



Ministerie van Volksgezondheid,
Welzijn en Sport

Functioneel Ontwerp

Generieke Functie Lokalisatie

Versie 0.9.0

Inhoudsopgave

1	1	Documenthistorie.....	5
2	2.	Leeswijzer.....	6
3		Deel A: Functioneel ontwerp generieke functie Lokalisatie	7
4	3.	Inleiding en samenhang	7
5	3.1.	Doel.....	7
6	3.2.	Doelgroep van dit document.....	7
7	3.3.	Samenhang generieke functies	8
8	3.4.	Scope	11
9	4.	Stakeholders en rollen	12
10	5.	Hoofdproces en usecases	14
11	5.1.	UC-GFL-01: Registreren lokalisatie-record	14
12	5.2.	UC-GFL-02: Opvragen lokalisatie-records.....	15
13	5.3.	UC-GFL-03: Opvragen van eigen lokalisatie-records	17
14	5.4.	UC-GFL-04: Verwijderen van lokalisatie-records.....	18
15	6.	Juridisch kader	20
16	6.1.	Relevante wet- en regelgeving	20
17	6.2.	Doorontwikkeling	23
18	7.	Requirements.....	23
19	7.1.	Registreren en beheren van lokalisatiegegevens.....	23
20	7.2.	Opvragen lokalisatie-records.....	23
21	8.	Gebruikersinteractie	23
22	8.1.	Huisartsenpraktijk maakt data vindbaar via de NVI	24
23	8.2.	Arts vraagt patiënt-samenvatting op	25
24	9.	Informatiemodellen	27
25	9.1.	Lokalisatie-record	27
26	9.2.	Lokalisatievraag	28
27	10.	Beveiliging	30
28		Deel B (informatief): Componenten	31
29	11.	Nationale Verwijsindex (NVI).....	31
30	11.1.	Rol en doel.....	31
31	11.2.	Stakeholders	32
32	11.3.	Usecases	33
33	11.4.	Requirements applicatielaag- en IT-infrastructuurlaag.....	37
34	11.5.	Data/gegevens.....	38
35	11.6.	Gedrag en randgevallen	38

36	11.7.	Beheer, verantwoordelijkheden en verwijzingen	39
37	12.	Pseudoniemenregistratieservice (PRS)	39
38	12.1.	Rol en doel.....	39
39	12.2.	Stakeholders en hun belang	40
40	12.3.	usecases.....	40
41	12.4.	Requirements applicatielaag- en IT-infrastructuurlaag.....	41
42	12.5.	Data/gegevens.....	41
43	12.6.	Gedrag en randgevallen	41
44	12.7.	Beheer, verantwoordelijkheden en verwijzingen	42
45	13.	Localization Registration Client.....	42
46	13.1.	Rol en doel.....	42
47	13.2.	Stakeholders en hun belang	42
48	13.3.	Usecases	42
49	13.4.	Requirements applicatielaag- en IT-infrastructuurlaag.....	43
50	13.5.	Data/gegevens.....	43
51	13.6.	Gedrag en randgevallen	43
52	13.7.	Beheer, verantwoordelijkheden en verwijzingen	43
53	14.	Localization Search Client	44
54	14.1.	Rol en doel.....	44
55	14.2.	Stakeholders en hun belang	44
56	14.3.	Usecases	44
57	14.4.	Requirements applicatielaag- en IT-infrastructuurlaag.....	45
58	14.5.	Data/gegevens.....	45
59	14.6.	Gedrag en randgevallen	45
60	14.7.	Beheer, verantwoordelijkheden en verwijzingen	47
61	15.	Custodian server	47
62	15.1.	Rol en doel.....	47
63	15.2.	Stakeholders en rollen.....	47
64	15.3.	Usecases	48
65	15.4.	Requirements applicatielaag- en IT-infrastructuurlaag.....	48
66	15.5.	Data	48
67	15.6.	Gedrag en randvoorwaarden	48
68	15.7.	Beheer, verantwoordelijkheden en verwijzingen	48
69	16.	LMR (optioneel)	48
70	Bijlage 1:	Requirements	50
71		Functionele requirements	50
72		Gerealiseerde functionele requirements.....	50
73		Niet-gerealiseerde functionele requirements	50

74	Niet-functionele requirements	51
75	Bijlage 2: Definities	53

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 commentaren van DA

2. Leeswijzer

Dit document bestaat uit 2 delen:

- Deel A bevat het Functioneel Ontwerp van de generieke functie Lokalisatie.
- Deel B is informatief en bevat samenvattingen van de functionele ontwerpen van de verschillende componenten die zijn gerelateerd aan de realisatie van de generieke functie Lokalisatie:
 - de NVI;
 - de PRS;
 - de Localization Registration Client;
 - de Localization Search Client;
 - de Custodian server; en
 - het LMR (optioneel).

De structuur van deel A en deel B is geïnspireerd door het [Nictiz Lagenmodel](#).

Deel A: Functioneel ontwerp generieke functie Lokalisatie

3. Inleiding en samenhang

De generieke functie Lokalisatie maakt inzichtelijk welke zorgaanbieders beschikken over relevante gezondheidsdata over een burger. Hierdoor kunnen eindgebruikers zoals zorgverleners gericht bepalen waar relevante gezondheidsdata beschikbaar zijn. Dit document beschrijft de functionele werking.

De realisatie van de generieke functie Lokalisatie is onderdeel van het programma Landelijk Dekkend Netwerk (vanaf hier “programma LDN”) dat onder regie van het Ministerie van VWS wordt uitgevoerd. De generieke functie Lokalisatie speelt een cruciale rol in het faciliteren van elektronische gegevensuitwisseling in de zorg, zoals vastgelegd in de Wet elektronische gegevensuitwisseling in de zorg (Wegiz).

De generieke functie Lokalisatie werkt samen met andere generieke functies. Zo wordt de generieke functie Lokalisatie in een elektronische gegevensuitwisseling aangevuld met de generieke functie Adressering. De generieke functie Lokalisatie maakt inzichtelijk welke zorgaanbieders beschikken over relevante gegevens over een bepaalde burger. De generieke functie Adressering maakt inzichtelijk via welke technische adressen deze gegevens kunnen worden benaderd. Paragraaf 3.2 beschrijft de relatie tussen de generieke functie Lokalisatie en de andere generieke functies.

3.1. Doel

Het gezondheidsinformatiestelsel (GIS) streeft ernaar dat gezondheidsdata over grenzen van organisaties, domeinen en landen kunnen worden gedeeld. Dat streven, ook wel aangeduid met “databeschikbaarheid”, vereist dat het systeem van een zorgverlener met een databehoeftte weet welke zorgaanbieders beschikken over relevante data over een bepaalde burger. Het doel van de generieke functie Lokalisatie is dat het systeem van een zorgaanbieder eenvoudig en veilig kan bepalen welke zorgaanbieders beschikken over relevante data over een burger. De generieke functie Lokalisatie biedt daarmee een van de onderdelen die nodig zijn om zorgverleners in staat te stellen relevante gegevens gericht op te vragen. Zonder generieke functie Lokalisatie ontbreekt een eenduidige oplossing voor het kunnen bepalen welke zorgaanbieders beschikken over relevante gegevens over een burger: zorgaanbieders onderhouden eigen lijsten of gebruiken systeem-, regio- of infrastructuur-specifieke oplossingen die onvoldoende op elkaar aansluiten. Door lokalisatie als generieke functie in te richten worden de kosten van naast elkaar bestaande specifieke oplossingen en de kosten van het beheer van eigen lijsten verlaagd: Zorgaanbieders sluiten op één generieke manier aan en relevante gegevens over een burger zijn, binnen de kaders van wet- en regelgeving, voor zorgverleners vindbaar.

3.2. Doelgroep van dit document

Dit document beschrijft de functionaliteit en gaat bewust niet in op technische details. Waar nodig wordt verwezen naar het technisch ontwerp en de Implementation Guide. Dit functioneel ontwerp is bedoeld voor de volgende doelgroepen:

- Zorgaanbieders en hun functioneel beheerders, om inzicht te krijgen in de werking van de generieke functie Lokalisatie en wat er van hen wordt verwacht bij het inrichten en beheren.
- IT-dienstverleners, ter voorbereiding op aansluiting, implementatie en beheer.
- Architecten en technisch ontwerpers, als uitgangspunt voor het opstellen van het technisch ontwerp en de technische specificaties van de generieke functie Lokalisatie.

