



Ministerie van Volksgezondheid,
Welzijn en Sport

Technisch Ontwerp

Generieke Functie Lokalisatie

Versie 0.9.0

Inhoudsopgave

1	1	Documenthistorie.....	4
2	2	Leeswijzer.....	5
3	3	Inleiding.....	5
4	3.1	Positie ten opzichte van het functioneel ontwerp en de implementation guide	5
5	3.2	Scope en afbakening.....	6
6	3.2.1	Binnen scope	6
7	3.2.2	Buiten scope	6
8	4	Systeemoverzicht.....	6
9	4.1	Componentlandschap.....	6
10	4.1.1	Nationale Verwijsindex (NVI)	8
11	4.1.2	Pseudoniemenregistratieservice (PRS)	8
12	4.1.3	Localization Registration Client.....	8
13	4.1.4	Localization Search Client.....	9
14	4.1.5	Custodian Server	9
15	4.2	Centraal en decentraal	9
16	4.3	Koppelvlakken	10
17	4.3.1	Pseudoniemenregistratieservice.....	10
18	4.3.2	Nationale Verwijsindex	11
19	4.3.3	Custodian Server	11
20	4.3.4	Wat hieruit volgt voor een aansluitende partij.....	12
21	5	Architectuurprincipes en -keuzes	12
22	5.1	Architectuurprincipes.....	12
23	5.1.1	Onderwerp pseudonimisering en gegevensminimalisatie.....	12
24	5.1.2	Onderwerp beveiliging en vertrouwen	13
25	5.1.3	Onderwerp Interoperabiliteit en standaarden	13
26	5.2	Architectuurkeuzes.....	13
27	5.2.1	Onderwerp lokaliseren en vervolgstappen	13
28	5.2.2	Onderwerp Pseudonimisering en gegevensminimalisatie.....	17
29	5.2.3	Onderwerp registreren en verwijderen	23
30	5.2.4	Onderwerp interoperabiliteit en standaarden	28
31	5.2.5	Onderwerp beveiliging en vertrouwen	29
32	6	Verdiepingen.....	34
33	6.1	Verdieping: pseudonimisering.....	34
34	7	Interfaces en transacties.....	38
35	7.1	Transactieoverzicht	38
36			

37	7.2	Transacties.....	38
38	8	Afhankelijkheden van andere generieke functies	39
39	8.1	Generieke functie Adressering	39
40	8.2	Generieke functie Autorisatie	40
41	8.3	Generieke functies Identificatie en Authenticatie	41
42	8.4	Generieke functie Toestemming	41
43	9	Referenties.....	43
44		Appendix A. Besluitonderbouwingen	43
45		A.1 De tussenoplossing voor autorisatie van de Bevragende Zorgaanbieder	43
46		A.2 Topologie: Gecentraliseerde verwijzindex	45
47		Appendix B. Bronvermeldingen	47

48

1 Documenthistorie

Versie	Status	Datum	Auteur	Wijziging
0.4	Concept	April 2026	VWS	- Initiële versie
0.6	Concept	Augustus 2026	VWS	- Verwerken interne review opmerkingen - Aanpassing hoofdstukindeling
0.8	Concept	Oktober 2026	VWS	- Verwerking commentaren van DA - Verwijderen van datacategorie uit lokalisatie-record - Introductie zoekcontext - Splitsen Lokalisatie-client in Localization Registration Client en Localization Search Client - Introductie Custodian server
0.9	Concept	Oktober 2026	VWS	- Verwerking DA 14 oktober 2026 - Nieuwe keuze 5.2.1.4 Zoekcontext op kenmerken van de bronhouder - Uniekheidssleutel en systeemconcept consistent gemaakt - Time-out Custodian Server verlaagd naar 1 seconde - Toestemming: huidige situatie en doorkijk naar EHDS; kruisverwijzingen hersteld

49

2 Leeswijzer

Hoofdstuk 5 is het kern-hoofdstuk: daar staan de architectuurprincipes en de architectuurkeuzes. De hoofdstukken eromheen bestaan om die keuzes plaatsbaar te maken.

In hoofdstuk 5 zijn de keuzes verdeeld over de volgende thema's:

- Pseudonimisering en gegevensminimalisatie: wat de NVI wel en niet mag weten, en hoe dat is afgedwongen.
- Registreren en verwijderen: de levenscyclus van een lokalisatie-record.
- Lokaliseren en vervolgstappen: het zoeken zelf en de overdracht naar Adressering.
- Interoperabiliteit en standaarden: de vervangbaarheid van het koppelvlak.
- Beveiliging en vertrouwen: toegang tot het koppelvlak, de autorisatie van vragen, de beslissing van de Datahoudende Zorgaanbieder en logging.

Hoofdstuk 6 bevat een verdieping: een mechanisme waar meerdere keuzes op steunen, apart uitgelegd zodat die keuzes kort kunnen blijven.

3 Inleiding

Dit document beschrijft het technisch ontwerp van de generieke functie Lokalisatie. Het legt vast welke architectuurkeuzes aan het ontwerp ten grondslag liggen en waarom die zo zijn gemaakt.

De lokalisatiefunctie beantwoordt één vraag: welke zorgaanbieders hebben gegevens over een bepaalde patiënt, binnen de zoekcontext die de zorgverlener opgeeft. De functie omvat de hele keten van de vraag van de zorgverlener tot en met het resultaat scherm. Daarbinnen is het opzoeken van endpoints gedelegeerd aan de generieke functie Adressering.

3.1 Positie ten opzichte van het functioneel ontwerp en de implementation guide

Er zijn drie documenten die elkaar niet overlappen.

- Het Functioneel ontwerp generieke functie Lokalisatie beschrijft wat de functie doet, gezien vanuit de zorggebruiker (deel A) en per component (deel B): use cases, functionele requirements, gegevens op logisch niveau en het informatiemodel.
- De Implementation Guide (IG) beschrijft normatief hoe het gebouwd wordt: FHIR-profielen, transacties, CapabilityStatements, ValueSets, zoekparameters en foutafhandeling.
- Dit document, het technisch ontwerp generieke functie Lokalisatie, beschrijft het waarom en het overzicht. Het legt de keuzes vast die de implementation guide veronderstelt maar niet motiveert, en die het Functioneel ontwerp generieke functie Lokalisatie niet noemt omdat ze technisch zijn. Normatieve uitwerking hoort in de IG; juridische beschouwing hoort in een eigen document.

Het TO herhaalt geen use cases, geen functionele requirements, geen profieldefinities en geen zoekparameters. Waar die nodig zijn voor het begrip, staat een verwijzing.

Het TO introduceert ook geen nieuwe begrippen. De begrippenlijst staat in het Functioneel ontwerp generieke functie Lokalisatie (Bijlage 2); de technische termen staan in de IG.

3.2 Scope en afbakening

3.2.1 Binnen scope

De lokalisatiefunctie omvat de keten van de vraag van de zorgverlener tot en met het tonen van het resultaat. Binnen dit document vallen:

- de Nationale Verwijsindex (NVI) als centrale dienst;
- de Pseudoniemenregistratieservice (PRS), voor zover de lokalisatiefunctie die gebruikt;
- de Localization Registration Client en de Localization Search Client als rollen bij de zorgaanbieder;
- de Custodian Server als rol bij de bronhoudende zorgaanbieder, voor zover die beslist over vermelding in het antwoord van de NVI.

3.2.2 Buiten scope

- Het opzoeken van endpoints. Dat is gedelegeerd aan de generieke functie Adressering.
- De inhoudelijke uitwisseling van medische gegevens: wat er precies wordt opgehaald en hoe dat wordt weergegeven.
- Identificatie en authenticatie van de zorgverlener.
- Het vaststellen van autorisatieregels. Het autoriseren van handelingen is belegd bij de generieke functie Autorisatie, zie 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie. Wanneer de regels bepaald zijn zullen die, waar nodig, toegepast worden op de lokalisatiecomponenten.

4 Systeemoverzicht

Dit hoofdstuk beschrijft de lokalisatiefunctie op systeemniveau, in drie stappen die steeds een niveau lager gaan:

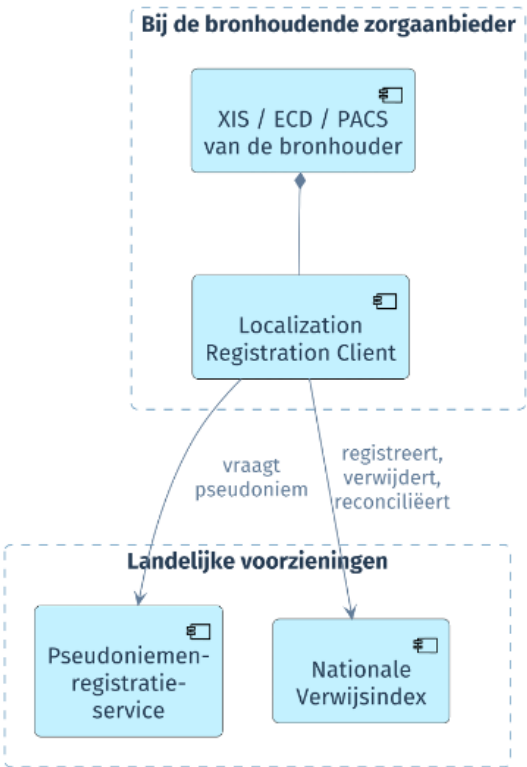
- welke systemen er zijn en hoe zij samenhangen;
- hoe de verantwoordelijkheden tussen centraal en decentraal zijn verdeeld; en
- waar een aansluitende partij op aansluit.

Verder dan dat gaat het niet. Hoe de betrokken systemen intern zijn opgebouwd, staat in hun eigen technische ontwerpen; dit document beschrijft wat zij aan de buitenkant bieden en waar ze qua technische eisen aan moeten voldoen. Gedetailleerde technische details staan in de IG.

4.1 Componentlandschap

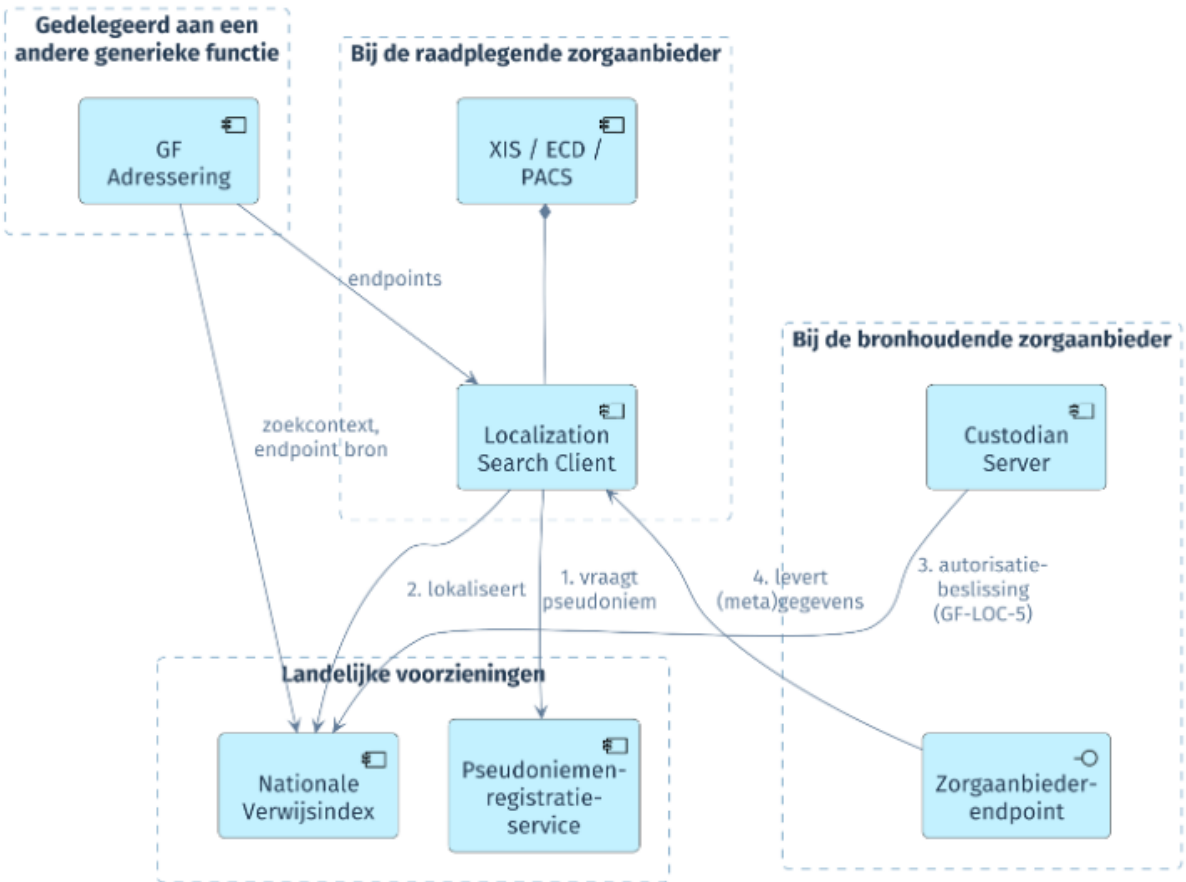
Onderstaande diagrammen tonen de volledige keten in twee delen. Het eerste diagram toont het registreren door de Localization Registration Client van de bronhouder. Het tweede toont het zoeken en raadplegen door de Localization Search Client, met de stappen in volgorde. Centraal staan in beide de NVI en de PRS. Waar in de keten geautoriseerd wordt, staat in 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie.

Systeemlandschap GF Lokalisatie: registreren



128
129

Systeemlandschap GF Lokalisatie: zoeken en raadplegen



130
131

Hieronder per component de verantwoordelijkheid en de reden dat het een eigen component is. De interne werking staat in de technische ontwerpen van de betrokken systemen.

4.1.1 Nationale Verwijsindex (NVI)

Verantwoordelijkheid: De NVI beheert de lokalisatie-records: registreren, verwijderen, doorzoeken en het teruggeven van de eigen registraties van een zorgaanbieder. Zij vraagt bij elke gevonden Datahoudende Zorgaanbieder een autorisatiebeslissing op. Zij houdt een index en geen inhoud.

Onderbouwing voor component: De index moet één logisch en consistent geheel zijn. Voor de achterliggende weging in voor en nadelen mbt de keuze voor deze inrichting zie 5.2.1.1 Een centrale index in plaats van een broadcast.

Implementatie: Centraal, één implementatie

4.1.2 Pseudoniemenregistratieservice (PRS)

Verantwoordelijkheid: De PRS leidt uit een (geblindeerd) BSN een ontvanger-specifiek (NVI) pseudoniem af. [Blindering](#) is een techniek waarmee de PRS wel een vertaling kan doen maar zelf niet weet op welke gegevens het werkt.

Onderbouwing voor component: Als de NVI dit zelf zou doen, dan heeft de NVI ook de sleutels om de pseudoniemen te maken. De scheiding is een essentieel onderdeel van de bescherming: gescheiden sleutels zorgen ervoor dat er geen BSN-naar-pseudoniem tabel gemaakt kan worden. Zie 5.2.2.1 Pseudonimisering door een aparte dienst.

Implementatie: Centraal, één implementatie, eigen ontwerp en beheer

De PRS is binnen dit document alleen beschreven voor zover de lokalisatiefunctie haar gebruikt.

4.1.3 Localization Registration Client

Verantwoordelijkheid: De Localization Registration Client registreert en verwijdert namens de bronhouder de lokalisatie-records bij de NVI, en houdt ze actueel. De Localization Registration Client vraagt het pseudoniem op bij de PRS. In dit document is Localization Client de verzamelterm voor Localization Registration Client en Localization Search Client.

Onderbouwing voor component: De keten vraagt bij de Datahoudende Zorgaanbieder een coördinatiepunt dat verschillende partijen aanroept. Dat punt kan niet bij de NVI liggen, want dan zou de NVI het BSN nodig hebben om het pseudoniem op te vragen, en dat is precies wat het ontwerp uitsluit.

Implementatie: Decentraal, twee rollen en geen product

Rol, geen product: Een XIS of een gedeelde voorziening van een leverancier kan deze rol vervullen. Eén partij kan de rol voor meerdere zorgaanbieders vervullen, en een zorgaanbieder kan meerdere clients hebben, bijvoorbeeld per bronsysteem. De diagrammen in dit document tonen een voorbeeldinvulling en geen beperking.

De Localization Registration Client is de plek waar de implementatielast van de functie neerslaat: het OPRF-protocol, de coördinatie van de aanroepen, en de foutafhandeling wanneer een daarvan mislukt.

4.1.4 Localization Search Client

Verantwoordelijkheid: De Localization Search Client stelt namens de Bevragende Zorgaanbieder vast of de vraag mag worden gesteld, en bevestigt de NVI. De Localization Search Client vraagt het pseudoniem op bij de PRS. In dit document is Localization Client de verzamelterm voor Localization Registration Client en Localization Search Client.

Onderbouwing voor component: De keten vraagt bij de Bevragende Zorgaanbieder een coördinatiepunt dat verschillende partijen aanroept. Dat punt kan niet bij de NVI liggen, want dan zou de NVI het BSN nodig hebben om het pseudoniem op te vragen, en dat is precies wat het ontwerp uitsluit.

