwaarden. Als een zorgverlener meerdere beroepstitels heeft, zal altijd duidelijk moeten zijn welk beroep hij vanuit een bepaalde vestiging uitoefent.
- Uitoefening binnen een zorginstelling is verplicht voor de meeste specialismen. Als een zorgverlener gaat werken voor een zorginstelling, draagt hij de aansprakelijkheid over aan de (medisch) directeur van die zorginstelling. Als een zorgverlener meerdere beroepstitels en/of specialismen heeft, zal de directeur hem gewoonlijk aanstellen in één beroep, met één of meerdere sterk gerelateerde specialismen.

Aldus definiëren we het begrip zorgverlener-functie als het beroep met één of meer gerelateerd(e) specialisme(n) dat een zorgverlener daadwerkelijk uitoefent vanuit zijn zorgverlenerpraktijk of volgens zijn aanstelling binnen een zorginstelling.

Merk op dat er geen exacte 1-op-1 relatie bestaat tussen zorgverlener-kwalificaties en zorgverlener-functie. Immers, iemand met bepaalde zorgverlener-kwalificaties, maar zonder vestiging of aanstelling als zodanig, heeft geen zorgverlener-functie. Dit onderscheid is belangrijk bij het toekennen van bevoegdheden tot inzage in patiëntgegevens, zie paragraaf 9.2.

Let op: sommige zorgpartijen hebben weliswaar arts als beroepstitel, maar zijn toch geen zorgverlener:

- Een keuringsarts onderzoekt de gezondheid van een (potentiële) werknemer, met als doel diens geschiktheid voor bepaalde werkzaamheden te bepalen. Zijn opdrachtgever is meestal de

(potentiële) werkgever.
- Een verzekeringsarts onderzoekt of bepaalde zorgdiensten in aanmerking komen voor vergoeding door de zorgverzekeraar. Zijn opdrachtgever is de zorgverzekeraar.

Daarentegen werkt de zorgverlener in opdracht van de patiënt/cliënt en is zijn doel gericht op de verbetering van diens gezondheidstoestand.

Opmerkingen:

- Het begrip functie komt overeen met het begrip role in [HL7v3] en het begrip structural role in [prENV13606:2003].
- De apotheekhoudende huisarts lijkt in eerste instantie niet in het bovenstaande stramien te vatten. Deze zorgverlener is formeel huisarts en heeft dus niet dezelfde bevoegdheden als een apotheker.
- Een co-assistent is geen arts en wordt hier dus niet als zorgverlener beschouwd, maar als medewerker. Een AG(N)IO is een arts, zij het zonder specialisme, en wordt dus wel als zorgverlener beschouwd. Zie verder paragraaf 3.3.3.

Bijlage E: Gegevenssoortentabel

(Bron: Informatiesysteemarchitectuur AORTA v3.0, § 5.4)

De gegevenssoortentabel vertelt het schakelpunt welke gegevenssoorten in aanmerking komen voor iedere soort opvraag. Deze tabel is nodig omdat op basis van een bepaalde HL7-interactie-id niet automatisch kan worden afgeleid welke aanmeldbare gegevenssoort wordt opgevraagd. De oorzaak daarvan ligt in het feit dat patiëntstukken en hun gegevenssoorten niet allemaal hetzelfde aggregatieniveau hebben [...].

Bijvoorbeeld, als een huisarts een eerstelijnsdossier als gegevenssoort aanmeldt bij de verwijsindex, komt dit dossier in principe in aanmerking voor opvraag van de volgende gegevenssoorten:

- Professionele samenvatting voor DWH
- Professionele samenvatting voor SEH
- Medicatievoorschriften

Gewoonlijk is is er een eenvoudige 1-op-1 relatie. Bijvoorbeeld, als een apotheek medicatieverstrekkingen aanmeldt bij de verwijsindex, komt diens dossier alleen in aanmerking voor opvraag van medicatieverstrekkingen.

De gegevenssoortentabel zal bestaan uit een lijst met regels die ieder bevatten:

- Een gegevenssoort-id als aanmeldbare gegevenssoort
- Een HL7-interaction-id als opleverbare gegevenssoort

Daarin kan iedere HL7-interactie en iedere gegevenssoort meer malen voorkomen. Op deze wijze kan één HL7-interactie gebonden worden aan meerdere opleverbare gegevenssoorten en andersom.

De onderstaande figuur geeft een voorbeeld (met suggestieve tekst in plaats van onbegrijpelijke codes) van deze tabel voor de zorgtoepassingen EMD en WDH.

Gegevenssoort	HL7-interaction
Index	opvragenIndex
Medicatievoorschrift	opvragenMedicatievooschriften
Medicatieverstrekking	opvragenMedicatieverstrekkingen
Eerstelijnsdossier	opvragenSamenvattingVoorDWH
Eerstelijnsdossier	opvragenSamenvattingVoorSEH

Bijlage F: Vertrouwensmodel AORTA

(Bron: Architectuurvisie AORTA v5.0, § 3.5)

Het vertrouwensmodel voor de landelijke basisinfrastructuur (AORTA) beschrijft de samenhang tussen wet- en regelgeving (zoals patiëntenrechten), informatiebeveiliging en de keten van: identificatie, authenticatie, autorisatie en logging. Bovendien maken communicatie en toezicht deel uit van het model. Het doel van het vertrouwensmodel is dat patiënten en zorgaanbieders (later ook zorgverzekeraars) vertrouwen kunnen hebben in veilige en betrouwbare elektronische gegevensuitwisseling in de zorg. Hierbij is met name de keten van identificatie, authenticatie, autorisatie en logging (plus toezicht) van belang. Onder andere vanwege het medisch beroepsgeheim is het belangrijk dat patiëntgegevens slechts ter beschikking komen van degenen die daartoe bevoegd zijn.