- Beleidsmedewerkers, ter toetsing aan beleidskaders
- Beheerders van voorzieningen die onderdeel zijn van de generieke functie Lokalisatie (NVI en PRS).

3.3.Samenhang generieke functies

Lokalisatie is een van de zes geprioriteerde generieke functies. In onderstaande tabel worden de generieke functies omschreven. Voor het realiseren van landelijke elektronische gegevensuitwisseling is een combinatie van meerdere generieke functies nodig.

Generieke functie	Omschrijving
Identificatie & Authenticatie	<p>De generieke functies Identificatie en Authenticatie zorgen ervoor dat de identiteit van een zorgprofessional, organisatie of systeem digitaal kan worden vastgesteld en gecontroleerd. Dit is een essentieel onderdeel in het realiseren van vertrouwen tussen partijen die gegevens met elkaar uitwisselen.</p> <p><i>Relatie tot de generieke functie Lokalisatie:</i></p> <ul style="list-style-type: none"> - De generieke functie Lokalisatie bevat een component NVI (meer informatie over deze component is opgenomen in hoofdstuk 11). Toegang tot het NVI vereist de identificatie en authenticatie van zorgaanbieders en IT-dienstverleners. Dit dient te worden uitgevoerd in lijn met de generieke functies Identificatie en Authenticatie. - De zorgaanbieder-identificer die via de generieke functie Lokalisatie beschikbaar wordt gesteld is onderdeel van de identiteit van zorgaanbieders. De identiteit van zorgaanbieders wordt nader gespecificeerd in de generieke functie Identificatie. - Voordat de NVI aan een Bevragende Zorgaanbieder (meer informatie over deze rol is opgenomen in hoofdstuk 4) lokalisatie-records oplevert, vraagt de NVI aan iedere Datahoudende Zorgaanbieder (meer informatie over deze rol is opgenomen in hoofdstuk 4) om een akkoord voor het delen van die lokalisatie-records. Deze actie vereist de identificatie en authenticatie van de NVI door de Datahoudende Zorgaanbieder. Dit dient te worden uitgevoerd in lijn met de generieke functies Identificatie en Authenticatie. Met de generieke functie Lokalisatie kunnen Datahoudende Zorgaanbieders worden gelokaliseerd. Wanneer met een gelokaliseerde zorgaanbieder een elektronische gegevensuitwisseling wordt geïnitieerd, dienen identificatie en authenticatie te worden uitgevoerd. Dit dient te worden uitgevoerd in lijn met de generieke functies Identificatie en Authenticatie. - De generieke functies Identificatie en Authenticatie zijn nog in ontwikkeling. Bij de totstandkoming van (de componenten van) de generieke functie Lokalisatie wordt hiermee rekening gehouden.
Autorisatie	De generieke functie Autorisatie bepaalt welke gegevens een persoon, systeem of organisatie mag bekijken, gebruiken of wijzigen. De functie zorgt

	<p>ervoor dat toegang aansluit bij de rol, verantwoordelijkheid en betrokkenheid van een persoon, systeem of organisatie.</p> <p><i>Relatie tot de generieke functie Lokalisatie:</i></p> <ul style="list-style-type: none"> - Met de generieke functie Lokalisatie kunnen Datahoudende Zorgaanbieders (zie hoofdstuk 4) worden gelokaliseerd. Wanneer met een gelokaliseerde zorgaanbieder een elektronische gegevensuitwisseling wordt geïnitieerd, dient autorisatie te worden uitgevoerd. De generieke functie Autorisatie is nog in ontwikkeling. Daarom vindt autorisatie momenteel nog niet conform landelijke afspraken en specificaties plaats. - De generieke functie Lokalisatie bevat een component NVI (zie hoofdstuk 11). Toegang tot de NVI vereist de autorisatie van zorgaanbieders en IT-dienstverleners. Dit dient te worden uitgevoerd in lijn met de generieke functie Autorisatie. - Voordat de NVI aan een Bevragende Zorgaanbieder (zie hoofdstuk 4) lokalisatie-records oplevert, vraagt de NVI aan iedere Datahoudende Zorgaanbieder om een akkoord voor het delen van die lokalisatie-records. Deze actie vereist de autorisatie van de NVI door de Datahoudende Zorgaanbieder. Dit dient te worden uitgevoerd in lijn met de generieke functie Autorisatie. - De generieke functie Autorisatie is nog in ontwikkeling. Bij de totstandkoming van (de componenten van) de generieke functie Lokalisatie wordt hiermee rekening gehouden.
Toestemming	<p>De generieke functie Toestemming legt vast welke keuzes een burger maakt over het delen en gebruiken van gezondheidsgegevens en maakt deze keuzes inzichtelijk. Hierdoor weten zorgverleners welke informatie beschikbaar mag worden gesteld en onder welke voorwaarden.</p> <p><i>Relatie tot de generieke functie Lokalisatie:</i></p> <ul style="list-style-type: none"> - De generieke functie Lokalisatie bevat een component NVI (zie hoofdstuk 11). Datahoudende Zorgaanbieders (zie hoofdstuk 4) mogen alleen lokalisatie-records over een burger in de NVI registreren indien de burger daarvoor uitdrukkelijke toestemming heeft gegeven. - Voordat de NVI aan een Bevragende Zorgaanbieder (zie hoofdstuk 4) lokalisatie-records oplevert, vraagt de NVI aan iedere Datahoudende Zorgaanbieder om een akkoord voor het delen van die lokalisatie-records. Om te bepalen of dat akkoord kan worden gegeven, toetst de Datahoudende Zorgaanbieder of er een grondslag en/of beperking van toepassing is. De grondslag en/of de beperking dienen te zijn gebaseerd op de generieke functie Toestemming. - De generieke functie Toestemming is nog in ontwikkeling. Bij de totstandkoming van (de componenten van) de generieke functie Lokalisatie wordt hiermee rekening gehouden.
Lokalisatie	<p>De generieke functie Lokalisatie maakt inzichtelijk welke zorgaanbieders beschikken over relevante gegevens over een burger waarop wel een grondslag en geen beperking van toepassing is. Hierdoor kunnen zorgverleners en zorgtoepassingen gericht bepalen waar informatie</p>

	<p>beschikbaar is.</p> <p><i>Relatie tot de generieke functie Lokalisatie:</i></p> <ul style="list-style-type: none"> - n.v.t.
Adressering	<p>De generieke functie Adressering maakt het mogelijk om digitale en fysieke adressen, organisatieonderdelen en zorgdiensten van zorgaanbieders op een gestandaardiseerde wijze te registreren, beheren en raadplegen.</p> <p><i>Relatie tot de generieke functie Lokalisatie:</i></p> <ul style="list-style-type: none"> - De generieke functie Lokalisatie maakt inzichtelijk welke Datahoudende Zorgaanbieders (zie hoofdstuk 4) beschikken over relevante gegevens over een burger en bereid zijn dit feit kenbaar te maken aan de Bevragende Zorgaanbieder (zie hoofdstuk 4). De generieke functie Adressering maakt voor ieder van deze Datahoudende Zorgaanbieders inzichtelijk hoe zij kunnen worden bereikt. - Bij een bevraging van de NVI (zie hoofdstuk 11) moet een zoekcontext (zie hoofdstuk 9) worden meegegeven. De zoekcontext bestaat uit eigenschappen van Datahoudende Zorgaanbieders die voor de context van de Bevragende Zorgaanbieder relevant zijn. Data over veel van deze eigenschappen van zorgaanbieders worden beschikbaar gemaakt door middel van de generieke functie Adressering.
Logging	<p>De generieke functie Logging legt vast welke acties plaatsvinden rondom gezondheidsdata. Denk aan wie gegevens heeft geraadpleegd, wanneer dat gebeurde, vanuit welke organisatie en met welk doel of welke aanleiding.</p> <p><i>Relatie tot de generieke functie Lokalisatie:</i></p> <ul style="list-style-type: none"> - Iedere Datahoudende Zorgaanbieder en Bevragende Zorgaanbieder (zie hoofdstuk 4) houdt conform de generieke functie Logging loggegevens bij. De generieke functie Logging bevat een component om burgers inzicht te geven in loggegevens. Deze component maakt gebruik van de generieke functie Lokalisatie om de loggegevens per zorgaanbieder te raadplegen. Daarnaast zal deze component van de generieke functie Logging loggegevens van de component NVI (zie hoofdstuk 11) van de generieke functie Lokalisatie raadplegen. Op deze manier kan de generieke functie Logging inzicht geven in de organisaties die betrokken zijn geweest bij acties rondom gezondheidsdata over een specifieke burger. - Waar van toepassing dienen interacties in het kader van de generieke functie Lokalisatie te voldoen aan de afspraken en specificaties van de generieke functie Logging. - De generieke functie Logging is nog in ontwikkeling. Bij de totstandkoming van (de componenten van) de generieke functie Lokalisatie wordt hiermee rekening gehouden.