Implementatie: Decentraal, twee rollen en geen product

Rol, geen product: Een XIS of een gedeelde voorziening van een leverancier kan deze rol vervullen. Eén partij kan de rol voor meerdere zorgaanbieders vervullen, en een zorgaanbieder kan meerdere clients hebben, bijvoorbeeld per bronsysteem. De diagrammen in dit document tonen een voorbeeldinvulling en geen beperking.

De Localization Search Client is de plek waar de implementatielast van de functie neerslaat: het OPRF-protocol, de coördinatie van de aanroepen, en de foutafhandeling wanneer een daarvan mislukt.

Ook het eerste autorisatiepunt: De vraag of deze zorgverlener voor deze patiënt mag lokaliseren, wordt in de Localization Search Client beantwoord: dit is het enige punt in de keten waar de zorgverlener en de patiënt tegelijk bekend zijn, en het ligt vóór de pseudonimisering. De regels daarvoor komen van de generieke functie Autorisatie, zie 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie; de client wint de beslissing in en dwingt haar af. Dat maakt de Localization Search Client meer dan een technisch koppelstuk. De NVI kent de patiënt niet en kan deze toets dus niet overnemen. De bronhouder beoordeelt later in de keten wel of zij in het antwoord wil worden vermeld, zie 4.1.5 Custodian Server.

4.1.5 Custodian Server

Verantwoordelijkheid: De Custodian Server geeft namens de bronhouder een autorisatiebeslissing. De NVI vraagt die beslissing op voor elke Datahoudende Zorgaanbieder die bij een zoekvraag gevonden wordt. Daarmee bepaalt de Datahoudende Zorgaanbieder of de Bevragende Zorgaanbieder mag weten dat zij gegevens heeft die bij de vraag passen.

Onderbouwing voor component: Alleen de Datahoudende Zorgaanbieder kent haar eigen beleid en de wensen van de patiënt. De NVI kent de patiënt niet en kan die afweging dus niet maken. Zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord.

Implementatie: Decentraal, een rol en geen product. De rol gebruikt de bestaande FHIR-API van de Datahoudende Zorgaanbieder.

4.2 Centraal en decentraal

Binnen de generieke functie Lokalisatie zijn er zowel centrale componenten (NVI, PRS) als decentrale componenten (Localization Registration Client, Localization Search Client, Custodian Server, zorgaanbieder-endpoint). Onderstaande tabel geeft per kant welke onderdelen dat zijn, wie ze beheert en welke gegevens zij beschikbaar stellen.

	Centraal	Decentraal
--	----------	------------

Wat	NVI, PRS	Localization Registration Client, Localization Search Client, Custodian Server, zorgaanbieder-endpoint
Beheer	landelijke beheerorganisatie	zorgaanbieder of diens leverancier
Verstrekt gegevens	gegevensbeschikbaarheid bij de bron	medisch-inhoudelijke gegevens

Toegang is in deze tabel bewust geen kolom. Het autoriseren van handelingen is niet belegd bij de centrale of de decentrale kant maar bij de generieke functie Autorisatie, op alle drie de punten waar dat in de keten aan de orde is. Zie 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie.

4.3 Koppelvlakken

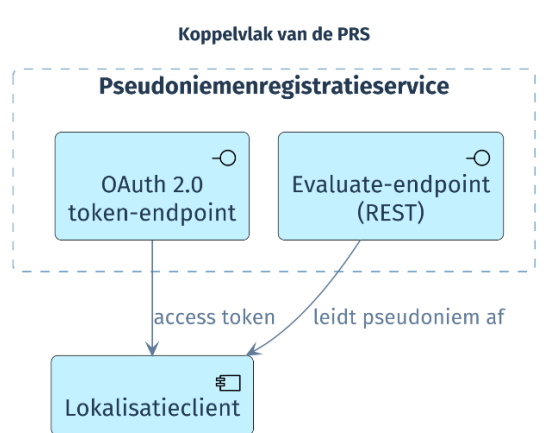
De vorige paragrafen beschreven welke partijen en systemen er in de keten zitten. Deze paragraaf beschrijft waar een Localization Client op aansluit en welk koppelvlak een Custodian Server aanbiedt, want dat bepaalt wat een aansluitende partij moet bouwen.

De Localization Client praat met drie systeemrollen. Alle drie schermen hun koppelvlak af met OAuth 2.0, en elke rol heeft daarnaast een eigen koppelvlak voor de inhoudelijke gegevens.

Elk van de drie systeemrollen voert daarnaast zijn eigen toegangscontrole uit. Bij de NVI en de bronhouder is dat het autoriseren van de vraag zelf. De Datahoudende Zorgaanbieder beslist daarnaast via de Custodian Server of zij in het antwoord van de NVI vermeld wordt, zie 4.3.3 Custodian Server. De regels voor die autorisatie zijn belegd bij de generieke functie Autorisatie en nog niet ingevuld; in de diagrammen hieronder staan zij daarom als losstaand blok. Zie 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie.

Een derde toets valt buiten deze paragraaf omdat er geen koppelvlak bij hoort: de vraag of deze zorgverlener voor deze patiënt mag lokaliseren. Die wordt bij de Bevragende Zorgaanbieder zelf beantwoord, voordat er via de lokalisatiefunctie een vraag wordt gesteld. Ook die regels komen van de generieke functie Autorisatie. Zie 4.1.3 Localization Registration Client en 4.1.4 Localization Search Client.

4.3.1 Pseudoniemenregistratieservice

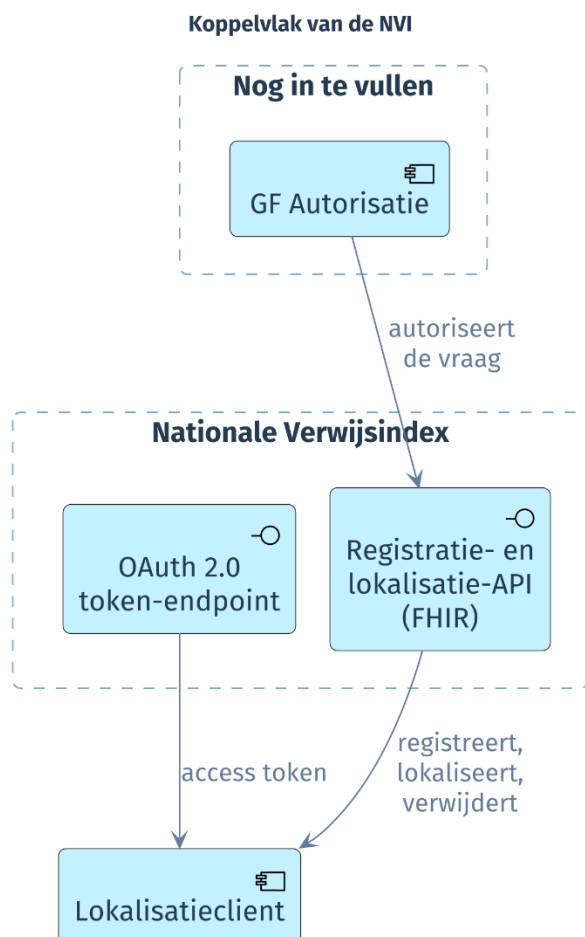


De PRS heeft binnen de generieke functie Lokalisatie één taak: het afleiden van een pseudoniem uit een geblindeerde invoer. Die invoer is de patiëntidentificatie (BSN). Het pseudoniem geldt voor één

ontvanger, zie 5.2.2.3 Pseudoniemen per ontvanger. Een client doet één aanvraag per registratie of zoekvraag.

Dit is een REST-koppelvlak. Via de PRS wordt geen zorginhoudelijke resource uitgewisseld: de invoer is een geblindeerde waarde en de uitkomst een versleuteld resultaat. Ook heeft de PRS een breder doel dan de primaire zorg.

4.3.2 Nationale Verwijsindex



Het functionele koppelvlak voor registreren, lokaliseren, verwijderen en het raadplegen van eigen registraties, aangeboden als FHIR R4. De transacties staan in hoofdstuk 7, de normatieve uitwerking in de IG. De NVI is daarnaast zelf afnemer: zij vraagt bij elke gevonden Datahoudende Zorgaanbieder een autorisatiebeslissing op bij de Custodian Server.

Het OAuth-endpoint is een aparte dienst. Zie 5.2.5.1 OAuth 2.0 met centrale clientregistratie voor toegang tot het koppelvlak.

4.3.3 Custodian Server

De Custodian Server biedt geen nieuw koppelvlak aan. De NVI stuurt HEAD-verzoeken naar de bestaande FHIR-API van de Datahoudende Zorgaanbieder, met de lokale patiënt-ID die de Datahoudende Zorgaanbieder bij registratie heeft opgegeven. De Datahoudende Zorgaanbieder antwoordt met "toestaan" of "weigeren". De NVI vindt de FHIR-API via de generieke functie Adressering. Zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord en 8.1 Generieke functie Adressering.

Bij deze aanroep is de NVI de afnemer. Zij authenticceert zich bij de Datahoudende Zorgaanbieder volgens de generieke functie Authenticatie.

4.3.4 Wat hieruit volgt voor een aansluitende partij

Elke Localization Client moet twee keer authenticeren en twee koppelvlakken ondersteunen, waarvan één FHIR en één REST. Zie 4.1.3 Localization Registration Client en 4.1.4 Localization Search Client. Een bronhouder biedt daarnaast de Custodian Server aan op haar bestaande FHIR-API, zie 4.3.3 Custodian Server.

De OAuth-endpoints staan los van elkaar: een token voor de NVI geeft geen toegang tot de PRS. Dat volgt uit het uitgangspunt dat elke partij zelf beslist over toegang tot wat zij beheert. Wat lokalisatie afneemt van de generieke functies Identificatie en Authenticatie staat in hoofdstuk 8.

Wat een Localization Client moet bouwen voor autorisatie is nog niet bekend.

De koppelvlakken hierboven beschrijven de toegang tot de dienst, niet de autorisatie van de handeling. Zodra de generieke functie Autorisatie kaders stelt, komt daar aan de kant van de NVI en de bronhouder iets bij: mogelijk een tweede token, een claim in het bestaande token, of het meesturen van attributen.

Daarnaast komt er een taak bij die de Bevragende Zorgaanbieder raakt: het vaststellen, vóór de vraag, of deze zorgverlener voor deze patiënt mag lokaliseren. Zie 4.1.3 Localization Registration Client en 4.1.4 Localization Search Client. Ook de vorm daarvan hangt af van de kaders die de generieke functie Autorisatie stelt.

Wat precies, is niet te zeggen voordat die kaders er zijn. Zie 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie.

5 Architectuurprincipes en -keuzes

5.1 Architectuurprincipes

Een principe is een leidende regel die aan meerdere keuzes ten grondslag ligt. Waar een keuze een besluit is over een concreet punt, is een principe de norm waaraan die besluiten zijn getoetst.

5.1.1 Onderwerp pseudonimisering en gegevensminimalisatie

5.1.1.1 De generieke functie lokalisatie borgt gegevensbeveiliging door technische maatregelen

De lokalisatiefunctie gaat over gevoelige informatie: behandelrelaties, ook voormalige, en gegevens over welk type zorg iemand heeft gehad. Een datalek heeft daarmee directe persoonlijke gevolgen voor betrokkenen.

De betrokken componenten worden daarom zo ontworpen dat zij, waar mogelijk, technische maatregelen treffen die de impact van een datalek beperken of voorkomen dat er nieuwe risico's ontstaan. Organisatorische waarborgen zijn daarbij aanvullend en niet vervangend.

Dit principe werkt door in de keuzes over pseudonimisering (5.2.2.1 Pseudonimisering door een aparte dienst tot en met 5.2.2.5 Antwoord zonder identificerende gegevens).

5.1.1.2 De NVI kent het BSN niet

Het BSN komt niet voor in het berichtenverkeer met de NVI en niet in haar opslag. Wat de NVI ontvangt is een pseudoniem dat buiten de NVI is afgeleid; wat zij bewaart is een hash daarvan.

Dit is geen afspraak maar een eigenschap van het ontwerp: de NVI kan het BSN niet zien, ook niet bij een fout of bij misbruik van de eigen toegang. Dat onderscheid is de reden dat de omzetting bij een aparte dienst ligt en niet bij de NVI zelf.

Zie de keuzes 5.2.2.1 Pseudonimisering door een aparte dienst tot en met 5.2.2.4 Hashing en versleuteling via een HSM en de verdieping in 6.1 Verdieping: pseudonimisering.

5.1.1.3 Zo min mogelijk gegevens, zo grof mogelijk

De lokalisatiefunctie legt alleen vast wat nodig is om de vraag te beantwoorden welke bronhouder gegevens heeft. Een registratie zegt alleen dát een zorgaanbieder gegevens over de patiënt heeft, niet welk type. Filteren gebeurt bij het zoeken, op kenmerken van de bronhouder: de zoekcontext.

Waar een gegeven wel nodig is, wordt de grofste vorm gekozen die nog werkt. Een fijnmazige indeling zegt meer over een persoon dan een grove, ook zonder dat die persoon bij naam bekend is.

De prijs hiervan is aanvaard: doordat de NVI minder weet, bevraagt een Bevragende Zorgaanbieder mogelijk bronnen die voor deze patiënt niet relevant blijken. Dat weegt op tegen het alternatief, waarin de NVI precies zou weten welke bronnen relevant zijn en daarmee een gedetailleerder beeld van de patiënt zou bevatten.

Zie de keuzes 5.2.1.2 Alleen de lijst bronhouders in het antwoord en 5.2.2.5 Antwoord zonder identificerende gegevens. Zie ook 5.2.1.4 Zoekcontext op kenmerken van de bronhouder. De codelijsten voor de zoekcontext staan in de IG.

5.1.2 Onderwerp beveiliging en vertrouwen

5.1.2.1 Lokaliseren is niet autoriseren

De generieke functie lokalisatie doet geen uitspraak over wie welke gegevens mag inzien. Zij beantwoordt de vraag welke bronhouders gegevens hebben; of die gegevens vervolgens worden verstrekt, beslist de bronhouder.

5.1.3 Onderwerp Interoperabiliteit en standaarden

5.1.3.1 Internationale standaarden, tenzij

De lokalisatiefunctie gebruikt breed geadopteerde internationale standaarden, om interoperabiliteit te bevorderen, leveranciersonafhankelijkheid te borgen en aansluiting op bestaande implementaties mogelijk te maken.

Afwijken van een standaard vraagt een expliciete motivering.

5.2 Architectuurkeuzes

Elke keuze volgt dezelfde opbouw: context, besluit, rationale, afgewezen alternatieven en consequenties. Waar de afweging te lang is voor de hoofdttekst, staat de uitwerking in appendix A.

5.2.1 Onderwerp lokaliseren en vervolgstappen

5.2.1.1 Een centrale index in plaats van een broadcast

Context

De vraag die de lokalisatiefunctie beantwoordt is: welke bronnen hebben gegevens over deze patiënt? Zonder centrale voorziening is er één manier om die vraag te beantwoorden, namelijk hem aan alle mogelijke bronnen stellen: een broadcast. Elke potentiële bronhouder krijgt dan de vraag en antwoordt of hij gegevens heeft.

Besluit

De lokalisatiefunctie gebruikt een centrale index, de NVI, waarin bronhouders vooraf registreren dat zij gegevens hebben. De Bevragende Zorgaanbieder stelt zijn vraag aan die index en niet aan de bronnen.

Rationale

Een broadcast heeft drie problemen:

Het lekt de behandelrelatie

Een broadcast stelt de vraag “heeft u gegevens over deze patiënt” aan iedere aangesloten zorgaanbieder, ook aan de partijen die geen behandelrelatie met deze patiënt hebben of ooit hadden. Die partijen leren daarmee twee dingen die hen niet aangaan: dat deze patiënt bestaat, en dat de vragende zorgaanbieder een behandelrelatie met hem heeft. Bij een landelijke uitrol betekent dat: bij elke vraag over elke patiënt worden alle zorgaanbieders (meer dan zesduizend) geïnformeerd over een behandelrelatie waar zij buiten staan. Een centrale index draait dit om: alleen de bronhouders die zelf hebben aangegeven gegevens te hebben, worden bevraagd.

Performance

Het antwoord op de vraag bij een broadcast is pas compleet als alle bronnen hebben geantwoord. De traagste Datahoudende Zorgaanbieder bepaalt de wachttijd van de zorgverlener.

In het geval van een centrale index is het enkel de snelheid van de index die bepalend is voor de eerste selectie binnen de generieke functie lokalisatie.

Beschikbaarheid

Bij een broadcast is elke Datahoudende Zorgaanbieder een schakel in de keten. Is een Datahoudende Zorgaanbieder niet bereikbaar, dan is onbekend of hij gegevens had, en is het antwoord dus onvolledig zonder dat zichtbaar is wat ontbreekt.

In de opzet met een centrale index is er wel een afhankelijkheid van een centrale component. Dit is dan een SPoF, maar de beschikbaarheid van het totale systeem is hoger dan wanneer alle bronnen worden gecombineerd in de beschikbaarheidsberekening.

Afgewezen alternatieven

Broadcast naar alle bronnen.

Afgewezen op bovenstaande gronden, waarbij het lekken van de behandelrelatie zwaarder weegt dan de technische bezwaren: dat is een structureel privacyprobleem en geen schaalprobleem dat met techniek is op te lossen.