Zorgverleners en patiënten moeten bij deelname aan de landelijke infrastructuur er op kunnen vertrouwen dat – via het LSP - alleen geautoriseerde zorgverleners bij de (medische) gegevens komen en dat deze zorgverleners op de juiste wijze met de gegevens omgaan. Daarbij hoort ook een onafhankelijke en onomstreden organisatie die toeziet op het gebruik van de transmurale elektronische gegevensuitwisseling. Door identificatie wordt de identiteit van zorgconsumenten en zorgverleners vastgesteld. Identificatie van zorgconsumenten zal gaan geschieden via het BSN. Voor de identificatie van zorgverleners worden UZI-nummers gebruikt.
Na identificatie is het noodzakelijk om via authenticatie met zekerheid te kunnen vaststellen dat iemand daadwerkelijk degene is die hij/zij, met zijn identificatienummer, zegt te zijn. Gezien de aard van de betrokken gegevens is het van belang dat authenticatiemiddelen worden gebruikt die een grote mate van zekerheid bieden. Het authenticatiemiddel dat deze zekerheid voor zorgaanbieders biedt is de persoonlijke UZI- pas. De UZI-pas is een elektronisch zorgverlenerpaspoort.

Als bekend is wie iemand is (identificatie) en ook zeker is dat het echt die persoon is (authenticatie), dan komt de volgende stap: autorisatie. Autorisatie gaat namelijk over de vraag wie, onder welke voorwaarde toegang mag krijgen tot de beschikbare gegevens van zorgconsumenten. Daarnaast gaat autorisatie over de vraag tot wélke gegevens iemand toegang mag krijgen. Bij het landelijk schakelpunt (LSP) krijgen zorgverleners op basis van hun beroep (rol) per zorgtoepassing (te beginnen met EMD en WDH) toegang tot een gespecificeerde set van zorggegevens. Voor het EMD zijn dit in eerste instantie artsen en apothekers. Voor het waarneemdossier zijn dit huisartsen en waarnemend huisartsen.

Door het vastleggen (logging) van wie, wanneer, welke gegevens heeft geraadpleegd of gewijzigd kan achteraf worden vastgesteld of dit rechtmatig is gebeurd op grond van wet- en regelgeving.

Eventueel misbruik door een zorgverlener (bijvoorbeeld het ten onrechte opvragen van het medicatiedossier van premier Balkenende) dient door het LSP en de bijbehorende onafhankelijke toezichthouder zelfstandig te kunnen worden vastgesteld, onder andere door logginganalyse op basis van de persoonlijke UZI-pas die door de zorgverlener is gebruikt. Zelfstandige authenticatie van de

zorgverlener door het LSP (inclusief het bepalen van de rol van de zorgverlener, zoals opgenomen in de persoonlijke UZI-pas) is een belangrijk uitgangspunt in de AORTA-specificaties en van het vertrouwensmodel dat in de afgelopen jaren met betrokken partijen is opgesteld. Op basis daarvan zijn eisen geformuleerd voor XIS-leveranciers.

Het autorisatiemechanisme dient ook rekening te houden met de wensen van de patiënt voor zover deze kenbaar zijn gemaakt. Daartoe voorziet de basisinfrastructuur in een centraal in te stellen autorisatieprofiel, waarin per patiënt kan worden vastgelegd welke beperkingen er in acht moeten worden genomen bij toegang tot zijn gegevens. Uiteindelijk dient in de basisinfrastructuur een voorziening te zijn opgenomen waarmee patiënten zelf hun autorisatieprofiel kunnen aanpassen. Dat zou bijvoorbeeld mogelijk kunnen worden zodra de eNIK (elektronische Nationale IdentiteitsKaart) of een andere 'sterke' authenticatievoorziening voor de burger gerealiseerd is. In de beginsituatie wordt gebruik gemaakt van een beperktere invulling van het autorisatieprofiel (alleen aan/uit), waarbij instelling ervan niet rechtstreeks door de patiënt hoeft plaats te vinden. Gedacht wordt aan een nog nader aan te wijzen autorisatiebeheerder die op basis van een schriftelijk verzoek van een patiënt, de toegang tot zijn medische gegevens kan vrijgeven en blokkeren.
Na introductie van de eNIK kan de patiënt direct zelf bepalen welke personen/instellingen of groepen voor welke zorgtoepassing toegang hebben dan wel hen de toegang ontzeggen. De patiënt kan dan in het LSP zijn autorisatieprofiel instellen, inzage krijgen in loggegevens waarin staat welke zorgverlener toegang heeft gekregen tot zijn zorggegevens, zien waar zijn zorggegevens ligt opgeslagen en toegang krijgen tot die gegevens.