Figuur 1: Positie Lokalisatie binnen het stelsel van generieke functies

3.4.Scope

De documentatie over de generieke functie Lokalisatie is verdeeld over drie documenten:

- Functioneel ontwerp
- Technisch ontwerp
- Implementation Guide

Ieder document beschrijft de werking van de generieke functie Adressering op een ander abstractieniveau. Onderstaande tabel maakt expliciet wat ieder document beschrijft en wat niet in de documentatie is opgenomen.

Document	Beschrijft	Bevat bewust niet
FO Lokalisatie (dit document)	Het achterliggende probleem en het doel, de rollen en stakeholders, het juridisch kader, de usecases, de functionele requirements, de gebruikersinteractie en het informatiemodel van de generieke functie Lokalisatie en de hieraan gerelateerde componenten zoals NVI en PRS.	Protocolkeuzes, berichtformaten, veldnamen en technische foutafhandeling.
TO Lokalisatie	Technische uitwerking van dit FO: architectuur, onderbouwingen van keuzes voor koppelvlakken en standaarden, de technische uitwerking van beveiliging, eisen aan beheer en beschikbaarheid.	Leveranciersspecifieke implementatiekeuzes en de inrichting van schermen in het eigen systeem, datamodel (zie IG).
Implementation Guide (IG)	Gedetailleerde technische uitwerking van FO en TO geschikt voor realisatie in systemen: datamodellen, waardelijsten, interacties, beveiliging en authenticatie.	De functionele motivatie en de beleidskaders; die staan in dit FO. De motivatie van technische keuzes, die is onderdeel van het TO.
Buiten scope van alle drie	De interne werking van de verschillende componenten die in	-

	het ontwerp van lokalisatie worden onderkend	
--	--	--

159

160 4. Stakeholders en rollen

161 De generieke functie Lokalisatie heeft voornamelijk als doel om zorgverleners een snelle en veilige
 162 manier te bieden om te achterhalen welke zorgaanbieders over relevante gegevens over een burger
 163 beschikken. Naast de zorgverlener zijn er ook andere stakeholders. Onderstaand overzicht bevat de
 164 belangrijkste stakeholders, hun rol en hun belang bij de generieke functie Autorisatie. Ter herkenning
 165 worden rollen in dit document geschreven met een hoofdletter.

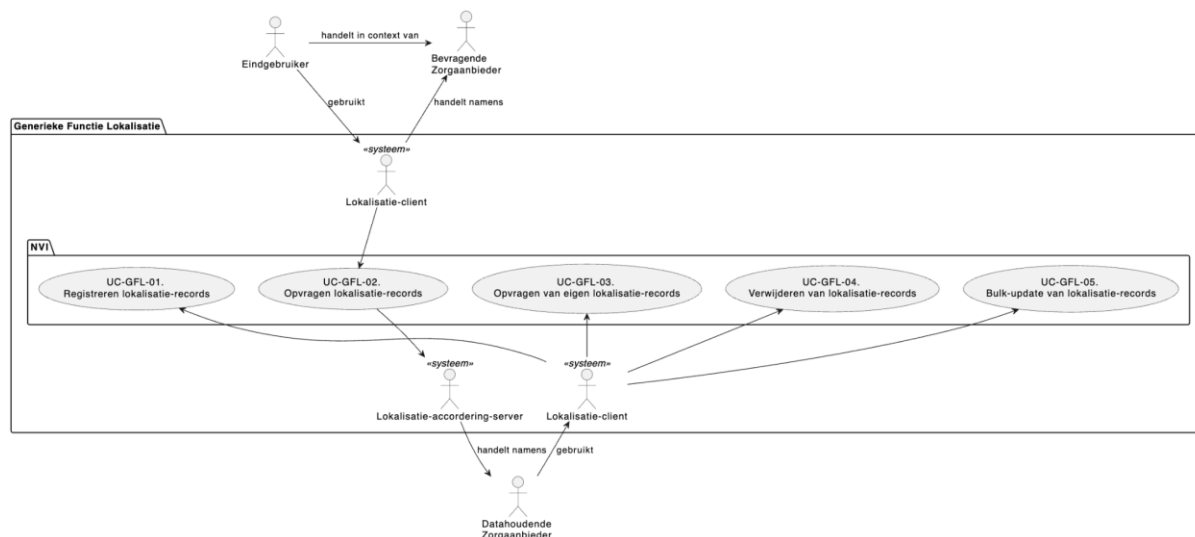
166

Stakeholder	Rol	Belang
Burger	Betrokkene	<ul style="list-style-type: none"> - Gezondheidsdata over Betrokkene zijn vindbaar voor de eigen behandeling, terwijl het BSN niet in de NVI voorkomt. Omwille van de leesbaarheid wordt in dit document de term BSN gebruikt, hier kan ook V-nummer (Vreemdelingennummer) worden gelezen. - Betrokkene heeft belang bij inzage in wie haar/zijn gegevens heeft gelokaliseerd - Betrokkene heeft belang bij het respecteren van door haar of hem gemaakte keuzes over het delen van gegevens.
Zorgverlener	Eindgebruiker	De Eindgebruiker wil relevante gegevens over Betrokkenen inzien, ook wanneer deze data zijn verdeeld over meerdere vooraf onbekende Datahoudende Zorgaanbieders. De Eindgebruiker maakt daartoe gebruik van een systeem dat op basis van de generieke functie Lokalisatie relevante gegevens over Betrokkenen lokaliseert. De Eindgebruiker handelt binnen de context van de Bevragende Zorgaanbieder. Het systeem dat de Eindgebruiker gebruikt voor lokalisatie, handelt namens de Bevragende Zorgaanbieder.
Zorgaanbieder (Bronhouder)	Datahoudende Zorgaanbieder	De Datahoudende Zorgaanbieder maakt gegevens vindbaar door het registreren en beheren van lokalisatiegegevens conform de afspraken van de generieke functie Lokalisatie. De Datahoudende Zorgaanbieder maakt daartoe gebruik van een systeem dat voldoet aan de afspraken en specificaties van de generieke functie Lokalisatie.

Stakeholder	Rol	Belang
Zorgaanbieder (Bevragend)	Bevragende Zorgaanbieder	De Eindgebruiker wil relevante gegevens over Betrokkenen inzien, ook wanneer deze data zijn verdeeld over meerdere vooraf onbekende Datahoudende Zorgaanbieders. De Eindgebruiker maakt daartoe gebruik van een systeem dat op basis van de generieke functie Lokalisatie relevante gegevens over Betrokkenen lokaliseert. De Eindgebruiker handelt binnen de context van de Bevragende Zorgaanbieder. Het systeem dat de Eindgebruiker gebruikt voor lokalisatie, handelt namens de Bevragende Zorgaanbieder.
IT-dienstverlener	Dienstverlener Localization-Registration- Client	De Dienstverlener Localization-Registration-Client implementeert ten dienste van de rol Datahoudende Zorgaanbieder de afspraken en specificaties van de generieke functie Lokalisatie in het algemeen en de component Localization Registration Client (zie hoofdstuk 13) in het bijzonder.
IT-dienstverlener	Dienstverlener Localization-Search-Client	De Dienstverlener Localization-Search-Client implementeert ten dienste van de rollen Bevragende Zorgaanbieder en Eindgebruiker de afspraken en specificaties van de generieke functie Lokalisatie in het algemeen en de component Localization Search Client (zie hoofdstuk 14) in het bijzonder.
IT-dienstverlener	Dienstverlener Custodian-Server	De Dienstverlener Custodian-Server implementeert ten dienste van de rol Datahoudende Zorgaanbieder de afspraken en specificaties van de generieke functie Lokalisatie in het algemeen en de Custodian Server (zie hoofdstuk 15) in het bijzonder.
Beheerorganisatie NVI	Dienstverlener NVI	Verantwoordelijk voor het beheer van de Nationale Verwijsindex (NVI), een component dat vereist is voor de realisatie van de generieke functie Lokalisatie.
Beheerorganisatie PRS	Dienstverlener PRS	Verantwoordelijk voor het beheer van de Pseudoniemenregistratieservice (PRS), een component dat benodigd is voor de realisatie van de generieke functie Lokalisatie.
VWS (opdrachtgever)	Beleidsverantwoordelijke	Bewaakt en/of stelt kaders, bewaakt voortgang en borgt aansluiting bij het programma LDN, de Wegiz en de verordening EHDS.