Broadcast met voorselectie, bijvoorbeeld op regio of op zorgaanbiedertype.

Dit verkleint de eerder genoemde problemen met broadcast maar mitigeert deze niet volledig.

Consequenties

- Bronhouders moeten registreren. De functie werkt alleen als registratie systematisch gebeurt; een Datahoudende Zorgaanbieder die niet registreert is onvindbaar. Zie 5.2.3.6 Registreren bij de gebeurtenis, reconciliëren als vangnet.
- De index bevat het gegeven wie waar onder behandeling (geweest) is. Dit is de aanleiding voor de pseudonimisering, zie 6.1 Verdieping: pseudonimisering.
- De centrale index is een beschikbaarheidsafhankelijkheid voor de hele keten.

5.2.1.2 Alleen de lijst bronhouders in het antwoord

Context

Een antwoord op een lokalisatievraag kan meer zeggen dan wie gegevens heeft: bijvoorbeeld hoeveel registraties er zijn, wanneer ze zijn gedaan, of om welke datacategorieën het precies gaat.

Besluit

Het antwoord op een lokalisatievraag bevat enkel de lijst bronhouders met de bijbehorende zorgaanbieder-identificer (URA). Het bevat geen andere (inhoudelijke) gegevens. Een Datahoudende Zorgaanbieder staat alleen in het antwoord als haar Custodian Server de vermelding toestaat, zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord.

Rationale

Elk extra veld in het antwoord is een uitspraak die de NVI doet over de patiënt.

Die informatie is voor het doel van de functie niet nodig: de Bevragede Zorgaanbieder moet weten welke Datahoudende Zorgaanbieders hij moet bevragen, en de rest haalt hij bij de Datahoudende Zorgaanbieder op, die daarover kan beslissen. Het pseudoniem, de lokale patiënt-ID en de registrerende client worden actief uit het antwoord verwijderd. Zie 5.2.2.5 Antwoord zonder identificerende gegevens.

Consequenties

- De Bevragede Zorgaanbieder kan uit het antwoord niet afleiden hoeveel gegevens er zijn, alleen bij wie ze zijn.
- Het ontbreken van een Datahoudende Zorgaanbieder in het antwoord is geen bewijs dat er geen gegevens zijn. De Datahoudende Zorgaanbieder kan ontbreken omdat zij niet registreerde, de vermelding weigerde of niet op tijd antwoordde. Dat is een eigenschap van de functie en moet in de gebruikersinterface duidelijk zijn; zie Functioneel ontwerp generieke functie Lokalisatie, deel B, hoofdstuk 12.

5.2.1.3 FHIR search voor lokalisatie**Context**

Voor het bevragen van de NVI is een koppelveld nodig. Dat kan een eigen operatie zijn die precies doet wat de lokalisatiefunctie vraagt, of een standaard FHIR-search op de resource waarin de records zijn vastgelegd.

Besluit

Lokalisatie gebruikt standaard FHIR search op Patient-resources (POST [base]/Patient/_search). De Localization Search Client zoekt op het pseudoniem en kan dat combineren met standaard geketende zoekparameters op de bron: URA, type zorgaanbieder, het type gegevens dat een endpoint aanbiedt en het zorgaanbod. De NVI zet die parameters om met haar kopie van de gegevens uit de generieke functie Adressering. Waarom de zoekcontext op kenmerken van de bronhouder werkt en niet op de data, staat in 5.2.1.4 Zoekcontext op kenmerken van de bronhouder.

Rationale

Standaard FHIR-zoekparameters en ketens worden breed ondersteund. Er is geen eigen semantiek, waardoor generieke FHIR-tooling en client-bibliotheken bruikbaar zijn. De zoekcontext gebruikt dezelfde gegevens als de generieke functie Adressering, zodat er één bron is voor de kenmerken van zorgaanbieders. Zoeken gaat via POST, zodat het pseudoniem en de zoekcontext niet in URL's en toegangslogs terechtkomen.

Een eigen operatie levert een iets eenvoudiger aanroep op. Dat weegt niet op tegen het verlies aan tooling-ondersteuning en tegen de afwijking van de standaard.

Afgewezen alternatieven

Eigen operatie Organization/\$localize.

Afgewezen: de eenvoud van de aanroep weegt niet op tegen het verlies aan standaardconformiteit en tooling-ondersteuning.

Zoeken volgens IHE MHD (ITI-66, Find Document Lists).

Afgewezen: MHD is bedoeld voor het vinden van documenten en gaat uit van een patiëntidentificatie die de server kan interpreteren. De NVI kent alleen een pseudoniem en bevat geen documenten. Zie ook 5.2.3.1 Patient als drager van het lokalisatie-record.

Consequenties

Localization Search Clients kunnen generieke FHIR-tooling gebruiken.

De zoekparameters liggen vast in de implementation guide en niet in dit document.

5.2.1.4 Zoekcontext op kenmerken van de bronhouder

Context

Een zorgverlener zoekt zelden naar alle bronnen van een patiënt. Meestal gaat het om bronnen die passen bij een zorgvraag, bijvoorbeeld medicatie of beeldvorming. Die afbakening heet de zoekcontext.

In een eerder ontwerp kreeg elke registratie een datacategorie, en filterde de NVI op de data zelf. Dat bleek om drie redenen niet werkbaar:

- Zorgdata laat zich moeilijk in vaste categorieën indelen.
- In veel gebruikssituaties was de vraag toch: geef alle gegevens van deze patiënt.
- Een nieuwe of gewijzigde categorie vraagt een software-update bij alle leveranciers. Zo'n migratie duurt maanden tot jaren.

Besluit

De NVI filtert op kenmerken van de bronhouder, niet op de inhoud van de data. Voorbeelden van kenmerken zijn de URA, het type zorgaanbieder, de datacategorieën die een endpoint aanbiedt en de zorgdiensten die de zorgaanbieder aanbiedt. De zorgaanbieder publiceert die kenmerken via de generieke functie Adressering. Een registratie in de NVI zegt alleen dat de bronhouder gegevens over de patiënt heeft.

Rationale

Een wijziging in de indeling werkt direct zodra zorgaanbieders hun kenmerken in Adressering bijwerken. Registraties en de software van bronhouders hoeven daarvoor niet te veranderen.

Er is nog maar één soort registratie: de patiënt is bekend bij de bronhouder. Dat beperkt profielvorming in de NVI, zie 5.2.2.3 Pseudoniemen per ontvanger.

Het ontwerp remt te breed zoeken af. Een Bevragende Zorgaanbieder die te breed zoekt, laat aan meer bronhouders zien dat zij een behandelrelatie met de patiënt heeft. Misbruik is achteraf vast te stellen via de logging, zie 5.2.5.4 Gescheiden logging voor SOC en burgerinzage. De Tuchtraad en de IGJ kunnen dan optreden.

Wat een zorgaanbieder zegt aan te bieden, is openbaar in Adressering. Een zorgaanbieder die zich ten onrechte breed profileert, valt daardoor op.

Afgewezen alternatieven

Een datacategorie per registratie.

Afgewezen om de redenen onder Context.

De zoekcontext omzetten bij de Bevragende Zorgaanbieder.

De Localization Search Client zet de zoekcontext via de generieke functie Adressering zelf om naar een lijst URA's, en stuurt die lijst naar de NVI. Het voordeel is dat lokalisatie en Adressering losser gekoppeld zijn, en dat de logs van de NVI minder over de zorgvraag zeggen. Het nadeel is dat bij een brede zoekcontext lange lijsten URA's naar de NVI gaan, en dat de logging voor burgerinzage lastiger wordt. Dit alternatief is nu niet gekozen en wordt meegenomen in de consultatie.

Een tijdsfilter in de zoekvraag.

De Bevragende Zorgaanbieder geeft een periode mee, zodat bronnen met alleen oude gegevens niet worden bevroegd. Dit kan ook bij het ophalen van de gegevens. Of een filter in de zoekvraag meerwaarde heeft, wordt nog onderzocht.

Consequenties

- Een bronhouder die aan de zoekcontext voldoet maar geen passende gegevens over deze patiënt heeft, kan toch in het antwoord staan. Dat is aanvaard. Bevat de zoekcontext een datacategorie, dan kan de Custodian Server dit afvangen, zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord.
- De NVI heeft een actuele kopie van de gegevens van Adressering nodig, zie 8.1 Generieke functie Adressering.
- Openstaand. Het is nog niet duidelijk of het zorgdiensttype voor lokalisatie hetzelfde kan zijn als de HealthcareService in Adressering. Bij Adressering gaat het eerder om de zorgvraag, bij lokalisatie om wat een zorgaanbieder aanbiedt. Dit wordt onderzocht in de consultatie en de praktijkbeproeving.
- Openstaand. De minimale specificiteit van een zoekcontext ligt nog niet vast.

5.2.2 Onderwerp Pseudonimisering en gegevensminimalisatie

5.2.2.1 Pseudonimisering door een aparte dienst

Context

Als informatiebeveiligingsmaatregel is gekozen om te zorgen dat de NVI niet over het BSN kan beschikken. Er is dus een omzetting nodig van BSN naar pseudoniem. De vraag is welke partij die omzetting uitvoert.

Twee partijen liggen voor de hand: de NVI zelf, of een aparte dienst. De Localization Client valt af als enige uitvoerder: pseudoniemen moeten bij elke registratie- en lokalisatievraag consistent zijn ongeacht de bron, anders vindt een Bevragende Zorgaanbieder de registraties van een Datahoudende Zorgaanbieder niet terug. De pseudoniemen mogen (en moeten in dit geval) wel uniek zijn voor de NVI. Zo zijn ze buiten de NVI niet direct aan een persoon te koppelen. Dit is ook de reden dat een zorgaanbieder zelf het pseudoniem niet mag kennen. Anders zouden zorgaanbieders bij een datalek de koppeling met het BSN kunnen maken.

Besluit

De omzetting wordt uitgevoerd door een aparte dienst, de Pseudoniemenregistratieservice (PRS). De NVI voert zelf geen pseudonimisering op basis van het BSN uit en ontvangt een reeds afgeleid pseudoniem.

Rationale

Zou de NVI de omzetting zelf doen, dan moet zij het BSN ontvangen om het te kunnen omzetten. Daarmee vervalt het uitgangspunt: de maatregel is dan een interne verwerkingsstap en geen eigenschap van het systeem. Wie toegang heeft tot de NVI op het moment van verwerking, ziet het BSN.

Een aparte dienst maakt de scheiding structureel in plaats van procedureel. De NVI kán het BSN niet zien, ook niet bij een fout of bij misbruik van de eigen toegang.

Die scheiding is nog meer effectief als zij ook organisatorisch bestaat. Worden beide door dezelfde partij beheerd met hetzelfde sleutelbeheer, dan zijn er restrisico's: zie 6.1 Verdieping: pseudonimisering.

Afgewezen alternatieven

Pseudonimisering in de NVI zelf.

Afgewezen: de NVI verwerkt dan alsnog het BSN in leesbare vorm, wat het uitgangspunt onderuit haalt.

Pseudonimisering uitsluitend bij de Localization Client.

Afgewezen: betekent dat alle zorgaanbieders kunnen de-pseudonimiseren.

Consequenties

- De NVI beschikt structureel niet over het BSN, niet in opslag en niet in verwerking.
- Afhankelijkheid van een externe dienst voor elke registratie en elke lokalisatievraag. Dit is de sterkste afhankelijkheid in de keten, zie hoofdstuk 8.
- De PRS heeft een eigen ontwerp, eigen beheer en eigen sleutelbeheer, gescheiden van de NVI. Zie 4.1.2 Pseudoniemenregistratieservice (PRS).
- Er is een extra aanroep nodig vóór elke registratie en elke lokalisatievraag.

5.2.2.2 Blinding via OPRF**Context**

Met de omzetting bij een aparte dienst is het probleem van BSN kennis bij een centraal systeem verplaatst, niet opgelost. Een dienst die het BSN ontvangt om er een pseudoniem van te maken, ziet dat BSN. En omdat de aanvrager een zorgaanbieder is, ziet die dienst ook de behandelrelatie.

Daarmee is de PRS qua informatiebeveiliging net zo belangrijk geworden als de NVI zou zijn geweest zonder pseudonimisering, met als verschil dat het probleem nu bij een andere partij ligt.

Besluit

De Localization Client blindeert de patiëntidentificatie voordat hij die naar de PRS stuurt. De PRS rekent met een Oblivious Pseudo-Random Function (OPRF) op de geblindeerde waarde en kent de oorspronkelijke waarde niet. Na de-blinderen (in de NVI) blijft dan het pseudoniem over.

Wat blinding is

Een pseudoniem kan gezien worden als een transformatie van een invoerwaarde (BSN) naar een nieuwe waarde (het pseudoniem) met gebruik van een geheime sleutel zodat iemand die enkel het pseudoniem heeft niet weet welke invoer waarde gebruikt is.

De PRS en NVI passen dit toe doordat bij de PRS een geheime sleutel is die enkel voor de NVI gebruikt wordt. Wat blinding toevoegt is een extra stap voor en na de pseudonisatie. Dit zorgt ervoor dat de transformatie met de NVI-sleutel gebeurt op geblindeerde data. Dat zorgt dat de PRS ook niet weet wat de invoerwaarde is.

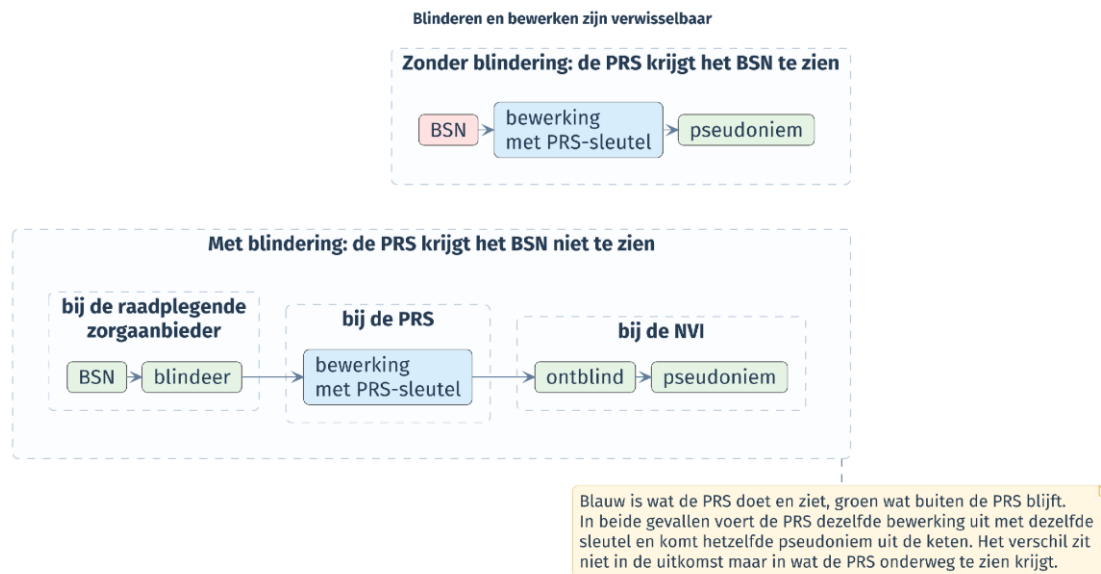
De onderstaande beschrijving is een vereenvoudiging van hoe blinding werkt: zij geeft de eigenschappen weer die het ontwerp draagt, niet de bewerking zelf. De werkelijke constructie is een OPRF conform RFC 9497, suite OPRF(ristretto255, SHA-512), waarin op punten van een elliptische kromme wordt gerekend en niet op getallen. Voor de normatieve uitwerking gelden de implementation guide en het technisch ontwerp van de PRS.

Vereenvoudigd weergegeven: de Localization Client blindeert de invoer door haar te combineren met een geheim dat hij zelf kiest en lokaal houdt, de blinderingsfactor. Wat de PRS ontvangt is voor haar niet te onderscheiden van een willekeurige waarde: zonder de factor is er geen manier om er de oorspronkelijke invoer uit te halen. Elke aanvraag gebruikt een nieuwe factor, dus twee aanvragen voor dezelfde patiënt leveren twee verschillende geblindeerde waarden op.

Wat de bewerking bijzonder maakt.

De blinding laat zich ná de berekening van de PRS weer opheffen. De PRS rekent met haar eigen sleutel op de geblindeerde waarde; wie daarna de blinderingsfactor kent, ontblindt het resultaat en houdt precies de uitkomst over die zou zijn ontstaan als de PRS op de onbewerkte invoer had gerekend. Blinderen en rekenen zijn in die zin verwisselbaar: voor de uitkomst maakt de volgorde niet uit, voor wat de PRS onderweg ziet wel.

Dat is de eigenschap waar alles op steunt, en zij is niet vanzelfsprekend. Blinding is geen versleuteling: bij versleuteling zou de PRS eerst moeten ontsleutelen om te kunnen rekenen, en dan ziet zij de invoer alsnog. Hier hoeft dat niet, omdat de bewerking van de PRS door de blinding heen werkt.



In de bovenste keten zou het BSN de PRS bereiken. In de onderste blijft het bij de Bevragende Zorgaanbieder: daar wordt geblindeerd, en het ontblinden gebeurt pas bij de ontvanger. De PRS ziet daartussen alleen een geblindeerde waarde. De uitkomst is in beide gevallen hetzelfde pseudoniem.

De ontvanger is hier de NVI, omdat het diagram de lokalisatiefunctie beschrijft. Het mechanisme is niet aan de NVI gebonden: elke ontvanger met een geregistreerde sleutel kan die rol vervullen.

Wat dat oplevert.

Twee partijen dragen elk een deel van het geheim en geen van beide kan het geheel samenstellen. De PRS heeft de sleutel maar ziet de invoer niet; de Localization Client ziet de invoer maar heeft de sleutel niet. Het pseudoniem ontstaat pas als beide delen samenkomen, en dat gebeurt bij de ontvanger.

Waar het pseudoniem ontstaat.

Het ontblinden gebeurt niet bij de Localization Client maar bij de ontvanger, bijvoorbeeld de NVI. De PRS versleutelt haar resultaat voor die ontvanger; de Localization Client geeft dat versleutelde resultaat samen met de blinderingsfactor door zonder het te kunnen openen. De ontvanger ontsleutelt en ontblindt, en houdt het pseudoniem over.

Daarmee ziet ook de Localization Client het pseudoniem niet. Dat zorgt ervoor dat de zorgaanbieder geen kennis krijgt over de pseudoniemen in de NVI en die dus niet kan de-pseudonimiseren.

De cryptografische uitwerking staat in de implementation guide en het technisch ontwerp van de PRS. Dit document beschrijft alleen wat de constructie oplevert.

Rationale

Dit is de enige van de overwogen constructies waarbij geen enkele partij zowel het BSN als de behandelrelatie ziet. De NVI ziet een pseudoniem zonder BSN; de PRS ziet een geblindeerde waarde zonder te weten om welk BSN het gaat.

De uitkomst is dezelfde als wanneer de PRS het BSN zelf had verwerkt: dezelfde patiënt levert bij dezelfde ontvanger hetzelfde pseudoniem. Die eigenschap is nodig om registraties terug te vinden, en is precies wat een gewone versleuteling van het BSN niet biedt.

Er is voor OPRF gekozen omdat het een gestandaardiseerde primitief is, vastgelegd in RFC 9497. Voor een voorziening die twintig jaar mee moet en door een breed leveranciersveld wordt geïmplementeerd, weegt dat zwaar: een eigen constructie zou per implementatie opnieuw beoordeeld moeten worden, terwijl een RFC-primitief publiek is geanalyseerd en in volwassen bibliotheken beschikbaar is. Dat laatste is niet triviaal, omdat de blinding aan de clientkant moet gebeuren en dus door elke leverancier wordt geïmplementeerd.

De keuze is bovendien vervangbaar gemaakt. De gebruikte suite is geversioneerd, zodat overstappen naar een andere of zwaardere variant mogelijk blijft zonder het ontwerp te wijzigen. Dat is nodig omdat de primitief niet post-quantum-veilig is en er nog geen gestandaardiseerd alternatief bestaat; de mitigatie is dat de suite vervangen kan worden zodra dat er wel is.

De werking van het mechanisme staat in 6.1 Verdieping: pseudonimisering. De suitekeuze zelf, en de afwegingen daarbinnen, staan in het technisch ontwerp van de PRS.

Afgewezen alternatieven

Een pseudoniemendienst zonder blinding.

Afgewezen: die dienst verwerkt dan de combinatie zorgaanbieder plus BSN, en daarmee de behandelrelatie. Het probleem verplaatst dan van de NVI naar de PRS in plaats van te verdwijnen.

Versleuteld aanleveren van het BSN aan de PRS.

Afgewezen: de PRS moet het BSN ontsleutelen om ermee te kunnen rekenen, en ziet het dan alsnog. Transportbeveiliging lost het probleem van de ontvangende partij niet op.

Consequenties

- Data protection by design: NVI noch PRS beschikt over het BSN in combinatie met de behandelrelatie.
- Leveranciers moeten het OPRF-protocol implementeren in de Localization Client. Dit is de zwaarste implementatie-eis die de generieke functie Lokalisatie aan clients stelt, en de reden dat een Localization Client meer is dan een gewone API-client. Zie ook 4.1.3 Localization Registration Client en 4.1.4 Localization Search Client.
- Een fout in de blinderingsstap aan clientzijde levert een onbruikbaar pseudoniem op, niet een gelekt BSN. Het faalgedrag is daarmee veilig.

5.2.2.3 Pseudoniemen per ontvanger

Context

Een pseudoniem is bedoeld om een patiënt aanduidbaar te maken zonder hem identificeerbaar te maken. Dat lukt alleen als het pseudoniem niet als identificerend nummer gaat functioneren. Twee vormen van koppelbaarheid bedreigen dat.

Koppeling tussen partijen.

Als elke ontvanger hetzelfde pseudoniem voor dezelfde patiënt krijgt, kunnen partijen hun registraties naast elkaar leggen en zo alsnog een beeld opbouwen van waar een patiënt onder behandeling is.

Koppeling binnen de NVI. Als één pseudoniem alle registraties van een patiënt bij elkaar houdt, ontstaat binnen de NVI een profiel: bij dit nummer horen deze datacategorieën. De datacategorie is dan een eigenschap van een persoon geworden, ook al is die persoon niet bij naam bekend. Sommige categorieën zijn zo onderscheidend dat zij de groep mogelijke personen sterk verkleinen: een registratie voor verloskundige zorg sluit het grootste deel van de bevolking uit. Een tweede categorie erbij verkleint de groep verder. Zo kan een reeks registraties samen identificerend worden terwijl elke registratie afzonderlijk dat niet is.

Besluit

Het pseudoniem wordt afgeleid uit de combinatie van patiëntidentificatie en ontvanger. Dezelfde patiënt heeft daardoor bij elke ontvanger een ander pseudoniem. Binnen de NVI heeft een patiënt één pseudoniem. Het pseudoniem bepaalt over welke patiënt wordt gezocht. Het zegt niets over het type gegevens. Verdere filtering gebeurt via de zoekcontext en de beslissing van de Datahoudende Zorgaanbieder.

Rationale

De ontvanger-scoping voorkomt koppeling tussen partijen. Zonder die eigenschap zou een pseudoniem functioneren als een landelijk patiëntnummer, met dezelfde koppelbaarheid als het BSN maar zonder de waarborgen die daaromheen staan.

Profielvorming binnen de NVI wordt op een andere manier beperkt. De NVI legt geen datacategorie per registratie vast. Een registratie zegt alleen dat een Datahoudende Zorgaanbieder gegevens over de patiënt heeft, niet welk type. Er is dus één soort registratie. Een zoekvraag kan een datacategorie bevatten, als kenmerk van een endpoint in de zoekcontext. Die wordt niet bij de registratie bewaard.

Of een Datahoudende Zorgaanbieder gegevens van het gevraagde type heeft, bepaalt de Datahoudende Zorgaanbieder zelf. De NVI selecteert bronnen op de zoekcontext, bijvoorbeeld op het type gegevens dat een endpoint aanbiedt. De Custodian Server bevestigt per vraag of zij gegevens van dat type wil melden, zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord.

Een Datahoudende Zorgaanbieder registreert een patiënt daardoor één keer, ongeacht het aantal datacategorieën dat zij voor die patiënt heeft. Een nieuw type gegevens vraagt geen nieuwe registratie.

Wie de NVI-database leest, ziet per pseudoniem een lijst bronhouders, zonder datacategorieën. Zie 6.1 Verdieping: pseudonimisering voor wat dat bij een datalek betekent.

Afgewezen alternatieven

Een pseudoniem per patiënt, ontvanger en datacategorie.

Afgewezen: dit voorkomt dat de NVI registraties van verschillende datacategorieën aan elkaar kan koppelen. Het vraagt wel een PRS-aanvraag en een registratie per datacategorie per patiënt, en een zoekvraag per datacategorie. Een deel van de bescherming ontstaat al doordat de NVI geen datacategorie vastlegt. Wat overblijft, is de lijst bronhouders per pseudoniem; zie 6.1 Verdieping: pseudonimisering.

Consequenties

- Partijen kunnen registraties niet onderling koppelen.

- Binnen de NVI horen alle registraties van één patiënt bij hetzelfde pseudoniem. Er is geen datacategorie aan gekoppeld.
- Een Localization Client vraagt één pseudoniem op per registratie of zoekvraag, ongeacht het aantal datacategorieën.
- Een lokalisatievraag over meerdere datacategorieën is één zoekvraag.
- De omzetting tussen pseudoniemdomeinen ligt bij de PRS, wat de PRS tot een kritieke component maakt. Zie 6.1 Verdieping: pseudonimisering, restrisiko's.
- Verwijderen gebeurt per registratie, door de client die registreerde. Een verzoek vanuit de burger loopt via de zorgaanbieder, zie 8.4 Generieke functie Toestemming.

5.2.2.4 Hashing en versleuteling via een HSM

Context

De NVI slaat het pseudoniem op. Bij compromittering van de database zou dat pseudoniem direct bruikbaar zijn voor wie ook toegang heeft tot de pseudoniemsleutels van de PRS (rainbow table). Daarnaast slaat de NVI de lokale patiënt-ID van de Datahoudende Zorgaanbieder op. Die is nodig om de autorisatiebeslissing bij de Datahoudende Zorgaanbieder op te vragen, zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord.

Besluit

De NVI slaat niet het pseudoniem op maar een hash daarvan, berekend met een sleutel die in een Hardware Security Module (HSM) blijft. De lokale patiënt-ID slaat de NVI versleuteld op, met een sleutel die ook in de HSM blijft. Een hash kan hier niet, omdat de NVI de ID bij de Datahoudende Zorgaanbieder (bij bevraging van de Custodian Server) moet kunnen gebruiken.

Rationale

Dit voegt een extra laag toe bovenop de pseudoniemen zelf. Om van de opgeslagen gegevens terug te komen bij een BSN moeten drie stappen worden gezet: de PRS moet een opzoektabel van BSN naar pseudoniem opleveren, alle pseudoniemen moeten via de HSM-sleutel van de NVI naar hun hash worden vertaald, en pas dan zijn de NVI-gegevens te herleiden. Alle controls bij zowel de PRS als de NVI moeten daarvoor worden omzeild, inclusief het sleutelbeheer van de HSM.

Dit beperkt ook de schade van een insider: database-toegang alleen is niet voldoende.

Afgewezen alternatieven

Alleen Transparent Data Encryption.

Afgewezen: bij compromittering van de database zijn de pseudoniemen direct leesbaar en vervalt de tweede stap uit de aanvalsketen.

Versleuteling in de applicatielaag.

Afgewezen: sleutels in het geheugen van de applicatie zijn kwetsbaarder dan sleutels in een HSM.

Hashing zonder HSM.

Afgewezen: geen hardwarematige bescherming van de sleutel.

Consequenties

- Meerdere onafhankelijke compromitteringen zijn nodig om gegevens te herleiden.
- Extra complexiteit door de HSM-integratie en het bijbehorende sleutelbeheer.
- Prestatie-overhead per HSM-bewerking en kosten voor de hardware.

- Elke autorisatievraag aan een Datahoudende Zorgaanbieder vraagt een ontsleuteling via de HSM.

5.2.2.5 Antwoord zonder identificerende gegevens

Context

Een registratie bevat het pseudoniem, de lokale patiënt-ID van de Datahoudende Zorgaanbieder en de registrerende client. Die gegevens zijn nodig om te registreren, te zoeken en de Datahoudende Zorgaanbieder om een beslissing te vragen. Ze mogen niet terugkomen in het antwoord aan de Bevragende Zorgaanbieder.

Besluit

De NVI geeft in het antwoord een ingekorte weergave van de registratie terug. Die bevat alleen de bronhouder. Alle identifiers en de registrerende client zijn weggelaten. De weergave is gemarkeerd als onvolledig (FHIR-tag SUBSETTED). Er is één profiel voor de registratie en geen apart profiel voor het antwoord.

Rationale

Het weglaten is een eis aan de NVI, niet aan de client. De SUBSETTED-markering is de standaard FHIR-manier om aan te geven dat een resource bewust onvolledig is. Een client herkent daardoor dat hij de weergave niet als registratie mag gebruiken. Of de NVI de gegevens echt weglaat, wordt getoetst in de conformance-test van de NVI.

Afgewezen alternatieven

Een apart uitvoerprofiel waarin de identifiers verboden zijn.

Afgewezen: een FHIR-validator toetst een gemarkeerde, ingekorte resource niet tegen het profiel. Het extra profiel voegt daardoor weinig toetsbaarheid toe, en het is een tweede profiel om te onderhouden.

Consequenties

- Het pseudoniem, de lokale patiënt-ID en de registrerende client komen niet in antwoorden voor.
- De NVI moet deze gegevens actief weglaten voordat zij antwoordt.
- Een Bevragende Zorgaanbieder kan de weergave niet gebruiken om een registratie te wijzigen.

5.2.3 Onderwerp registreren en verwijderen

5.2.3.1 Patient als drager van het lokalisatie-record

Context

Een lokalisatie-record drukt uit: zorgaanbieder X heeft gegevens over patiënt Z. Daar is een FHIR-resource voor nodig. Er zijn meerdere kandidaten, waaronder een eigen resource.

Besluit

Het lokalisatie-record wordt vastgelegd als een FHIR Patient-resource: één Patient per patiënt, per bronhouder en per registrerende client. Het pseudoniem en de lokale patiënt-ID staan in Patient.identifier, de bronhouder in Patient.managingOrganization.

Rationale

Een Patient bij een zorgaanbieder drukt in FHIR precies uit wat het record zegt: deze zorgaanbieder kent deze patiënt. Via managingOrganization kan met standaard geketende zoekparameters op de

kenmerken van de bronhouder worden gezocht, zie 5.2.1.3 FHIR search voor lokalisatie. Er zijn geen extensies nodig, en de tooling-ondersteuning is breed.

Afgewezen alternatieven

Eigen resource NVIDataReference.

Afgewezen: semantisch helderder, maar buiten de standaard en daarmee zonder tooling-ondersteuning.

FHIR List volgens IHE MHD.

Afgewezen: MHD is bedoeld voor het vinden van documenten en gaat uit van een patiëntidentificatie die de server kan interpreteren. De NVI kent alleen een pseudoniem en registreert geen documenten. Een List vraagt daarom extensies en afwijkingen van MHD, waardoor de voordelen van MHD grotendeels vervallen.

Consequenties

- Standaard FHIR-resource met Nederlandse profilering.
- Zoeken op kenmerken van de bronhouder werkt met standaard FHIR-zoekparameters.
- De afbeelding van functionele concepten op FHIR-elementen staat in de IG.

5.2.3.2 Wel aanmaken en verwijderen, niet wijzigen

Context

Een lokalisatie-record kan onjuist zijn: een verkeerde lokale patiënt-ID, een registratie die niet had moeten plaatsvinden. Er moet een manier zijn om dat te corrigeren.

Besluit

De NVI ondersteunt aanmaken en verwijderen. Wijzigen wordt niet ondersteund; een correctie bestaat uit verwijderen en opnieuw aanmaken.

Rationale

Een lokalisatie-record bestaat uitsluitend uit sleutelvelden: bronhouder, pseudoniem, lokale patiënt-ID en registrerende client. Er is geen veld dat kan wijzigen zonder dat het een ander record wordt.

Wijzigen zou daarom een operatie zijn die intern toch neerkomt op verwijderen en aanmaken, met als verschil dat de identiteit van het record behouden lijkt te blijven terwijl de inhoud volledig is vervangen. Dat is misleidend.

Consequenties

- Correctie is twee handelingen. Gaat de tweede mis, dan is de registratie verdwenen zonder vervanging; de Localization Registration Client moet dat afvangen. De reconciliatie herstelt het uiterlijk bij de volgende ronde, zie 5.2.3.6 Registreren bij de gebeurtenis, reconciliëren als vangnet.
- De implementation guide legt vast dat de NVI aanmaken en verwijderen ondersteunt en geen wijziging.
- Verwijderen is de enige route om een registratie ongedaan te maken. Wie dat mag initiëren is beperkt tot de client die registreerde, zie 5.2.3.4 OAuth-client als registrerende partij. Een verzoek vanuit de burger loopt via de zorgaanbieder. Zie 8.4 Generieke functie Toestemming.

5.2.3.3 Idempotente registratie

Context

Een Localization Registration Client kan dezelfde registratie meermaals aanbieden, bijvoorbeeld na een time-out waarbij onduidelijk is of de eerste poging is aangekomen.

Besluit

De combinatie van bronhouder, lokale patiënt-ID en registrerende client is uniek. De client registreert met een voorwaardelijke aanmaak (FHIR conditional create): bestaat de combinatie al, dan maakt de NVI geen tweede record. Daarnaast ontdebelt de NVI na het ontblinden op de combinatie van bronhouder, pseudoniem en registrerende client. Ook dan levert een herhaalde registratie geen tweede record op. Deze sleutels gelden overal in dit document en in de IG.

De client kent het pseudoniem niet, zie 5.2.2.2 Blinding via OPRF. De eerste sleutel is daarom de enige die de client zelf kan controleren. De tweede sleutel vangt het geval af dat een Datahoudende Zorgaanbieder dezelfde patiënt onder twee lokale patiënt-ID's registreert.