5. Hoofdproces en usecases

De generieke functie Lokalisatie omvat verschillende usecases voor inrichting en gebruik. De usecases voor gebruik zijn opgenomen in dit hoofdstuk. De usecases voor inrichting zijn opgenomen in deel B van dit document. Hieronder is een schematische weergave van de verhoudingen en een beschrijving per usecase opgenomen.



5.1.UC-GFL-01: Registreren lokalisatie-record

Een Datahoudende Zorgaanbieder (zie hoofdstuk 4) kan gezondheidsdata over een specifieke Betrokkene (zie hoofdstuk 4) vindbaar maken door een lokalisatie-record te registreren in de component NVI van de generieke functie Lokalisatie (NVI). Een samenvatting van het functioneel ontwerp van de component NVI is opgenomen in hoofdstuk 10. Nationale Verwijsindex (NVI). Het registreren van een lokalisatie-record vindt plaats aan de hand van:

- een pseudoniem van het BSN van de Betrokkene;
- de URA van de Datahoudende Zorgaanbieder; en
- de identifier van het systeem dat de data beschikbaar stelt.

Het registreren van een lokalisatie-record wordt geïnitieerd door een systeem dat de component Localization Registration Client heeft geïmplementeerd. Een samenvatting van het functioneel ontwerp van de component Localization Registration Client is opgenomen in hoofdstuk 13.

In de communicatie met de NVI dienen BSN's te zijn gepseudonimiseerd. Het opvragen van pseudoniemen vindt plaats door de Localization Registration Client bij de component PRS. Een samenvatting van het functioneel ontwerp van de component PRS is opgenomen in hoofdstuk 11. Pseudoniemenregistratieservice (PRS).

Kenmerk	Beschrijving
Rol	Datahoudende Zorgaanbieder
Component	<ul style="list-style-type: none"> - initiërend: Localization Registration Client, responderend: PRS - initiërend: Localization Registration Client, responderend: NVI

Wanneer	Een Datahoudende Zorgaanbieder registreert dat die Datahoudende Zorgaanbieder gezondheidsdata over een Betrokkene beschikbaar stelt.
Precondities	<ul style="list-style-type: none"> - De Datahoudende Zorgaanbieder maakt gebruik van een systeem dat de afspraken en specificaties van de generieke functie Lokalisatie in het algemeen en de component Localization Registration Client in het bijzonder heeft geïmplementeerd. - De Datahoudende Zorgaanbieder heeft in de NVI het systeem geautoriseerd om namens die Datahoudende Zorgaanbieder lokalisatie-records te registreren. - Het BSN van de Betrokkene is bekend. - De Betrokkene heeft toestemming gegeven aan de Datahoudende Zorgaanbieder voor het in de NVI registreren van een lokalisatie-record betreffende de Betrokkene.
Hoofdscenario	De Datahoudende Zorgaanbieder registreert een lokalisatie-record in de NVI. Om dat te kunnen doen vraagt het systeem van de Datahoudende Zorgaanbieder eerst een pseudoniem van het BSN op bij de PRS. De NVI antwoordt met een bevestiging van de registratie.
Alternatief scenario	n.v.t.
Postcondities	<ul style="list-style-type: none"> - Het Lokalisatie-record is opgeslagen in de NVI. - UC-GFL-02 is mogelijk gemaakt

5.2.UC-GFL-02: Opvragen lokalisatie-records

De Eindgebruiker wil relevante gezondheidsdata over een specifieke Betrokkene inzien, ook wanneer deze gezondheidsdata zijn verdeeld over meerdere vooraf onbekende Datahoudende Zorgaanbieders. De Eindgebruiker maakt daartoe gebruik van een systeem dat relevante gezondheidsdata over een specifieke Betrokkene kan vinden door

lokalisatie-records op te vragen bij de component NVI van de generieke functie Lokalisatie (zie hoofdstuk 11). Het opvragen van lokalisatie-records vindt plaats aan de hand van:

- een pseudoniem van het BSN van de Betrokkene;
- de zoekcontext.

Het opvragen van lokalisatie-records wordt geïnitieerd door een systeem dat de component Localization Search Client heeft geïmplementeerd (zie hoofdstuk 14). Bij het opvragen van lokalisatie-records handelt een Localization Search Client namens de Bevragende Zorgaanbieder (hoofdstuk 4).

In de communicatie met de NVI dienen BSN's te zijn gepseudonimiseerd. Het opvragen van pseudoniemen vindt plaats door de component Localization Search Client bij de component PRS (zie hoofdstuk 12).

Bij een bevraging van de NVI moet een zoekcontext worden meegegeven. De zoekcontext bestaat uit eigenschappen van Datahoudende Zorgaanbieders die voor de context van de Eindgebruiker relevant zijn. De werking en inhoud van de zoekcontext wordt nader toegelicht in hoofdstuk 9 Zoekcontext. De component NVI bepaalt op basis van het BSN-pseudoniem en de zoekcontext welke Datahoudende Zorgaanbieders relevante gezondheidsdata aanbieden.

214
 215 Voordat de component NVI aan het systeem van de Eindgebruiker lokalisatie-records oplevert, vraagt
 216 de NVI aan iedere - op basis van het BSN-pseudoniem en de zoekcontext gevonden - Datahoudende
 217 Zorgaanbieder om een akkoord voor het delen van diens lokalisatie-records met de Bevragende
 218 Zorgaanbieder (de zorgaanbieder vanwaaruit de Eindgebruiker handelt). Hiervoor communiceert de
 219 NVI met de component Custodian server van de Datahoudende Zorgaanbieder. Een samenvatting van
 220 het functioneel ontwerp van de component Custodian server is opgenomen in hoofdstuk 15.
 221

Kenmerk	Beschrijving
Rol	initiërend: Eindgebruiker, Bevragende Zorgaanbieder responderend: Datahoudende Zorgaanbieder
Component	<ul style="list-style-type: none"> - initiërend: Localization Search Client, responderend: PRS - initiërend: Localization Search Client, responderend: NVI - initiërend: NVI, responderend: Custodian server
Wanneer	De Eindgebruiker is op zoek naar gezondheidsdata over een specifieke Betrokkene.
Precondities	<ul style="list-style-type: none"> - De Eindgebruiker maakt gebruik van een systeem dat de afspraken en specificaties van de generieke functie Lokalisatie in het algemeen en de component Localization Search Client in het bijzonder heeft geïmplementeerd. - Het systeem van de Eindgebruiker is geautoriseerd om namens de Bevragende Zorgaanbieder (de zorgaanbieder vanwaaruit de Eindgebruiker handelt), de NVI te bevragen. - Het BSN van de Betrokkene is bekend. - De te bevragen zoekcontext is bekend voor de Localization Search Client. Dit vereist een mapping tussen de context van de Eindgebruiker en de door de Localization Search Client gebruikte zoekcontext.
Hoofdscenario	<p>Het systeem van de Eindgebruiker vraagt lokalisatie-records op bij de NVI. Om dat te kunnen doen vraagt het systeem eerst een pseudoniem van het BSN op bij de PRS. De NVI stelt een lijst samen van Datahoudende Zorgaanbieders die relevante data aanbieden. De NVI vraagt per Datahoudende Zorgaanbieder die relevante data aanbiedt om een akkoord voor het ontsluiten van diens lokalisatie-record met de Bevragende Zorgaanbieder. De NVI antwoordt met een lijst van Datahoudende Zorgaanbieders die:</p> <ul style="list-style-type: none"> - beschikken over gezondheidsdata over een specifieke Betrokkene; én - relevant zijn voor de context van de Eindgebruiker; én - hebben gecontroleerd dat er wel een grondslag en geen beperking van toepassing is op het delen van het lokalisatie-record met de Bevragende Zorgaanbieder (de zorgaanbieder van waaruit de Eindgebruiker handelt).

Alternatief scenario	n.v.t.
Postcondities	Het systeem van de Eindgebruiker weet welke Datahoudende Zorgaanbieders over relevante gezondheidsdata beschikken én akkoord zijn met het delen van hun lokalisatie-record. Het systeem kan op basis van deze informatie een gerichte bevraging per gevonden Datahoudende Zorgaanbieder initiëren en uiteindelijk de data aan de Eindgebruiker tonen.