Rationale

Zonder deze eigenschap zou elke onbeantwoorde registratiepoging een risico op duplicaten opleveren, en zou de Localization Client moeten controleren of een registratie al bestaat voordat hij het opnieuw probeert. Dat is precies de situatie waarin een dergelijke controle onbetrouwbaar is.

Afgewezen alternatieven

Alleen ontdebelen op het pseudoniem.

Afgewezen: de waarde die de client verstuurt, is bij elke aanvraag anders door de nieuwe blinderingsfactor. De NVI kan pas na het ontblinden vergelijken. De client kan dan niet zelf vaststellen of zijn registratie al bestaat.

Consequenties

- Een Localization Registration Client kan veilig opnieuw proberen.
- Er is geen aantal registraties per patiënt dat iets zegt over de hoeveelheid gegevens; per combinatie bestaat hooguit één record.
- De NVI slaat de lokale patiënt-ID op. Zie 5.2.2.4 Hashing en versleuteling via een HSM en 6.1 Verdieping: pseudonimisering.

5.2.3.4 OAuth-client als registrerende partij

Context

Een zorgaanbieder kan meerdere systemen hebben die registreren, bijvoorbeeld een EPD en een PACS. Ook tijdens een migratie kunnen twee systemen tijdelijk dezelfde patiënten registreren, bijvoorbeeld een EPD en een bestaande LSP-index. Een voorbeeld laat zien waarom de NVI ook het systeem vastlegt. Zorgaanbieder X heeft twee systemen, A en B. Beide melden aan de NVI dat X patiënt P kent. Later verwijdert systeem B zijn gegevens over P en trekt zijn melding in. Systeem A heeft nog wel gegevens over P. Bij een zoekvraag naar P moet X dus gevonden blijven worden. Legt de NVI alleen de organisatie vast, dan is er maar één registratie voor X en P. De intrekking door B verwijdert die registratie, en X is niet meer vindbaar. Legt de NVI ook het systeem vast, dan zijn er twee registraties. B verwijdert alleen zijn eigen registratie, en die van A blijft staan.

Besluit

Elk lokalisatie-record legt vast welke OAuth-client het registreerde. De NVI neemt die over uit het access token en legt hem vast in de registratie (meta.source). De client geeft hem niet zelf op. Een zorgaanbieder mag meerdere systemen laten registreren, elk met een eigen OAuth-client. Dat is optioneel: een zorgaanbieder met één systeem hoeft hiervoor niets te doen.

Rationale

Het doel is isolatie. Daarnaast levert het drie dingen op: traceerbaarheid van registraties naar het systeem dat ze deed, beheer doordat een zorgaanbieder zijn registraties per systeem kan opvragen, audit doordat de herkomst vastligt. Isolatie betekent dat een systeem uitsluitend zijn eigen registraties kan verwijderen.

Isolatie is de reden voor deze keuze. Zonder onderscheid per systeem zou het PACS de registraties van het XIS kunnen verwijderen. Dit zou kunnen gebeuren wanneer een verwijderverzoek op de beeldinformatie komt. Het PACS verwijdert dan haar informatie en de registratie bij de NVI. Alleen het weet niet dat het XIS ook gegevens geregistreerd had.

Een instelling heeft hiermee de mogelijkheid om meerdere zorgsystemen direct aan de NVI te koppelen zonder dat hier coördinatie op hoeft plaats te vinden.

Voor Bevragende Zorgaanbieders is dit onzichtbaar. De registrerende client heeft geen invloed op de zoekresultaten, zie 5.2.3.5 Registrerende client niet in het antwoord.

De client uit het token is niet te vervalsen. De NVI hoeft daardoor niet te controleren of een opgegeven identifier bij de client hoort.

Afgewezen alternatieven

Een eigen bronsysteem-identificer, los van de authenticatie.

Afgewezen: de NVI moet dan bijhouden welke identifier bij welke client hoort, en die koppeling beheren. Het voordeel is dat registraties bij een wissel van client bij het systeem blijven. Dat weegt niet op tegen het extra beheer, omdat de reconciliatie een wissel al opvangt; zie 5.2.3.6 Registreren bij de gebeurtenis, reconciliëren als vangnet.

Coördinatie bij de zorgaanbieder.

De zorgaanbieder zet een eigen tussenvoorziening (proxy) voor de eigen systemen, die de registraties coördineert. Afgewezen: dat vraagt een extra voorziening van elke zorgaanbieder met meerdere systemen, terwijl de implementatie in de NVI klein is.

Consequenties

- Een zorgaanbieder met meerdere registrerende systemen geeft elk systeem een eigen OAuth-client.
- Wisselt een systeem van client, bijvoorbeeld bij een andere leverancier, dan verwijdert de oude client zijn registraties en registreert de nieuwe client opnieuw.
- Een client kan alleen zijn eigen registraties opvragen en verwijderen.
- Verwijderen is daarmee gebonden aan de client die registreerde.

5.2.3.5 Registrerende client niet in het antwoord

Context

De registrerende client is nodig voor het beheer van registraties. Bij een bronhouder met meerdere systemen zou het antwoord kunnen vermelden welk systeem registreerde. De Bevragende Zorgaanbieder zou dan gericht dat systeem kunnen bevragen in plaats van alle systemen van die bronhouder.

Besluit

De NVI geeft de registrerende client niet terug in het antwoord.

Rationale

Gerichte routing werkt niet op basis van de registrerende client. Een zorgaanbieder kan alle registraties via één systeem laten lopen, bijvoorbeeld het XIS, ook als andere systemen ook gegevens hebben. De registrerende client zegt dus niet waar de gegevens staan. Bereikbaarheid is een vraagstuk van de generieke functie Adressering: een Bevragende Zorgaanbieder zoekt via de URA de endpoints van de bronhouder op en kiest op grond van connectionType en payloadType. Blijven er meerdere endpoints over, dan bevrage hij ze allemaal.

Afgewezen alternatieven

De registrerende client in het antwoord, voor gerichte routing.

Afgewezen: de client is niet naar een endpoint te vertalen, omdat de generieke functie Adressering geen systeembegrip kent. Het antwoord zou bovendien iets prijsgeven over de interne inrichting van de Datahoudende Zorgaanbieder.

Consequenties

- Een Bevragende Zorgaanbieder gebruikt altijd GF Adressering om het gewenste endpoint te vinden wat past bij de use-case.
- Bij een Datahoudende Zorgaanbieder met meerdere passende endpoints doet de Bevragende Zorgaanbieder meerdere bevestigingen. Dat is een geaccepteerde prijs.

5.2.3.6 Registreren bij de gebeurtenis, reconciliëren als vangnet**Context**

De functie werkt alleen als de registraties in de NVI overeenkomen met de situatie bij de Datahoudende Zorgaanbieder. Een ontbrekende registratie maakt een Datahoudende Zorgaanbieder onvindbaar. Een overbodige registratie leidt tot onnodige vragen aan de Datahoudende Zorgaanbieder. Registraties kunnen uit de pas lopen door storingen, fouten of gemiste gebeurtenissen.

Besluit

Een Datahoudende Zorgaanbieder registreert een patiënt zodra aan twee voorwaarden is voldaan: de Datahoudende Zorgaanbieder heeft gegevens over de patiënt, en de Datahoudende Zorgaanbieder mag de patiënt in de NVI registreren. De Localization Registration Client registreert direct, als onderdeel van de gebeurtenis die dat veroorzaakt. Kan een client niet op het moment van de gebeurtenis registreren, dan registreert hij binnen 24 uur. Vervalt een van beide voorwaarden, dan verwijdert de client de registratie.

Daarnaast vergelijkt de client minstens wekelijks zijn eigen registraties bij de NVI met de lokale situatie (reconciliatie). Hij registreert wat ontbreekt en verwijdert wat er niet meer hoort, ook dubbele registraties. Het stappenplan staat in de IG.

Rationale

Registreren bij de gebeurtenis maakt een Datahoudende Zorgaanbieder zo snel mogelijk vindbaar. Dat telt voor de patiëntveiligheid: een patiënt die net is behandeld, moet bij een volgende zorgverlener vindbaar zijn.

Gebeurtenissen kunnen gemist worden. De reconciliatie herstelt dat, zonder dat de Datahoudende Zorgaanbieder hoeft te weten wat er misging.

De client haalt eerst zijn registraties bij de NVI op en stelt pas daarna de lokale lijst samen. Een patiënt die tussendoor wordt geregistreerd, staat dan wel in de lokale lijst maar mogelijk niet in de NVI-lijst. Dat leidt hooguit tot een herhaalde registratie, en die levert geen duplicaat op; zie 5.2.3.3

Idempotente registratie. De omgekeerde volgorde kan een net geregistreerde patiënt onterecht laten verwijderen.

Afgewezen alternatieven

Alleen periodiek registreren, bijvoorbeeld in een nachtelijke batch.

Afgewezen: een Datahoudende Zorgaanbieder is dan tot een dag onvindbaar na een behandeling. Dat is alleen aanvaardbaar voor clients die niet op gebeurtenissen kunnen reageren.

Alleen registreren bij de gebeurtenis.

Afgewezen: een gemiste gebeurtenis wordt dan nooit hersteld, en niemand merkt het.

Automatisch verlopen van registraties (time-to-live).

Een registratie vervalt dan als de client haar niet op tijd vernieuwt. Afgewezen: de NVI moet dan per registratie een datum bewaren, en die zegt iets over het moment van zorg. In plaats daarvan toetsen de kwalificatie-eisen en testscenario's dat verwijderen in het bronsysteem ook leidt tot verwijderen in de NVI.

Consequenties

- De Localization Registration Client moet zijn eigen registraties kunnen opvragen bij de NVI.
- Een fout in eerdere registraties of een wissel van client is uiterlijk binnen een week hersteld.
- Een verwijderverzoek van de burger moet ook lokaal verwerkt zijn, anders registreert de reconciliatie de patiënt opnieuw. Zie 8.4 Generieke functie Toestemming.

5.2.4 Onderwerp interoperabiliteit en standaarden

5.2.4.1 Het koppelvlak is vervangbaar

Context

Het koppelvlak is nu FHIR R4. Alhoewel deze keuze goed aansluit bij de [EU Health Data API Implementation Guide](#) is deze keuze mogelijk niet voor de hele levensduur houdbaar: EHDS publiceert standaarden op 26 maart 2027, met een eerste verplichting op 26 maart 2029 en volledige verplichting op 26 maart 2031. De impact van deze standaarden op de generieke functie Lokalisatie zal worden gemonitord.

Besluit

De NVI moet een nieuwe API-standaard kunnen ondersteunen zonder dat de verwerkings- en opslaglaag daarvoor hoeft te wijzigen.

Rationale

De eis gaat over vervangbaarheid, niet over het naast elkaar aanbieden van varianten. Wat vastligt is dat het koppelvlak een laag is en geen eigenschap van de kern: de NVI werkt intern met pseudoniem, URA, lokale patiënt-ID en registrerende client, en welke standaard die gegevens naar buiten draagt staat daar los van.

Dat is geen vanzelfsprekendheid. Zou de opslag zijn gemodelleerd naar de FHIR-resources waarin nu wordt uitgewisseld, dan raakt elke standaardwijziging de datastore, en dan is adoptie van EHDS een herbouw in plaats van een uitbreiding.

Consequenties

- Het interne model volgt het informatiemodel en niet het FHIR-profiel.
- Een nieuwe standaard raakt de verwerkings- en opslaglaag niet.

5.2.5 Onderwerp beveiliging en vertrouwen

5.2.5.1 OAuth 2.0 met centrale client-registratie voor toegang tot het koppelvak

Context

Voordat de vraag aan de orde is óf een specifieke vraag gesteld mag worden, moet vaststaan welke systemen überhaupt met de NVI mogen praten en namens wie zij dat doen. Veel zorgaanbieders laten dit uitvoeren door een leverancier.

Dit is een andere vraag dan die van 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie. Daar gaat het om de autorisatie van een individuele vraag; hier om toegang tot het koppelvak als zodanig.

Besluit

Toegang tot het koppelvak verloopt via een aparte OAuth 2.0-dienst die access tokens uitgeeft. Client-registraties staan in een centrale database, waarin leveranciers expliciet zijn gekoppeld aan de zorgaanbieders die zij bedienen, en aan de rol waarvoor zij zijn aangesloten: registreren als bron, of bevragen als Bevragende Zorgaanbieder.

Deze dienst beslist niet over individuele vragen. Dat is belegd bij de generieke functie Autorisatie, zie 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie.

Rationale

De scheiding van de kern maakt het mogelijk het toegangsmodel te wijzigen zonder de NVI aan te passen, en biedt ruimte voor toekomstige toegang door bijvoorbeeld burgerapplicaties. OAuth 2.0 sluit aan bij de keuzes van het Forum Standaardisatie.

De expliciete koppeling van leveranciers is de kern. Het alternatief is dat een zorgaanbieder zijn eigen sleutelmateriaal, bijvoorbeeld een UZI-servercertificaat, aan meerdere leveranciers verstrekt. Dat maakt achteraf niet vaststelbaar wie een handeling heeft verricht en verspreidt sleutelmateriaal over partijen die het niet zouden moeten hebben.

Die herleidbaarheid is een voorwaarde voor elk autorisatiemodel dat de generieke functie Autorisatie vaststelt: een beslissing over een vraag heeft geen betekenis als achteraf niet vaststaat wie hem stelde.

Afgewezen alternatieven

Delen van het certificaat van de zorgaanbieder met leveranciers.

Afgewezen: verspreidt sleutelmateriaal en maakt auditing onmogelijk.

Consequenties

- Access tokens voor toegang tot het koppelvak.
- Een centrale client-registratie, gerepliceerd zoals de rest van de NVI.
- Een aanmeldproces buiten de API om, waarin de koppeling leverancier tot zorgaanbieder wordt vastgelegd.
- De verhouding tussen dit access token en de autorisatiebeslissing van de generieke functie Autorisatie moet worden uitgewerkt: het kan een tweede token zijn, een claim in hetzelfde token, of een aparte toets. Zie 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie.
- Elke handeling is herleidbaar tot de organisatie en de client die haar verrichtte. Dit is geen bijproduct maar een eis: zonder herleidbaarheid is verantwoording achteraf onmogelijk en valt de grond onder elk autorisatiemodel weg, ongeacht welke vorm de generieke functie Autorisatie kiest.

- Openstaand. Hoe een zorgaanbieder een leverancier machtigt, is nog niet uitgewerkt. Zie ook generieke functies Autorisatie en Authenticatie.

5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie

Context

Op drie punten in de keten moet worden vastgesteld of een handeling is toegestaan.

1. Bij de Bevragende Zorgaanbieder, vóór de vraag.

Mag deze zorgverlener, onder deze omstandigheden, voor deze patiënt überhaupt een lokalisatievraag stellen? Dit is het enige punt waar alle benodigde gegevens aanwezig zijn: de identiteit van de zorgverlener, zijn rol, de patiënt en de context waarin hij handelt. Het is ook het enige punt dat vóór de pseudonimisering ligt, en dus vóór het moment waarop de patiënt uit beeld verdwijnt.

2. Bij de bron, bij het beantwoorden van de lokalisatievraag.

Mag de Bevragende Zorgaanbieder weten dat deze Datahoudende Zorgaanbieder gegevens over de patiënt heeft? De NVI kent de zorgverlener niet, en door de pseudonimisering kent zij de patiënt niet. De Datahoudende Zorgaanbieder kent de patiënt en haar eigen beleid wel. Zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord.

3. Bij de bron, bij het verstrekken van gegevens.

Mag deze zorgverlener deze gegevens inzien? Dit valt buiten de lokalisatiefunctie, maar volgt dezelfde regels.

Besluit

Het autoriseren van handelingen wordt belegd bij de generieke functie Autorisatie: bij de Bevragende Zorgaanbieder vóór de vraag, bij de Datahoudende Zorgaanbieder bij het beantwoorden van de lokalisatievraag en bij de Datahoudende Zorgaanbieder bij het verstrekken van gegevens. De lokalisatiefunctie definieert geen eigen autorisatieregels.

De lokalisatiefunctie levert wat daarvoor nodig is: de handeling is herleidbaar tot organisatie en client, en de NVI vraagt de beslissing van de Datahoudende Zorgaanbieder op voordat zij een Datahoudende Zorgaanbieder in het antwoord opneemt.

Voor de identiteit waarop die beslissing steunt, worden naar verwachting de generieke functies Identificatie en Authenticatie gebruikt.

Rationale

Autorisatie is geen eigenschap van de lokalisatiefunctie maar van het stelsel. Dezelfde vraag, gesteld door dezelfde partij, hoort hetzelfde antwoord te krijgen ongeacht welke generieke functie hem verwerkt. Dat vraagt één plek waar de regels worden vastgesteld.

Zou de lokalisatiefunctie eigen regels definiëren, dan ontstaat een tweede autorisatiemodel naast dat van het stelsel, met twee gevolgen. Regels lopen uiteen zodra een van beide wijzigt. En de bronhouder krijgt te maken met autorisatieregels die per bevrage functie verschillen, terwijl hij één endpoint aanbiedt.

De keuze legt daarmee een afhankelijkheid vast in plaats van een oplossing. Dat is bewust: het alternatief is een tijdelijke eigen invulling die later moet worden teruggedraaid.