222

223 5.3.UC-GFL-03: Opvragen van eigen lokalisatie-records

224 Een Datahoudende Zorgaanbieder of diens Dienstverlener Localization-Registration-Client controleert
 225 welke lokalisatie-records over een bepaald systeem van die Datahoudende Zorgaanbieder in de NVI
 226 staan om vast te stellen of deze juist en actueel zijn. Een Datahoudende Zorgaanbieder ziet uitsluitend
 227 de eigen lokalisatie-records. Alleen de lokalisatie-records van een specifiek systeem van de
 228 Datahoudende Zorgaanbieder zijn inzichtelijk. Het is binnen de context van een specifiek systeem
 229 mogelijk om:

- 230 - alle geregistreerde lokalisatie-records op te vragen; of
- 231 - alleen de geregistreerde lokalisatie-records over een specifieke Betrokkene op te vragen.

232

233 Het opvragen van de eigen lokalisatie-records vindt plaats bij de component NVI van de generieke
 234 functie Lokalisatie (zie hoofdstuk 11). Het opvragen van de eigen lokalisatie-records wordt geïnitieerd
 235 door een systeem dat de component Localization Registration Client heeft geïmplementeerd (zie
 236 hoofdstuk 13). In de communicatie met de NVI dienen BSN's te zijn gepseudonimiseerd. Het opvragen
 237 van pseudoniemen vindt plaats door de component Localization Registration Client bij de component
 238 PRS (zie hoofdstuk 12).

239

Kenmerk	Beschrijving
Rol	Datahoudende Zorgaanbieder Dienstverlener Localization-Registration-Client
Component	<ul style="list-style-type: none"> - initiërend: Localization Registration Client, responderend: PRS - initiërend: Localization Registration Client, responderend: NVI
Wanneer	Periodieke controle, of bij twijfel over de juistheid van de geregistreerde lokalisatie-records
Precondities	<ul style="list-style-type: none"> - De Datahoudende Zorgaanbieder of Dienstverlener Localization-Registration-Client maakt gebruik van een systeem dat de afspraken en specificaties van de generieke functie Lokalisatie in het algemeen en de component Localization Registration Client in het bijzonder heeft geïmplementeerd.

	<ul style="list-style-type: none"> - Het systeem is geautoriseerd om namens de Datahoudende Zorgaanbieder door dat systeem geregistreerde lokalisatie-records bij de NVI te bevragen. - De identifier van het systeem is bekend. - Indien de lokalisatie-records van een specifieke Betrokkene worden opgevraagd: Het BSN van de Betrokkene is bekend.
Hoofdscenario	Het systeem van de Datahoudende Zorgaanbieder of van een Dienstverlener Localization-Registration-Client van de Datahoudende Zorgaanbieder vraagt de lokalisatie-records over een specifiek systeem van die Datahoudende Zorgaanbieder op, voor één specifieke Betrokkene (zie hoofdstuk 4) of voor alle Betrokkenen. Wanneer de vraag voor één specifieke Betrokkene wordt gesteld, vraagt het systeem eerst een pseudoniem van het BSN op bij de PRS.
Alternatief scenario	n.v.t.
Postcondities	De Datahoudende Zorgaanbieder of de Dienstverlener Localization-Registration-Client weet welke lokalisatie-records over een specifiek systeem van die Datahoudende Zorgaanbieder zijn geregistreerd en kan afwijkingen corrigeren via UC-GFL-04 en UC-GFL-01, of UC-GFL-05.

5.4.UC-GFL-04: Verwijderen van lokalisatie-records

Een Datahoudende Zorgaanbieder of Dienstverlener Localization-Registration-Client verwijdert lokalisatie-records:

- wanneer de data die door een lokalisatie-record vindbaar worden gemaakt niet langer beschikbaar zijn;
- wanneer een Betrokkene de toestemming voor de registratie van lokalisatie-records over die Betrokkene in de NVI intrekt; of
- wanneer er een fout in een lokalisatie-record is geconstateerd.

Een individueel lokalisatie-record wordt nooit gewijzigd: een correctie bestaat uit verwijderen en opnieuw registreren. Een systeem kan alleen lokalisatie-records verwijderen die vanuit datzelfde systeem zijn geregistreerd. Het is binnen de context van een specifiek systeem mogelijk om:

- alle geregistreerde lokalisatie-records te verwijderen; of
- alleen de geregistreerde lokalisatie-records over een specifieke Betrokkene te verwijderen.

Het verwijderen van lokalisatie-records vindt plaats bij de component NVI van de generieke functie Lokalisatie (zie hoofdstuk 11). Het betreft een logische verwijdering. Het verwijderen van lokalisatie-records wordt geïnitieerd door een systeem dat de component Localization Registration Client heeft geïmplementeerd (zie hoofdstuk 13). In de communicatie met de NVI dienen BSN's te zijn gepseudonimiseerd. Het opvragen van pseudoniemen vindt plaats door de component Localization Registration Client bij de component PRS (zie hoofdstuk 12).

Kenmerk	Beschrijving
Rol	Datahoudende Zorgaanbieder Dienstverlener Localization-Registration-Client
Component	<ul style="list-style-type: none"> - initiërend: Localization Registration Client, responderend: PRS - initiërend: Localization Registration Client, responderend: NVI
Wanneer	<ul style="list-style-type: none"> - Data die door het lokalisatie-record vindbaar worden gemaakt zijn niet langer beschikbaar - Betrokkene trekt de toestemming voor de registratie van lokalisatie-records over die Betrokkene in de NVI in - Er is een fout in een lokalisatie-record geconstateerd.
Precondities	<ul style="list-style-type: none"> - De Datahoudende Zorgaanbieder of Dienstverlener Localization-Registration-Client maakt gebruik van een systeem dat de afspraken en specificaties van de generieke functie Lokalisatie in het algemeen en de component Localization Registration Client in het bijzonder heeft geïmplementeerd. - Het systeem is geautoriseerd om namens de Datahoudende Zorgaanbieder door dat systeem geregistreerde lokalisatie-records uit de NVI te verwijderen. - Er zijn voor het systeem van de Datahoudende Zorgaanbieder lokalisatie-records geregistreerd. - De identifier van het systeem is bekend. - Indien de lokalisatie-records van een specifieke Betrokkene worden verwijderd: Het BSN van de Betrokkene is bekend.
Hoofdscenario	De Datahoudende Zorgaanbieder of Dienstverlener Localization-Registration-Client verwijdert lokalisatie-records over een specifiek systeem uit de NVI. Wanneer de lokalisatie-records van één specifieke Betrokkene dienen te worden verwijderd, vraagt het systeem eerst een pseudoniem van het BSN op bij de PRS.
Alternatief scenario	n.v.t.
Postcondities	<ul style="list-style-type: none"> - Alle lokalisatie-records betreffende een specifiek systeem van de Datahoudende Zorgaanbieder én een specifieke Betrokkene zijn logisch verwijderd uit de NVI; of

Kenmerk	Beschrijving
	- Alle lokalisatie-records betreffende een specifiek systeem van de Datahoudende Zorgaanbieder zijn logisch verwijderd uit de NVI.

6. Juridisch kader

Dit hoofdstuk beschrijft de juridische context rondom de generieke functie Lokalisatie. Daarbij wordt ingegaan op de toepasselijke wet- en regelgeving en de wijze waarop deze van toepassing is op de positionering en inrichting van de NVI en de PRS.

6.1.Relevante wet- en regelgeving

6.1.1 AVG

Bij het gebruik van de NVI en PRS worden persoonsgegevens verwerkt. De PRS verwerkt het BSN ten behoeve van het genereren van sleutelmateriaal en pseudoniemen. Binnen de NVI wordt uitsluitend het voor de NVI gegenereerde pseudoniem verwerkt, in combinatie met gegevens over de zorgaanbieder en de categorieën gezondheidsgegevens die daar beschikbaar zijn. Het pseudoniem dat door de PRS wordt aangemaakt speelt een belangrijke rol in het voorkomen dat er niet meer gegevens worden verwerkt dan strikt noodzakelijk is.

In beginsel is verwerking van bijzondere persoonsgegevens verboden op basis van artikel 9 van de AVG. Op dit verbod bestaan echter uitzonderingen. Voor de verwerking van gezondheidsgegevens is de uitzondering van artikel 9, tweede lid, onder h van de AVG in samenhang met artikel 30, derde lid, onder a van de UAVG relevant. Deze uitzondering is van toepassing op het moment dat de verwerking van gezondheidsgegevens noodzakelijk is voor een goede behandeling of verzorging, zoals artikel 7 Wkkgz voorschrijft. Het lokaliseren via de NVI en daarmee toegang verschaffen aan de locatie(s) waar deze gegevens beschikbaar zijn, stelt de zorgverlener in staat om vervolgens, buiten de NVI om, de voor de behandeling noodzakelijke gezondheidsgegevens op te halen.

VWS draagt vanuit haar rol als stelselverantwoordelijke zorg voor de (door)ontwikkeling, het beheer en het onderhoud van de NVI en de PRS ten behoeve van het genereren van pseudoniemen. De NVI en PRS worden als voorzieningen ter beschikking gesteld aan zorgaanbieders. De zorgaanbieder is verwerkingsverantwoordelijke voor de persoonsgegevens die hij in het kader van zijn gebruik van de NVI verwerkt (artikel 4, onderdeel 7, AVG). De beheerder van de NVI is wel verantwoordelijk voor een juiste en veilige verwerking van gegevens in het systeem.

6.1.2 WGBO (medisch beroepsgeheim)

De Wet op de geneeskundige behandelovereenkomst (WGBO) regelt de wettelijke rechten en plichten in de relatie tussen een patiënt en zorgverlener. Het medisch beroepsgeheim is wettelijk verankerd in de WGBO (artikel 7:457 BW). Dit betekent dat zorgverleners een geheimhoudingsplicht hebben ten aanzien van informatie die herleidbaar is tot de patiënt en de behandeling. Deze plicht kan alleen worden doorbroken op het moment dat er een duidelijke wettelijke plicht of uitzondering bestaat, of wanneer er toestemming is gegeven door de patiënt.

Op grond van de artikelen 7:457 lid 2 BW kan een zorgverlener zonder toestemming van de patiënt informatie verstrekken aan medebehandelaars en vervangers (zoals bijvoorbeeld waarnemende ANW-artsen). In deze gevallen wordt de benodigde toestemming verondersteld. Zorgverleners die

geen behandelrelatie meer hebben met een patiënt, maar wel informatie kunnen verstrekken over behandelrelaties die zij in het verleden met de desbetreffende patiënt hebben gehad, mogen deze informatie slechts beschikbaar stellen aan een zorgaanbieder die een actuele behandelrelatie met die patiënt heeft als hun voormalige patiënt daarvoor toestemming geeft. Ook hier geldt een uitzondering op het toestemmingsvereiste wanneer het niet verstrekken van de informatie kan leiden tot ernstig nadeel voor de patiënt of een derde.

Het medisch beroepsgeheim vanuit de WGBO¹ is van toepassing op het registreren en beschikbaar stellen van lokalisatierecords in de NVI evenals de daaropvolgende gegevensuitwisseling op basis van een bevraging van de NVI. In de aansluitafspraken² voor de NVI wordt vastgelegd dat zorgaanbieders verantwoordelijk zijn voor het voldoen aan de vereisten uit de WGBO die gelden voor het delen van gezondheidsgegevens met derden.

6.1.3 Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)

De Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) stelt regels voor het gebruik van het BSN en de elektronische uitwisseling van medische gegevens. Artikel 15a Wabvpz verplicht zorgaanbieders om uitdrukkelijke toestemming te vragen voordat patiëntgegevens via een elektronisch uitwisselingssysteem beschikbaar kunnen worden gesteld.

De NVI maakt zelf geen dossiers, gedeelten van dossiers of gegevens uit dossiers raadpleegbaar en kwalificeert daarmee niet zelfstandig als elektronisch uitwisselingssysteem in de zin van de Wabvpz (artikel 1, onderdeel j, Wabvpz). Voor een voorziening die op basis van een lokalisatievraag de gezondheidsgegevens daadwerkelijk bij de bronhouder opvraagt en aan de zorgverlener beschikbaar stelt, is de uitdrukkelijke toestemming van de patiënt wel vereist.

Om te waarborgen dat de NVI proportioneel wordt ingezet en te voorkomen dat lokalisatiegegevens wel worden gevonden, maar vanwege het ontbreken van uitdrukkelijke toestemming niet kunnen worden opgehaald, wordt in de aansluitafspraken als voorwaarde opgenomen dat de patiënt voorafgaand aan het lokaliseerbaar maken van gegevens in de NVI uitdrukkelijke toestemming heeft gegeven.

De wettelijke verantwoordelijkheid voor het controleren van deze toestemming ligt bij de zorgaanbieder. De beheerder van de NVI (VWS) heeft geen rol in het controleren of voor een lokalisatierecord daadwerkelijk uitdrukkelijke toestemming van de patiënt is verkregen. Deze verplichting brengt niet met zich mee dat de zorgaanbieder een afschrift of registratie van de verkregen toestemming met de beheerder van de NVI moet delen. Het is niet wenselijk dat een overheidsorganisatie een rol vervult bij het controleren van toestemmingen van patiënten, omdat de verantwoordelijkheid voor het verkrijgen en controleren van deze toestemmingen primair bij de betrokken zorgverleners en zorgorganisaties ligt. Betrokkenheid van een overheidsorganisatie bij deze controle kan leiden tot onduidelijkheid over de verdeling van verantwoordelijkheden en roept vragen op over de bescherming van de privacy van patiënten. Daarnaast wordt binnen de NVI met pseudoniemen gewerkt en heeft de beheerder geen inzage in het BSN van personen. Hierdoor kan de beheerder de toestemming niet aan de identiteit van een specifieke patiënt koppelen of vaststellen of de gegevens van een specifieke patiënt daadwerkelijk in de NVI zijn opgenomen.

Aangesloten zorgaanbieders dragen daarom zelf de verantwoordelijkheid om te borgen dat er sprake is van uitdrukkelijke toestemming van de patiënt voorafgaande aan registratie in de NVI. Het hanteren van uitdrukkelijke toestemming als voorwaarde voor het registreren in de NVI zal in ieder geval gelden

¹ Boek 7 Titel 7 Afdeling 5 BW.

² Voorwaarden voor Deelname aan Pilot I NVI.

350 totdat de EHDS (en alle bijbehorende rechten) volledig zijn ingericht en landelijk geïmplementeerd
351 zijn. Deze inrichting moet vanuit de EHDS uiterlijk in maart 2029 gereed zijn.

353 6.1.4 EHDS

354 De EHDS is een Europese verordening die tot doel heeft het verbeteren van (grensoverschrijdende)
355 uitwisseling van gezondheidsgegevens. De EHDS gaat voor primair gebruik uit van toegang van
356 gezondheidswerkers tot relevante en noodzakelijke persoonlijke elektronische gezondheidsgegevens
357 van personen die zij behandelen. Daartegenover staan rechten van burgers om de toegang tot hun
358 gegevens onder bepaalde voorwaarden te beperken³ (toegangsbeperkingsrecht en een opt-out-
359 recht⁴).

360
361 Een vereiste vanuit de EHDS is dat lidstaten toegangsdiensten voor gezondheidswerkers en burgers
362 dienen in te richten. Deze toegangsdiensten moeten ervoor zorgen dat zorgverleners en burgers op
363 een veilige wijze toegang krijgen tot relevante elektronische gezondheidsgegevens. Vanuit VWS wordt
364 momenteel onderzoek gedaan naar de nationale invulling voor zowel de toegangsdienst voor
365 gezondheidswerkers als voor burgers vanuit de EHDS. De NVI wordt daarbij gezien als een onderdeel
366 van beide toegangsdiensten.

367
368 Om deze toegangsdiensten tijdig gereed te hebben voordat de relevante bepalingen van de EHDS van
369 toepassing worden in maart 2029, zijn pilots nodig om de daarvoor benodigde ICT-voorzieningen te
370 ontwikkelen en in de praktijk te beproeven. Vanuit de beoogde rol van de NVI en de PRS in beide
371 toegangsdiensten is daarom de vraag gesteld aan de Autoriteit Persoonsgegevens (AP) of de taak van
372 de lidstaat op grond van de EHDS om de toegangsdiensten in te richten, grondslag biedt voor de NVI.
373 In haar wetgevingsadvies oordeelde de AP dat de verplichtingen uit artikel 4 en 12 van de EHDS
374 voldoende grondslag bieden voor de voorgenomen verwerkingen van bijzondere persoonsgegevens
375 door de toegangsdiensten, ook in de fase van ICT-ontwikkeling. Vanuit de gedachte dat de NVI een
376 onderdeel is van de toegangsdiensten, vloeit de grondslag voort uit de EHDS.