Afgewezen alternatieven

Een eigen autorisatiemodel in de lokalisatiefunctie.

Afgewezen: duplicceert wat op stelselniveau hoort en loopt onvermijdelijk uiteen met de generieke functie Autorisatie.

Consequenties

- De lokalisatiefunctie is voor autorisatie afhankelijk van de generieke functie Autorisatie, op drie punten. Zie 8.2 Generieke functie Autorisatie.
- De Localization Search Client moet een autorisatiebeslissing kunnen inwinnen vóór hij een pseudoniem opvraagt, en het resultaat kunnen afdwingen. Zie 4.1.3 Localization Registration Client en 4.1.4 Localization Search Client.
- De NVI vraagt de beslissing van de Datahoudende Zorgaanbieder op en dwingt die af, zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord. Op welke regels de Datahoudende Zorgaanbieder haar beslissing baseert, hangt af van de kaders die de generieke functie Autorisatie stelt.
- Herleidbaarheid van handelingen blijft een eis van de lokalisatiefunctie zelf, ongeacht het autorisatiemodel. Zie 5.2.5.1 OAuth 2.0 met centrale clientregistratie voor toegang tot het koppelvlak.
- Zolang die kaders er niet zijn, is niet vast te stellen wat een aansluitende partij op dit punt moet bouwen.

Generieke functie Autorisatie moet hier nog kaders voor stellen.

Dit besluit legt vast waar autorisatie wordt belegd, niet hoe zij werkt. De volgende punten zijn nodig voordat dit ontwerp op dit punt uitvoerbaar is:

- Op welk niveau wordt geautoriseerd: organisatie, zorgverlener, of een combinatie. Dit bepaalt of, en zo ja welke, gegevens over de zorgverlener bij een autorisatiebeslissing betrokken raken.
- Waarop de beslissing steunt: behandelrelatie, toestemming, rol, of een combinatie daarvan, en welke partij die gegevens aanlevert.
- Waar de beslissing wordt genomen: centraal bij de generieke functie Autorisatie, of lokaal bij de NVI en de bronhouder op grond van meegeleverde attributen.
- Hoe de beslissing wordt overgedragen: het formaat waarin de NVI haar ontvangen en kunnen verifiëren.
- Of de drie punten hetzelfde model volgen, of dat de toets bij de Bevragende Zorgaanbieder, het lokaliseren en het verstrekken verschillend worden geautoriseerd. Het zijn drie wezenlijk verschillende handelingen: de eerste beoordeelt of de vraag gesteld mag worden, de tweede levert een lijst bronhouders, de derde levert gegevens.
- Wat de toets bij de Bevragende Zorgaanbieder precies weegt: behandelrelatie, rol van de zorgverlener, spoedsituatie, toestemming, of een combinatie. Dit is het punt waar de meeste gegevens beschikbaar zijn en dus de meeste keuzevrijheid bestaat.
- Hoe wordt geborgd dat die toets ook plaatsvindt. De toets ligt bij de Bevragende Zorgaanbieder zelf. Zonder aanvullende maatregel is voor de NVI en de bronhouder niet zichtbaar of hij is uitgevoerd; een verklaring daarover in het verzoek is een mogelijkheid, maar dat is een keuze van de generieke functie Autorisatie.

Tot die kaders er zijn, beschrijft appendix A.1 de huidige tussenoplossing voor de toets bij de Bevragende Zorgaanbieder, en niet het beoogde eindbeeld.

5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord

Context

Een lokalisatie-antwoord vertelt de Bevragende Zorgaanbieder bij welke bronnen een patiënt bekend is. Die (voormalige) behandelrelaties zijn zelf gevoelige informatie. De Datahoudende Zorgaanbieder is verantwoordelijk voor het delen ervan, en alleen de Datahoudende Zorgaanbieder kent haar eigen beleid en de wensen van de patiënt. De NVI kent de patiënt niet en kan die afweging niet maken.

Besluit

De NVI vraagt bij elke gevonden Datahoudende Zorgaanbieder een autorisatiebeslissing op voordat zij die Datahoudende Zorgaanbieder in het antwoord opneemt. De Custodian Server van de Datahoudende Zorgaanbieder beslist. Daarbij geldt:

- De NVI stuurt een HEAD-verzoek naar de bestaande FHIR-API van de bron, met de lokale patiënt-ID. Bevat de zoekcontext een datacategorie, dan is er één verzoek per resourcetype van die datacategorie. Bevat zij geen datacategorie, dan gaat het verzoek naar de resource Patient.
- Antwoord 200 betekent toestaan. Elk ander antwoord betekent weigeren.
- De Datahoudende Zorgaanbieder antwoordt binnen 1 seconde. Een later antwoord of geen antwoord telt als weigeren.
- Eén keer toestaan per Datahoudende Zorgaanbieder is genoeg om de Datahoudende Zorgaanbieder in het antwoord op te nemen.
- De NVI bewaart de uitkomst niet. Elke zoekvraag leidt tot nieuwe verzoeken.

Rationale

De Datahoudende Zorgaanbieder doorbreekt haar beroepsgeheim als zij laat weten dat zij een patiënt kent. Daarom beslist de Datahoudende Zorgaanbieder en niet de NVI. De lokalisatiefunctie definieert daarbij geen eigen regels: de Datahoudende Zorgaanbieder past haar eigen beleid toe, en dat volgt de generieke functie Autorisatie. Zie 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie.

De HEAD-verzoeken gebruiken de FHIR-API die de Datahoudende Zorgaanbieder al heeft. HEAD geeft alleen een status terug en geen gegevens. De Datahoudende Zorgaanbieder hoeft geen nieuw koppelvlak te bouwen, en de beslissing volgt dezelfde regels als het latere ophalen van de gegevens.

Weigeren bij een fout of time-out is de veilige keuze: bij twijfel deelt de NVI niets. Voor de Bevragende Zorgaanbieder is een weigering daardoor niet te onderscheiden van een Datahoudende Zorgaanbieder die onbereikbaar was. Dat is bewust: anders lekt een weigering alsnog dat de Datahoudende Zorgaanbieder de patiënt kent.

De NVI bewaart de uitkomst niet, omdat beleid en toestemming tussen twee vragen kunnen veranderen.

Afgewezen alternatieven

Een toestemmingscontrole door de NVI via Mitz.

Afgewezen: Mitz is geen landelijke verplichting. Dit wordt opnieuw bekeken zodra er onder de EHDS een centraal zeggenschapsregister is, zie 8.4 Generieke functie Toestemming. Bovendien kent de NVI de patiënt niet. Zij zou daarvoor gegevens moeten ontvangen die het ontwerp juist buiten de NVI houdt.

Een apart autorisatiekoppelvlak bij de Datahoudende Zorgaanbieder.

Afgewezen: dat vraagt van elke Datahoudende Zorgaanbieder een nieuw koppelvlak, met eigen regels naast die van haar FHIR-API.

De uitkomst tijdelijk bewaren.

Afgewezen: een gewijzigde beslissing van de Datahoudende Zorgaanbieder zou dan pas later gelden.

Consequenties

- Elke Datahoudende Zorgaanbieder moet de rol van Custodian Server op haar FHIR-API ondersteunen. Een Datahoudende Zorgaanbieder die dat niet doet, komt nooit in een antwoord.
- De NVI moet de FHIR-API van de Datahoudende Zorgaanbieder kunnen vinden via de generieke functie Adressering. Zonder vindbaar endpoint komt de Datahoudende Zorgaanbieder niet in het antwoord. Zie 8.1 Generieke functie Adressering.
- Een zoekvraag duurt hooguit ongeveer 1 seconde langer dan het zoeken in de NVI zelf. De eis van 1 seconde wordt onderdeel van de kwalificatie-eisen voor de Custodian Server.
- De Datahoudende Zorgaanbieder leert dat er naar haar patiënt is gezocht. Welke gegevens over de Bevragende Zorgaanbieder zij daarbij ontvangt, hangt af van de kaders van de generieke functie Autorisatie. Zie 6.1 Verdieping: pseudonimisering.
- Bevat de zoekcontext een datacategorie, dan kan een Datahoudende Zorgaanbieder per datacategorie anders beslissen, omdat de verzoeken dan per resourcetype gaan. Dat is ook een inhoudelijke controle: een bron die aan de zoekcontext voldoet maar geen gegevens van dat type heeft, kan weigeren.

5.2.5.4 Gescheiden logging voor SOC en burgerinzage

Context

Logging dient twee doelen die weinig met elkaar te maken hebben: detectie van misbruik door een Security Operations Center, en inzage door de burger in wat er met zijn gegevens is gebeurd. EHDS stelt eisen aan dat laatste.

Besluit

De NVI voert beide vormen van logging langs gescheiden kanalen.

Rationale

De twee doelen stellen andere eisen aan retentie, aan detailniveau en aan wie toegang heeft. SOC-logging is fijnmazig en operationeel; inzagelogging is begrijpelijk en op de burger gericht. Eén logstroom betekent dat de strengste eis voor beide geldt, en dat de burger inzage krijgt in gegevens die daar niet voor bedoeld zijn.

Consequenties

- Twee logstromen met eigen retentie-instellingen.
- Verwerking buiten de applicatie, zodat keuzes over opslag en retentie los van de NVI kunnen worden gemaakt.

De uitwerking van de logging-eisen is nog niet afgerond. Dit hangt samen met de eisen en invulling uit de burgerinzage-rechten uit de EHDS.

6 Verdiepingen

Een verdieping legt een mechanisme uit waar meerdere architectuurkeuzes op steunen. Zij geeft uitleg en context die over meerdere keuzes heen loopt en daarom bij geen van die keuzes afzonderlijk thuishoort.

Wat een onderwerp tot verdieping maakt: er hangen meerdere architectuurkeuzes aan, het mechanisme is niet af te leiden uit die keuzes zelf, en de normatieve uitwerking staat elders. Een verdieping legt uit; zij specificiert niet.

Dit TO heeft één verdieping.

6.1 Verdieping: pseudonimisering

Het probleem

Een centrale index die vastlegt welke zorgaanbieder gegevens over welke patiënt heeft, bevat geen gedetailleerde medische inhoud maar wel het gegeven wie waar onder behandeling is of is geweest. Een index van 17 miljoen burgers en enkele duizenden zorgaanbieders is daarmee een grote verzameling bijzondere gegevens.

Vanuit gegevensbescherming is de opgave: zorg dat de index ook bij volledige inzage niet vertelt over wie hij gaat.

Het mechanisme

Het mechanisme bestaat uit een reeks stappen die elk een specifieke partij iets onthouden. Ze staan hieronder in de volgorde waarin ze worden doorlopen; de onderliggende besluiten staan in 5.2 Architectuurkeuzes en worden hier niet herhaald.

De keten begint bij de Localization Client, de enige partij die het BSN kent. Die haalt het uit het eigen dossier. Het BSN is de enige invoer. Zie 5.2.2.3 Pseudoniemen per ontvanger.

Voordat er iets de deur uit gaat, versluiert de Localization Client die invoer met een geheim dat hij zelf kiest en lokaal houdt. De dienst die vervolgens gaat rekenen, ziet daardoor een waarde die voor haar niet te onderscheiden is van willekeur. Zie 5.2.2.2 Blindering via OPRF.

Het rekenwerk gebeurt niet bij de NVI maar bij een aparte dienst, de PRS, met eigen beheer en eigen sleutelbeheer. Die scheiding is essentieel: zonder haar zou één partij zowel de sleutel als de invoer zien, en dan zijn alle andere stappen zinloos. Zie 5.2.2.1 Pseudonimisering door een aparte dienst.

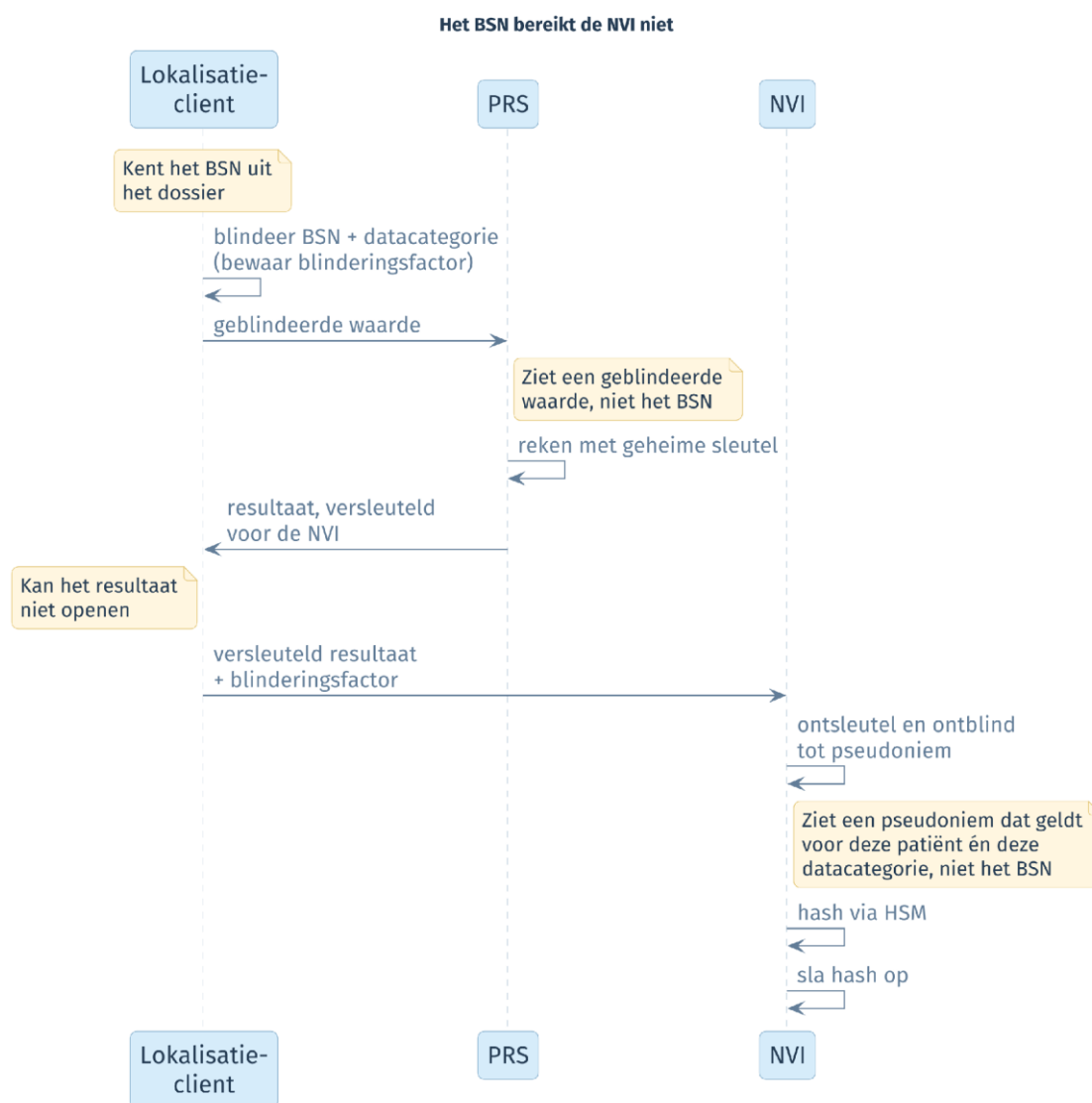
De PRS rekent met haar sleutel op de versluierte waarde. De bewerking werkt door de versluiting heen, zodat de uitkomst dezelfde is als wanneer zij op de onbewerkte invoer had gerekend, terwijl zij die invoer nooit heeft gezien. Het resultaat versleutelt zij voor de beoogde ontvanger.

De Localization Client krijgt dat resultaat terug maar kan het niet openen. Hij geeft het door aan de NVI, samen met het geheim waarmee hij versluierte. Pas daar komen beide delen samen en ontstaat het pseudoniem. Dat de Localization Client het zelf niet ziet is geen bijvangst: het voorkomt dat een zorgaanbieder pseudoniemen van verschillende ontvangers naast elkaar legt.

Het pseudoniem dat zo ontstaat geldt alleen voor deze ontvanger. Een andere ontvanger krijgt voor dezelfde persoon een andere waarde, waardoor registraties tussen partijen niet te koppelen zijn. Zie 5.2.2.3 Pseudoniemen per ontvanger.

Wat de NVI ten slotte opslaat is niet dat pseudoniem maar een hash ervan, berekend met een sleutel die haar HSM niet verlaat. Ook wie de database volledig leest, houdt daarmee een waarde over die zonder die sleutel nergens naartoe leidt. De lokale patiënt-ID van de Datahoudende Zorgaanbieder slaat de NVI versleuteld op, ook met een sleutel in de HSM. Zie 5.2.2.4 Hashing en versleuteling via een HSM.

Onderstaand diagram toont dezelfde keten in de tijd.



De cryptografische specificatie staat in de implementation guide en in het Technisch Ontwerp van de PRS.

Wat het oplevert

De NVI beschikt niet over het BSN.

Niet in opslag, niet in het berichtenverkeer. Wie de NVI-database volledig leest, ziet hashes waaruit geen BSN valt af te leiden.

De PRS beschikt niet over de behandelrelatie.