377
378 Het advies biedt daarmee voldoende basis voor het operationeel gebruik van de NVI en PRS in de
379 huidige fase, maar een aantal onderdelen van de EHDS zijn nog niet volledig ingericht. Dit geldt in het
380 bijzonder voor het recht op beperking en het opt-out-recht van de burger (artikelen 8 en 10 EHDS).
381 De wijze waarop deze rechten in de praktijk worden ingevuld, is in aanloop naar de EHDS nog niet
382 afdoende geborgd. Daarom wordt, totdat de EHDS en de daarin opgenomen rechten volledig zijn
383 geborgd, het operationeel gebruik van de NVI en PRS proportioneel ingericht binnen de huidige
384 wettelijke kaders. Daarbij wordt enerzijds recht gedaan aan de voorliggende situatie en anderzijds
385 voldoende inzicht geboden in de werking van de componenten, zodat deze inzichten kunnen worden
386 benut voor de verdere implementatie van de EHDS.

³ Natuurlijke personen hebben het recht de toegang van gezondheidswerkers en zorgaanbieders tot hun persoonlijke elektronische gezondheidsgegevens geheel of gedeeltelijk te beperken. Het feit dat iemand de toegang heeft beperkt, mag zijn niet zichtbaar voor de zorgaanbieders. Een en ander is vastgelegd in artikel 8 EHDS.

⁴ Uit artikel 10 EHDS volgt dat de wetgeving van de lidstaten kan bepalen dat natuurlijke personen een opt-out-recht hebben ten aanzien van primair gebruik wat betreft de toegang tot hen betreffende persoonlijke elektronische gezondheidsgegevens die in een EPD-systeem zijn geregistreerd via een voor toegang tot elektronische gezondheidsgegevens voor natuurlijke personen en hun vertegenwoordigers (artikel 4 EHDS) of via een toegangsdiensten voor gezondheidswerkers (artikel 12 EHDS). In dergelijke gevallen zorgen de lidstaten ervoor dat de uitoefening van dat recht omkeerbaar is.

6.2.Doorontwikkeling

Binnen het hiervoor beschreven juridisch kader kunnen tijdens de ontwikkeling van de NVI en PRS nadere (technische, juridische en organisatorische) voorwaarden worden gesteld aan de aansluiting op en het gebruik van beide voorzieningen, onder meer ten aanzien van gerechtigd gebruik, authenticatie en autorisatie, informatiebeveiliging, logging, toezicht en de verantwoordelijkheden van aangesloten partijen. In praktijkbeproevingen met de NVI en PRS worden de technische, juridische en organisatorische aspecten in samenhang getest en beoordeeld.

7. Requirements

De requirements voor de generieke functie Lokalisatie zijn tot stand gekomen in verschillende werksessies met de werkgroep Lokalisatie. Het resultaat is een lijst met requirements die te vinden is op <https://github.com/orgs/minvws/projects/60/views/1>.

Dit hoofdstuk beschrijft de requirements gerelateerd aan de Organisatielaag en Proceslaag die in de huidige afspraken en specificaties zijn verwerkt. In Bijlage 1 staat de volledige lijst.

Het uitgangspunt is dat IT-dienstverleners met de afspraken en specificaties de functionaliteiten kunnen ontwikkelen in de eigen applicaties en keuzes kunnen maken in het vormgeven van de benodigde schermen.

7.1.Registreren en beheren van lokalisatiegegevens

Datahoudende Zorgaanbieders registreren de aanwezigheid van gezondheidsdata over een specifieke Betrokkene in de NVI met behulp van lokalisatiegegevens. Datahoudende Zorgaanbieders kunnen de aan zichzelf gekoppelde lokalisatiegegevens ook raadplegen, verwijderen en aanpassen.

7.2.Opvragen lokalisatie-records

De generieke functie Lokalisatie stelt de systemen van Eindgebruikers in staat om die Datahoudende Zorgaanbieders op te vragen die:

- beschikken over gezondheidsdata over een specifieke Betrokkene; én
- relevant zijn voor de context van de Eindgebruiker; én
- hebben gecontroleerd dat er wel een grondslag en geen beperking van toepassing is op het delen van het lokalisatie-record met de Bevragende Zorgaanbieder (de zorgaanbieder van waaruit de Eindgebruiker handelt).

8. Gebruikersinteractie

Dit hoofdstuk beschrijft de gebruikersinteracties van de generieke functie Lokalisatie aan de hand van concrete gebruikerssituaties gemodelleerd in user journeys. Elke user journey bevat verwijzingen naar de betrokken usecases en een stappenmatrix die de gebruikersinteracties beschrijft.

8.1.Huisartsenpraktijk maakt data vindbaar via de NVI

Betrokken usecases

UC-GFL-01

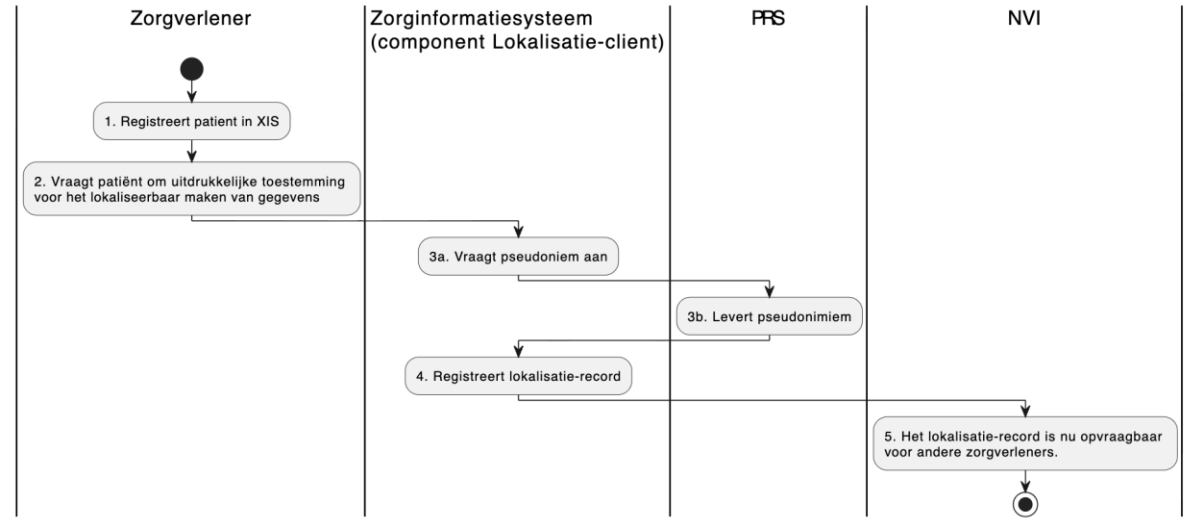
Situatie

Dhr. Carter, huisartsassistent, schrijft een patiënt in bij de huisartsenpraktijk. Om andere zorgverleners in staat te stellen de data, die worden geregistreerd wanneer de patiënt zorg ontvangt van de huisartspraktijk, te vinden, registreert de huisartsenpraktijk een lokalisatie-record in de Nationale Verwijsindex (NVI). Dit proces omvat het pseudonimiseren van het BSN van de patiënt bij de component PRS en het registreren van een lokalisatie-record bij de component NVI.

Narratief

1. Dhr. Carter registreert de patiënt in het huisartsinformatiesysteem.
2. Dhr. Carter vraagt de patiënt om uitdrukkelijke toestemming voor het registreren van gegevens in de NVI.
3. Het huisartsinformatiesysteem pseudonimiseert het BSN van de patiënt met behulp van de pseudoniemenregistratieservice (PRS)
4. Het huisartsinformatiesysteem registreert een lokalisatie-record bij de NVI.
5. Het lokalisatie-record is nu opvraagbaar voor andere zorgverleners.