De PRS voert de omzetting uit zonder te weten om welk BSN het gaat. Zij leert dus niet dat een bepaalde zorgaanbieder naar een bepaalde patiënt vraagt.

Herleiden vraagt meerdere onafhankelijke compromitteringen.

Om van de NVI-gegevens terug te komen bij een BSN moeten drie stappen worden gezet: de PRS moet een opzoektafel van BSN naar pseudoniem opleveren, alle pseudoniemen moeten via de HSM-sleutel van de NVI naar hun hash worden vertaald, en pas dan zijn de NVI-gegevens te herleiden.

Dat vraagt dat de controls bij zowel de PRS als de NVI volledig worden omzeild, inclusief het sleutelbeheer van de HSM.

Partijen kunnen niet onderling koppelen.

Door de ontvanger (NVI)-specifieke pseudoniemen levert het vergelijken van registraties tussen NVI en door PRS uitgegeven pseudoniemen voor andere partijen niets op.

De client (zorgaanbieder) ziet het pseudoniem niet.

Het ontblinden gebeurt bij de ontvanger, niet bij de Localization Client. Zie 5.2.2.2 Blindering via OPRF.

Binnen de NVI ontstaat geen profiel per datacategorie.

De NVI legt geen datacategorie per registratie vast. Wat zij per pseudoniem kent, is alleen een lijst bronhouders. Zie 5.2.2.3 Pseudoniemen per ontvanger.

Wat het niet oplost

De maatregelen zijn ontworpen tegen het scenario dat de NVI-database in verkeerde handen valt. Deze paragraaf beschrijft wat in dat geval overblijft. Een aangesloten zorgaanbieder is hier niet het uitgangspunt: die kent zijn eigen patiënten toch al, en wat hij bij de NVI mag opvragen is een autorisatievraagstuk (5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie) en geen eigenschap van de pseudonimisering.

Wat een gelekte database bevat, is per registratie: een gehasht pseudoniem, de URA van de bronhouder, de registrerende client en de versleutelde lokale patiënt-ID. Geen BSN, geen naam, geen tijdstip en geen datacategorie.

De verzameling zelf is een gegeven.

Ook zonder één pseudoniem te herleiden, laat de database zien hoeveel registraties er per zorgaanbieder zijn. Dat zegt iets over de omvang van de patiëntenpopulatie van elke aangesloten zorgaanbieder. Dat is bedrijfsgevoelige informatie, geen patiëntgegevens, maar het is er wel.

Wat er niet uit blijkt, is waar die registraties over gaan. De NVI slaat geen datacategorie op. Uit een gelekte database is dus niet af te leiden hoe de registraties van een zorgaanbieder over datacategorieën zijn verdeeld.

Een pseudoniem is te toetsen als je een BSN hebt.

De hash beschermt tegen lezen, niet tegen raden. Wie de database heeft én van een specifiek persoon het BSN kent, kan niet zomaar het pseudoniem afleiden: daarvoor is de sleutel van de PRS nodig, en

de HSM-sleutel van de NVI om bij de hash te komen. Zolang beide sleutels buiten bereik blijven, blijft een gelekte database een verzameling losse waarden. Dit is de reden dat 5.2.2.4 Hashing en versleuteling via een HSM en de organisatorische scheiding van 5.2.2.1 Pseudonimisering door een aparte dienst samen moeten gelden: valt één van beide weg, dan wordt toetsen van een BSN-lijst tegen de database wél mogelijk.

Een reeks kan onderscheidend zijn, ook zonder herleiding.

Binnen de database horen registraties met hetzelfde gehashte pseudoniem bij elkaar. Dat levert per pseudoniem een lijst zorgaanbieders op. Bij een ongebruikelijke combinatie van zorgaanbieders kan die lijst op zichzelf al naar een kleine(re) groep personen wijzen, zonder dat er iets is herleid en zonder dat bekend is om welk type zorg het gaat.

Die lijst bevat alle bronnen van een persoon, over alle datacategorieën heen. Het type van een bron, af te leiden uit de URA, kan daardoor iets zeggen over de zorg die iemand kreeg. Dit restrisico is aanvaard, zie 5.2.2.3 Pseudoniemen per ontvanger.

Bevestiging van bestaan.

De pseudonimisering verbergt niet dát er een registratie is, alleen over wie hij gaat. Wie langs een andere weg al weet welk pseudoniem bij iemand hoort, leert uit de database bij welke zorgaanbieders die persoon bekend is.

De lokale patiënt-ID.

De NVI slaat per registratie de lokale patiënt-ID van de Datahoudende Zorgaanbieder op. Wie die ID aan een persoon kan koppelen, bijvoorbeeld iemand met toegang tot de systemen van de bron, kan via het pseudoniem zien bij welke andere bronnen die persoon geregistreerd is. Twee maatregelen beperken dit. De NVI slaat de ID versleuteld op met een sleutel in de HSM, zie 5.2.2.4 Hashing en versleuteling via een HSM. En de Datahoudende Zorgaanbieder gebruikt een ondoorzichtig nummer dat zij alleen voor de NVI gebruikt, zodat het buiten de Datahoudende Zorgaanbieder niet aan een persoon te koppelen is.

De Datahoudende Zorgaanbieder leert dat er gezocht is.

Bij elke zoekvraag stuurt de NVI de lokale patiënt-ID naar de gevonden bronnen, zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord. Een Datahoudende Zorgaanbieder leert daardoor dat er naar haar patiënt is gezocht. Zij kent de patiënt al, maar dit gegeven is nieuw. Zij leert ook wie er zoekt, voordat vaststaat of er toestemming is; zie 8.4 Generieke functie Toestemming.

De positie van de PRS.

De PRS beschikt over het sleutel materiaal waarmee pseudoniemen worden afgeleid. Zij kan het BSN niet uit een enkele aanvraag halen, maar is wel de partij die in samenwerking met de NVI de herleiding mogelijk zou maken. De scheiding tussen PRS en NVI is daarmee niet alleen technisch maar ook organisatorisch van belang: worden beide door dezelfde partij beheerd met hetzelfde sleutelbeheer, dan is het één systeem met twee namen en vervalt de bescherming.

Het BSN bij de bronbevraging.

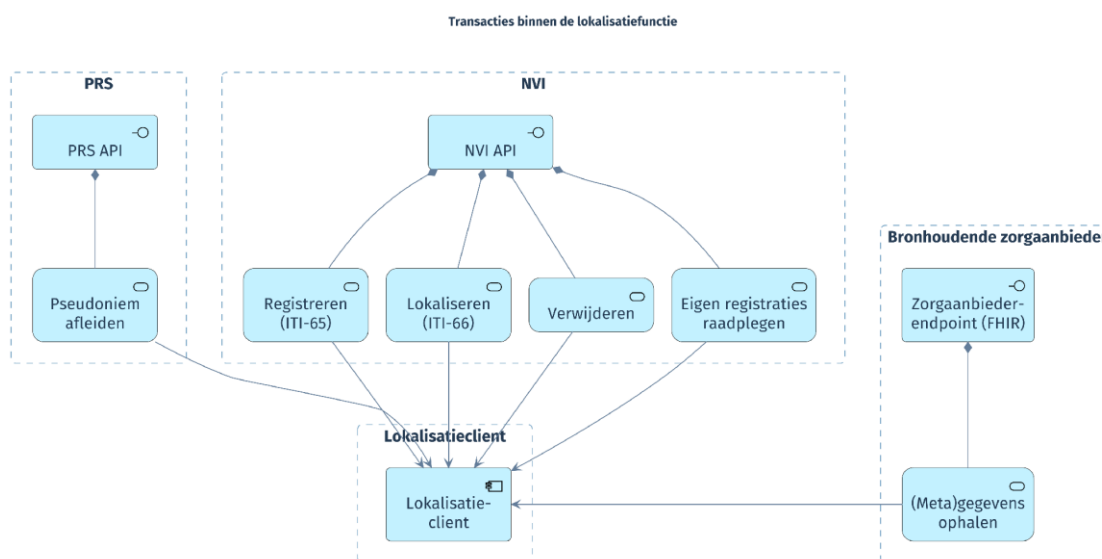
Nadat de bronhouders zijn gevonden, bevraagt een client hen met het BSN. Dat is nodig omdat de bronhouder zijn dossier op BSN voert. De pseudonimisering beschermt de NVI, niet de keten daarna.

Keuzes die hierop steunen

- 5.2.2.1 Pseudonimisering door een aparte dienst
- 5.2.2.2 Blindering via OPRF
- 5.2.2.3 Pseudoniemen per ontvanger
- 5.2.2.4 Hashing en versleuteling via een HSM
- 5.2.2.5 Antwoord zonder identificerende gegevens

7 Interfaces en transacties

7.1 Transactieoverzicht



7.2 Transacties

De normatieve uitwerking van elke transactie, inclusief zoekparameters, foutcodes en voorbeelden, staat in de IG. Hieronder alleen wat de transactie doet en waar zij op steunt.

GF-PSD-1 Evaluate blinded input

Aangeboden door de PRS, afgenomen door beide Localization Clients. Zet een geblindeerd BSN om naar een ontvanger-specifiek pseudoniem, versleuteld voor de NVI. Zie 6.1 Verdieping: pseudonimisering.

GF-LOC-1 Register Patient

Aangeboden door de NVI, afgenomen door de Localization Registration Client. Legt vast dat een bronhouder gegevens over een patiënt heeft. Idempotent, zie 5.2.3.3 Idempotente registratie.

GF-LOC-4 Search Localization

Aangeboden door de NVI, afgenomen door de Localization Search Client. Levert de lijst bronhouders die bij de zoekcontext passen en de vermelding toestaan. Zie 5.2.1.2 Alleen de lijst bronhouders in het antwoord en 5.2.1.3 FHIR search voor lokalisatie.

GF-LOC-5 Authorization Decision

Aangeboden door de Custodian Server, afgenomen door de NVI. Geeft per gevonden Datahoudende Zorgaanbieder de beslissing of de Datahoudende Zorgaanbieder in het antwoord vermeld mag worden. Zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord.

GF-LOC-2 Delete Patient

Aangeboden door de NVI, afgenomen door de Localization Registration Client. Verwijdert een registratie. Een client kan uitsluitend eigen registraties verwijderen, zie 5.2.3.4 OAuth-client als registrerende partij.

GF-LOC-3 Retrieve Registrations

Aangeboden door de NVI, afgenomen door de Localization Registration Client. Levert de registraties die deze client heeft gedaan, voor beheer en reconciliatie. Zie 5.2.3.6 Registreren bij de gebeurtenis, reconciliëren als vangnet.

Wijzigen

Wijzigen bestaat niet als transactie. Zie 5.2.3.2 Wel aanmaken en verwijderen, niet wijzigen.

Openstaand. Wie een registratie mag intrekken buiten de registrerende client om, is nog niet belegd. Dit raakt ook verwijderverzoeken vanuit de burger en EHDS-blokkeringen; zie 8.4 Generieke functie Toestemming.

8 Afhankelijkheden van andere generieke functies

De lokalisatiefunctie is niet zelfstandig bruikbaar. Dit hoofdstuk legt per afhankelijkheid vast wat wordt afgenomen en waar de grens ligt tussen wat de lokalisatiefunctie zelf regelt en wat zij overneemt.

Wat hier niet staat is een beschouwing over uitval. Een generieke functie is geen systeem maar een verzameling afspraken, standaarden en rollen; “de generieke functie Adressering is down” is daarom geen zinvolle uitspraak. Uitval speelt op het niveau van concrete voorzieningen, en die worden per functie in het eigen technisch ontwerp belegd. Bovendien is de uitkomst voor de keten in vrijwel alle gevallen dezelfde: valt een schakel weg, dan komt er geen resultaat op het scherm.

Wat wél per afhankelijkheid verschilt, en dus hier staat, is iets anders: welke afspraken de lokalisatiefunctie nodig heeft van de andere functie, en wat er nog niet is vastgelegd. Dat bepaalt of dit ontwerp uitvoerbaar is.

Eén gevolg van deze afhankelijkheden is wel op voorhand duidelijk. De keten is niet beter beschikbaar dan haar zwakste schakel, en de NVI is daarin één voorziening naast andere: de PRS, en de voorzieningen die de generieke functie Adressering en de generieke functie Autorisatie invullen, bepalen mede de uitkomst. Een beschikbaarheidsafpraak over de NVI alleen zegt daarom weinig over wat de zorgverlener merkt. Zulke afspraken horen op ketenniveau te worden gemaakt, tussen de beheerorganisaties van die voorzieningen.

8.1 Generieke functie Adressering

Wat wordt afgenomen

De Localization Search Client zoekt na lokalisatie het endpoint op waarop een gevonden bronhouder bereikbaar is. De NVI gebruikt de gegevens van Adressering ook zelf, op twee plekken. Zij zet de

zoekcontext om met haar kopie van die gegevens, zie 5.2.1.3 FHIR search voor lokalisatie. En zij vindt daarmee de FHIR-API van de Datahoudende Zorgaanbieder voor de autorisatiebeslissing, zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord.

Grens

Adressering levert het adres; lokalisatie bepaalt wie er benaderd wordt. Zie 5.2.3.5 Registrerende client niet in het antwoord.

Wat de afspraak dekt

De lokalisatiefunctie levert een URA; de generieke functie Adressering levert de endpoints van die zorgaanbieder. De client selecteert daaruit op connectionType en payloadType. Blijven er meerdere over, dan bevraagt hij ze alle. Zie 5.2.3.5 Registrerende client niet in het antwoord.

Dat is een bewuste uitkomst en geen tekortkoming. De extra bevestigingen zijn een geaccepteerde prijs.

Voor de NVI dekt de afspraak twee punten. Haar kopie van de gegevens moet actueel zijn, anders filtert zij op verouderde kenmerken. En een Datahoudende Zorgaanbieder moet een vindbaar endpoint voor haar FHIR-API hebben. Zonder dat endpoint kan de NVI geen beslissing opvragen, en komt de Datahoudende Zorgaanbieder niet in het antwoord.

Voor de zorgverlener is het verschil tussen “geen registraties gevonden” en “wel gevonden, maar niet bereikbaar” betekenisvol: het eerste zegt iets over de patiënt, het tweede over de keten. De Localization Search Client moet die twee onderscheiden kunnen tonen.

8.2 Generieke functie Autorisatie

Wat wordt afgenomen

De beslissing of een handeling is toegestaan. Dit geldt op drie plekken: bij de Bevragende Zorgaanbieder vóór de vraag (mag deze zorgverlener voor deze patiënt lokaliseren), bij de Datahoudende Zorgaanbieder bij het beantwoorden van de lokalisatievraag (mag de Bevragende Zorgaanbieder weten dat de Datahoudende Zorgaanbieder gegevens heeft) en bij de Datahoudende Zorgaanbieder bij het verstrekken van gegevens. Zie 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie.

Grens

De lokalisatiefunctie definieert geen autorisatieregels. Zij zorgt dat handelingen herleidbaar zijn en dat de Datahoudende Zorgaanbieder per zoekvraag kan beslissen over vermelding in het antwoord, zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord.

Wat de afspraak moet dekken

De generieke functie Autorisatie moet vaststellen op welk niveau wordt geautoriseerd, waarop de beslissing steunt, waar zij wordt genomen en hoe zij wordt overgedragen. Zolang dat niet vastligt, is niet vast te stellen wat een aansluitende partij op dit punt moet bouwen. Zie het kader bij 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie.

Deze afhankelijkheid raakt de architectuur dieper dan de andere: de NVI roept al per gevonden Datahoudende Zorgaanbieder de Custodian Server aan. Waar de overige beslissingen worden genomen, bepaalt of daar nog een externe aanroep bij komt.

8.3 Generieke functies Identificatie en Authenticatie

Wat wordt afgenomen

De identiteit van de aansluitende organisatie, waarop de client-registratie steunt. Naar verwachting ook de identiteit waarop de generieke functie Autorisatie haar beslissing baseert; dat hangt af van de kaders die daar worden gesteld.

Grens

De NVI authenticceert de zorgaanbieder, niet de zorgverlener. Of de identiteit van de zorgverlener elders in de keten nodig is, volgt uit het autorisatiemodel en is nog niet bepaald. Zie 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie.

Wat de afspraak moet dekken

De lokalisatiefunctie gaat ervan uit dat een leverancier die namens meerdere zorgaanbieders handelt, per handeling herleidbaar is tot de zorgaanbieder voor wie hij optreedt (zie 5.2.5.1 OAuth 2.0 met centrale clientregistratie voor toegang tot het koppelvlak). Zonder die eigenschap vervalt de grond onder het autorisatiemodel, want dan is achteraf niet vast te stellen wie een vraag stelde.

8.4 Generieke functie Toestemming

Toestemming komt in deze functie op twee verschillende momenten voor, met een verschillende positie in de architectuur. Ze uit elkaar houden voorkomt de verwarring dat de NVI ergens toestemming zou moeten toetsen.

Bij bevraging en raadpleging: onderdeel van autorisatie

De vraag of een zorgverlener gegevens over een patiënt mag opvragen, kan mede afhangen van toestemming. Die vraag wordt niet apart gesteld: zij is een van de gronden waarop de autorisatiebeslissing steunt, en die beslissing is belegd bij de generieke functie Autorisatie. Zie 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie. Of toestemming daarin meeweegt, en op welk van de drie autorisatiepunten, is een van de punten die daar moeten worden vastgesteld.

De lokalisatiefunctie neemt van de generieke functie Toestemming dus niets rechtstreeks af. Wat zij afneemt is de autorisatiebeslissing; of daar toestemming in verwerkt zit, is voor de NVI en de bronhouder niet zichtbaar en hoeft dat ook niet te zijn.

Bij registratie: bij de zorgaanbieder

Of de beschikbaarheid van gegevens wordt geregistreerd, bepaalt de zorgaanbieder die de gegevens houdt. Dat is een afweging in het zorgproces, met de patiënt, en niet een handeling die de NVI kan toetsen: zij ontvangt een registratie en kan niet vaststellen wat eraan voorafging.

De NVI voert daarom geen toestemmingscontrole uit bij registratie. Wat zij wel doet is het mogelijk maken een registratie te verwijderen, zodat een zorgaanbieder een eerdere afweging kan terugdraaien. Zie 5.2.3.2 Wel aanmaken en verwijderen, niet wijzigen.

Uitdrukkelijke toestemming van de patiënt is juridisch niet strikt nodig voor een registratie in de NVI. Zij wordt wel als aanvullende eis gesteld. Of een bestaande toestemming voor dossieruitwisseling ook geldt voor registratie in de NVI, wordt juridisch nog uitgewerkt.

Verwijderverzoeken vanuit de burger

Verwijderen kan alleen door de client die de registratie deed, zie 5.2.3.4 OAuth-client als registrerende partij. Een burger dient het verwijderverzoek in bij de betreffende zorgaanbieder. Deze voert vervolgens de verwijderoperatie in de NVI uit.

Een alternatief wat afgewezen is, is dat de NVI direct zelfstandig burgers gegevens laat verwijderen. Het nadeel hiervan is dat de Datahoudende Zorgaanbieder dan ziet dat het record er niet meer is en het bij de volgende reconciliatie opnieuw aanmeldt, zie 5.2.3.6 Registreren bij de gebeurtenis, reconciliëren als vangnet. Om dit te voorkomen kan bijgehouden worden in de NVI dat een burger dit niet wil - maar dat is qua informatie gelijk aan het record zelf beheren.

De zorgaanbieder dient bij de verwerking van dit verwijderverzoek dus zowel de lokaal geregistreerde gezondheidsdata als ook de in de NVI geregistreerde lokalisatie records te verwijderen. Dit voorkomt herregistratie.

Relatie tot EHDS-blokkeringen

EHDS voorziet in het recht van de burger om toegang tot zijn gegevens te blokkeren. Een blokkering is iets anders dan een verwijdering: zij laat de registratie bestaan maar verhindert dat er gevolg aan wordt gegeven. Waar die blokkering wordt afgedwongen, is een ontwerpvrage op stelselniveau, met drie mogelijkheden die elk andere gevolgen hebben:

- Bij de bronhouder, die niet verstrekt. De registratie blijft dan zichtbaar in de lokalisatie-uitkomst, en de Bevragende Zorgaanbieder ziet dat er gegevens zijn maar krijgt ze niet.
- Bij de autorisatiebeslissing, waarmee de blokkering een grond wordt in het model van de generieke functie Autorisatie. Dit ligt het dichtst bij hoe toestemming bij raadpleging is gepositioneerd.
- Bij de NVI, die de registratie niet teruggeeft. Dit vraagt dat de NVI de blokkering kent, en daarmee iets weet over de betrokken persoon; dat staat op gespannen voet met 5.1.1.2 De NVI kent het BSN niet en 5.1.1.3 Zo min mogelijk gegevens, zo grof mogelijk.

Deze vragen horen bij de generieke functie Toestemming en de generieke functie Autorisatie, niet bij de lokalisatiefunctie. Wat dit document wel vastlegt is dat de derde optie consequenties heeft voor de uitgangspunten van dit ontwerp en niet zonder meer kan worden gekozen.

Huidige situatie en doorkijk naar EHDS

Toestemming is nu decentraal geregeld: bij de zorgaanbieder, al dan niet via Mitz. De NVI kent de patiënt niet en kan toestemming dus niet zelf toetsen. Daarom ligt de toets nu bij de Datahoudende Zorgaanbieder, in de Custodian Server. Dit is een tijdelijke situatie.

Die situatie heeft twee nadelen. Ten eerste wordt toestemming meerdere keren getoetst: bij de Custodian Server tijdens het lokaliseren, en opnieuw bij het ophalen van de gegevens. Ten tweede leert de Datahoudende Zorgaanbieder wie er zoekt voordat de toets is gedaan, omdat zij die identiteit nodig heeft om toestemming te toetsen. Een deel van de behandelrelatie is dan zichtbaar voordat vaststaat dat er toestemming is.

Onder de EHDS komt er een centraal zeggenschapsregister. Uiterlijk maart 2029 moeten het recht op beperking en de opt-out werken. Zodra dat register er is, kan de toestemmingstoets naar de voorkant van de keten: vóór de zoekvraag, in plaats van bij de bron. Wie het zeggenschapsregister invult, is nog niet besloten. Het uitgangspunt is dat ook dat register met pseudoniemen werkt, via de PRS.

9 Referenties

Standaarden, specificaties en documenten waarnaar dit document verwijst. De kolom Type geeft aan wat de status is: een standaard of kader is extern en kaderstellend, een specificatie is normatief voor de bouw, een document beschrijft een ander deel van hetzelfde ontwerp.

Titel	Type	Verwijzing
HL7 FHIR R4	standaard	https://hl7.org/fhir/R4/
RFC 9497 (OPRF)	standaard	https://datatracker.ietf.org/doc/rfc9497
Baseline Informatiebeveiliging Overheid	standaard	https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/bio-en-ensia/baseline-informatiebeveiliging-overheid/
EU Aanbeveling 2019/243	kader	https://eur-lex.europa.eu/eli/reco/2019/243/oj
Netherlands - Generic Functions for data exchange Implementation Guide, Localization	specificatie	https://minvws.github.io/generiekefuncties-docs/localization.html
Netherlands - Generic Functions for data exchange Implementation Guide, Pseudonymisation	specificatie	https://minvws.github.io/generiekefuncties-docs/pseudonymisation.html
Netherlands - Generic Functions for data exchange Implementation Guide, section Localization, Care Services Directory	specificatie	https://minvws.github.io/generiekefuncties-docs/care-services.html

Appendix A. Besluitonderbouwingen

A.1 De tussenoplossing voor autorisatie van de Bevragende Zorgaanbieder

Behoort bij 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie. Autorisatie van handelingen is belegd bij de generieke functie Autorisatie, maar die heeft daar nog geen kaders voor gesteld. Deze appendix beschrijft wat er voor de toets bij de Bevragende Zorgaanbieder geldt zolang die kaders ontbreken, en waarom dat verdedigbaar is als tussenoplossing. De beslissing van de Datahoudende Zorgaanbieder over vermelding in het antwoord staat in 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord.

Tussenoplossing

Elke aangesloten zorgaanbieder mag elke vraag stellen. De NVI toetst dat de Localization Search Client is geauthenticeerd en voor de betreffende rol is geregistreerd, en toetst niet of er voor deze specifieke vraag een grondslag bestaat. Wel beslist elke gevonden Datahoudende Zorgaanbieder of zij in het

antwoord vermeld wordt, zie 5.2.5.3 Datahoudende Zorgaanbieder beslist over vermelding in het antwoord. Misbruik door de Bevragende Zorgaanbieder wordt achteraf gedetecteerd.

Dit is niet het beoogde eindbeeld. Zodra de generieke functie Autorisatie kaders stelt, vervangt dat de tussenoplossing.

Wat de NVI niet kan toetsen

De NVI zou drie dingen moeten weten om de rechtmatigheid van een vraag te beoordelen: wie de zorgverlener is, om welke patiënt het gaat, en of er tussen die twee een behandelrelatie bestaat.

Het eerste weet zij niet: autorisatie vindt plaats op organisatieniveau en de identiteit van de zorgverlener blijft bij de Bevragende Zorgaanbieder. Het tweede weet zij niet: de pseudonimisering zorgt er juist voor dat zij dat niet weet. Het derde volgt uit de eerste twee.

Een toets vooraf zou dus berusten op gegevens die de NVI niet heeft. Zij zou de verklaring van de afnemer moeten aannemen, en die verklaring toetsen betekent hem herhalen.

Waarom dit verdedigbaar is

Lokaliseren geeft geen toegang tot gegevens. Het antwoord is een lijst bronhouders; wie die lijst heeft, heeft nog niets gezien. De bronhouder beslist zelf over vermelding in het antwoord en over verstrekking, en die beschikt wel over de behandelrelatie.

De NVI is dus niet het enige controlepunt in de keten, en ook niet het punt waar de inhoudelijke afweging thuishoort. Zij is het punt waar de handeling herleidbaar wordt vastgelegd.

Ook in deze tussenoplossing geldt dat de Bevragende Zorgaanbieder de enige partij is die de zorgverlener en de patiënt tegelijk kent. Dat zij die afweging maakt is hier echter een aanname en geen afdwingbare eis: er is geen kader dat vastlegt waarop zij toetst, en voor de NVI en de bronhouder is niet zichtbaar of het is gebeurd. Dat is precies wat de generieke functie Autorisatie moet invullen, zie 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie.

Wat dat vraagt

Het model verplaatst de waarborg van preventie naar detectie. Dat werkt alleen onder drie voorwaarden:

- Herleidbaarheid. Elke vraag is te herleiden tot organisatie en client. Zie 5.2.5.1 OAuth 2.0 met centrale clientregistratie voor toegang tot het koppelvlak.
- Detectie. Er wordt actief gemonitord op afwijkende patronen. Zonder monitoring is er geen detectie en dus geen waarborg.
- Consequenties. Geconstateerd misbruik heeft gevolgen. Zonder consequenties is detectie een registratie zonder werking.

De derde voorwaarde ligt buiten de techniek en buiten dit document, maar zonder die voorwaarde is de keuze niet houdbaar.

Geaccepteerde prijs

Een Bevragende Zorgaanbieder kan een vraag stellen waarvoor geen grond bestaat, en dat wordt pas achteraf zichtbaar. Aanvaard omdat het alternatief, een toets op gegevens die de NVI niet heeft, schijnzekerheid geeft en de pseudonimisering zou moeten opgeven.

Vervanging

Deze tussenoplossing vervalt zodra de generieke functie Autorisatie kaders stelt. Dat is geen mogelijkheid maar een verwachting: het model zoals hier beschreven is niet bedoeld als eindsituatie.

De vervanging raakt de rest van de architectuur niet. Toegang tot het koppelvak en autorisatie van vragen zijn gescheiden (5.2.5.1 OAuth 2.0 met centrale client-registratie voor toegang tot het koppelvak en 5.2.5.2 Autorisatie belegd bij generieke functie Autorisatie), zodat een autorisatiemodel kan worden toegevoegd zonder het functionele koppelvak te wijzigen. Wat blijft gelden ongeacht het model is de eis van herleidbaarheid, zie 5.2.5.1 OAuth 2.0 met centrale clientregistratie voor toegang tot het koppelvak.

A.2 Topologie: Gecentraliseerde verwijzindex

Bij de keuze voor een topologie voor de generieke functie Lokalisatie zijn de volgende aspecten meegewogen:

1. Patiëntveiligheid
2. Beschikbaarheid
3. Privacy: lekken van behandelrelaties
4. Privacy: rolvastheid AVG
5. Afhankelijkheden per zorgaanbieder
6. Change management
7. Governance
8. Security: concentratie van gegevens en risico
9. Privacy: concentratie van gegevens

Patiëntveiligheid

In het kader van patiëntveiligheid moet een zorgverlener kunnen vertrouwen op een volledig beeld (voor zover toestemming dit toelaat), of weten dat het beeld niet volledig beschikbaar is. In een federatief model kan een storing bij één index leiden tot een gedeeltelijk resultaat dat er onterecht uitziet als een volledig beeld. Informatie die ontbreekt vanwege een storing in een index kan dan onterecht worden aangezien voor informatie die er niet is.

Als een volledige zoekactie alle n decentrale indexen nodig heeft, en de beschikbaarheid van elke index A is, dan is de kans dat alle indexen beschikbaar zijn A^n (bij onafhankelijke storingen). Bij een centrale voorziening met beschikbaarheid A is de totale beschikbaarheid A . Bijvoorbeeld: bij $A = 99,9\%$ en $n = 10$ is de centrale beschikbaarheid $99,9\%$, tegenover ongeveer $99,0\%$ voor een zoekactie die alle tien decentrale indexen nodig heeft.

In een model waarbij data bij de bron blijft moet er rekening gehouden worden met een combinatie van SAAS (meerdere zorgaanbieders in een centraal systeem) en on-site installaties. Een schatting (die mogelijk hoger dan wel lager kan zijn) brengt het aantal systemen op 100. Dit heeft dan al snel gevolgen voor de totale beschikbaarheid.

Omdat vooraf niet duidelijk is bij welke indexen een patiënt bekend is zal dat daarmee regelmatig consequenties hebben voor de duidelijkheid bij de zorgverlener.

Privacy: lekken van behandelrelaties

Tenzij dit wettelijk en technisch goed is geregeld, kan een federatieve zoekactie neerkomen op een broadcast naar meerdere bronnen. Ook bronnen die geen relevante informatie over de patiënt hebben, ontvangen dan gegevens over de Bevragende Zorgaanbieder en de patiënt. Uit het verzoek blijkt dat de Bevragende Zorgaanbieder betrokken is bij de zorg voor die patiënt. Zo kan de behandelrelatie bekend worden bij partijen die daar geen rol in hebben.

Dit hangt samen met de juridische status van een index. In een strikt decentraal model is een leverancier (ook SAAS) een verwerker. De impact hiervan kan via pseudoniemen (deels) technisch gemitigeerd worden; maar vereist ook juridische onderbouwing en governance.

Afhankelijkheden per zorgaanbieder

Leveranciers kunnen de index dienst als onderdeel van het EPD systeem leveren. Dit is voordelig voor het realiseren van data bij de bron. Wel betekent dit dat een zorgaanbieder daarmee afhankelijk wordt van meerdere indexdiensten, elk met eigen aansluiting, beheer, monitoring, beschikbaarheid, storingsmeldingen, contracten en wijzigingsplanning. Dat vergroot de beheerlast en maakt het lastiger om bij een storing vast te stellen waar de oorzaak ligt en of het zoekresultaat volledig is. Zie ook het eerdere punt over patiëntveiligheid.

Change management

Wijzigingen in gegevensmodel, beveiliging of interface moeten met meerdere indexbeheerders worden afgestemd en in verschillende combinaties worden getest. Verschillen in tempo of implementatie kunnen leiden tot tijdelijke incompatibiliteit, afwijkend gedrag of vertraging.

Governance

Bij meerdere indexen moet worden geregeld wie indexen mag beheren, aan welke eisen ze moeten voldoen en hoe toezicht, wijzigingen en incidenten worden afgehandeld. Ook moeten indexen worden geregistreerd en moet voor zorgaanbieders duidelijk zijn bij welke indexen zij moeten aansluiten. Dat vraagt om afspraken over toelating, kwaliteit, beveiliging, interoperabiliteit en vindbaarheid, plus beheer, financiering en duidelijke verantwoordelijkheden. Zeker ook het prestatie vraagstuk maakt dit extra ingewikkeld. De snelheid van lokalisatie wordt bepaald door de traagste index. Prestatieproblemen spelen breed in de zorginfrastructuur, het is dan ook onduidelijk hoe dit adequaat gemanaged kan/ zal worden.

Security: concentratie van gegevens en risico

Een centrale voorziening kan security-risico's vergroten: door de concentratie van gegevens kan een incident een grotere impact hebben. De afweging is tussen volledigheid en beheersbaarheid voor patiëntveiligheid enerzijds, en concentratie van gegevens en risico anderzijds.

Privacy: concentratie van gegevens

Een centrale voorziening kan privacy-risico's vergroten: één partij krijgt mogelijk meer inzicht in zoekgedrag. De afweging is tussen volledigheid en beheersbaarheid voor patiëntveiligheid enerzijds, en concentratie van gegevens, macht en risico anderzijds.

Conclusie

Op basis van een weging van bovenstaande punten is door VWS gekozen voor een centrale inrichting. Hierbij is voor security en privacy borging geïnvesteerd in maatregelen als pseudonimisering via technieken die dataminimalisatie toepassen, best practises voor versleuteling en defence in depth (waaronder hardware security modules) zodat ook de beheerders van de index geen inhoudelijke kennis krijgen van de (eerdere) behandelrelaties in de index.

Appendix B. Bronvermeldingen

De inhoud van dit document is gebaseerd op:

Bron	Wat daaruit is overgenomen
Functioneel ontwerp generieke functie Lokalisatie, deel A en B	Use cases, functionele requirements, informatiemodel, begrippen
Technisch Ontwerp NVI	Componenten, besluiten NVI-DEC-003 tot en met NVI-DEC-016, functies
Technisch Ontwerp PRS	Werking van het pseudonimiseringsmechanisme
NL Generic Functions Implementation Guide	Profielen en transacties
Technisch Ontwerp generieke functie Adressering	Documentstructuur en de opbouw van architectuurkeuzes