Activiteitendiagram



Stappenmatrix

Stap	UC	Actie gebruiker	Systeemrespons	Scherf
1	n.v.t.	Dhr. Carter registreert patiënt in XIS	XIS slaat patiëntgegevens op	XIS-inschrijfscherf
2	n.v.t.	Dhr. Carter vraagt de patiënt om uitdrukkelijke toestemming voor het registreren van gegevens in de NVI.	XIS slaat uitdrukkelijke toestemming op	XIS-inschrijfscherf
3	UC-GFL-01	Geen	XIS pseudonimiseert BSN via PRS	Geen
4	UC-GFL-01	Geen	XIS registreert een lokalisatierecord bij de NVI	Geen
5	UC-GFL-01	Geen	De NVI slaat het lokalisatierecord op.	Geen
6	UC-GFL-01	Geen	Record beschikbaar voor opvragingen	Geen

8.2.Arts vraagt patiënt-samenvatting op**Betrokken usecases**

UC-GFL-02

Situatie

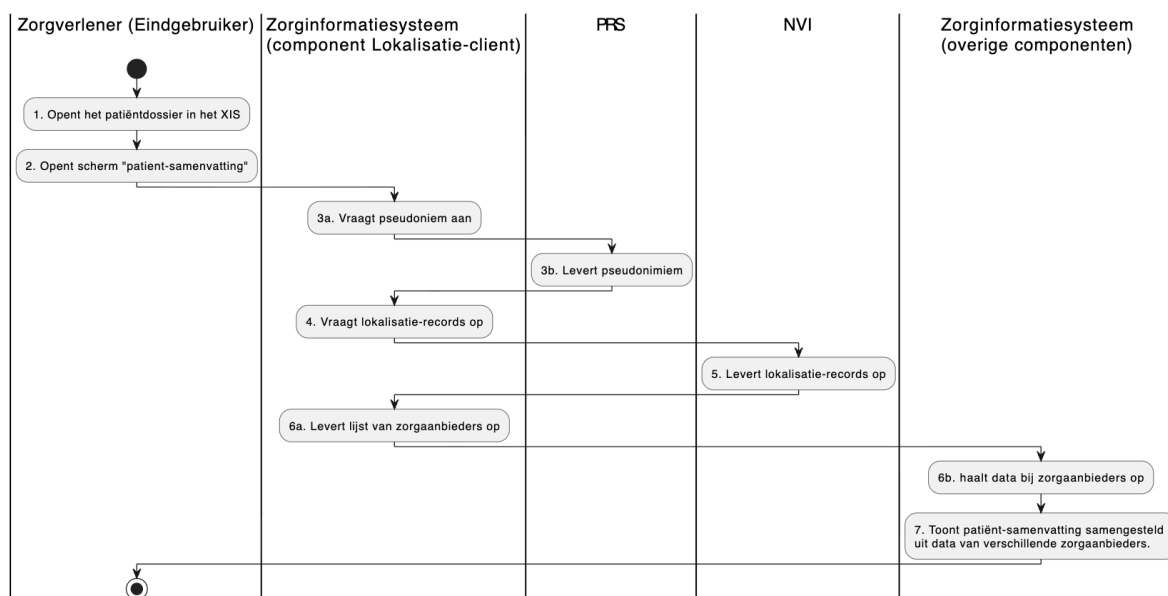
Dr. Smith, arts bij Ziekenhuis A, behandelt een patiënt die recent is verwezen vanuit een ander ziekenhuis. Zij wil graag de patiënt-samenvatting inzien. De data voor de patiënt-samenvatting is verdeeld over verschillende andere zorgaanbieders (bijvoorbeeld huisartsenpraktijk, apotheek en ziekenhuis). Dit proces omvat het pseudonimiseren van het BSN van de patiënt bij de component PRS, het door het XIS bepalen van de zoekcontext en het opvragen van lokalisatierecords bij de component NVI.

Narratief

1. Dr. Smith opent het patiëntdossier in het XIS; het BSN wordt vastgesteld.
2. Dr. Smit maakt in het XIS kenbaar dat ze de patiënt-samenvatting wil inzien; de zoekcontext wordt vastgesteld.
3. Het XIS pseudonimiseert het BSN van de patiënt met behulp van de pseudoniemenregistratieservice (PRS).
4. Het XIS vraagt lokalisatierecords op bij de NVI inclusief de zoekcontext
5. De NVI levert lokalisatierecords op.

6. XIS gebruikt lokalisatie-records voor ophalen van data bij verschillende zorgaanbieders (bijv. huisartsenpraktijk, apotheek en ziekenhuis).
7. XIS toont patiënt-samenvatting die is samengesteld uit data van verschillende zorgaanbieders aan Dr. Smith.

Activiteitendiagram



Stappenmatrix

Stap	UC	Actie gebruiker	Systeemrespons	Scherm
1	Geen	Dr. Smith opent patiëntdossier	XIS toont gegevens van de patiënt, BSN vastgesteld	XIS - Dossier
2	UC-GFL-02	Dr. Smith maakt kenbaar dat ze patiënt-samenvatting wil inzien	XIS stelt zoekcontext vast	XIS - patiënt-samenvatting
3	UC-GFL-02		XIS laat BSN pseudonimiseren via PRS	Geen
4	UC-GFL-02		XIS voert een zoekopdracht uit bij de NVI met gepseudonimiseerde BSN	Geen
5	UC-GFL-02		De NVI levert lokalisatie-records op. Deze stap omvat: a: NVI verstuurt verzoek aan de gelokaliseerde Datahoudende Zorgaanbieders of de lokalisatie-informatie mag worden gedeeld met de Bevragende Zorgaanbieder partij. b. Datahoudende Zorgaanbieder checkt of er een grondslag (bijvoorbeeld met een online	Geen

			<p>toestemmingsvoorziening (OTV) of dossierhouderstoestemmingsvoorziening (DHTV) en/of een beperking van toepassing is op het delen van de lokalisatie-informatie met de Bevragende Zorgaanbieder.</p> <p>c. Datahoudende Zorgaanbieder koppelt akkoord of niet-akkoord terug aan de NVI.</p> <p>Deze stappen zijn omwille van de leesbaarheid niet in het activiteitendiagram opgenomen.</p>	
6	Geen		XIS gebruikt lokalisatie-records voor ophalen van data bij verschillende zorgaanbieders (bijvoorbeeld huisartsenpraktijk, apotheek en ziekenhuis).	Geen
7	Geen		XIS toont aan Dr. Smith de patiënt-samenvatting die is samengesteld uit data van verschillende zorgaanbieders	XIS-patiënt-samenvatting

9. Informatiemodellen

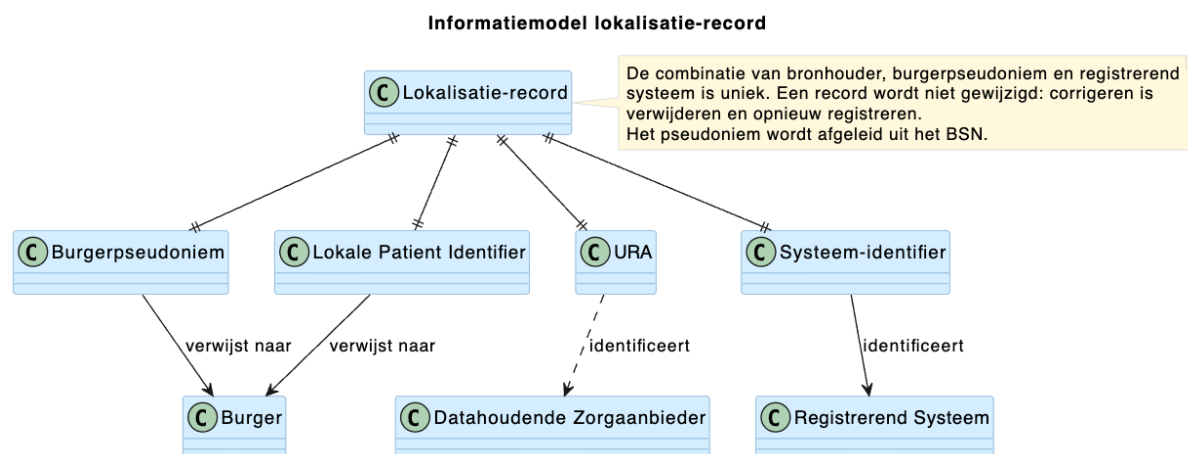
Binnen de generieke functie zijn twee informatiemodellen relevant:

- het lokalisatie-records
- de lokalisatievraag

Deze informatiemodellen worden hieronder toegelicht.

9.1. Lokalisatie-record

Een lokalisatie-record legt vast dat een zorgaanbieder beschikt over gezondheidsdata over een specifieke burger. Onderstaand informatiemodel toont de onderdelen van een lokalisatie-record en hun onderlinge relaties.



Het model leest als volgt:

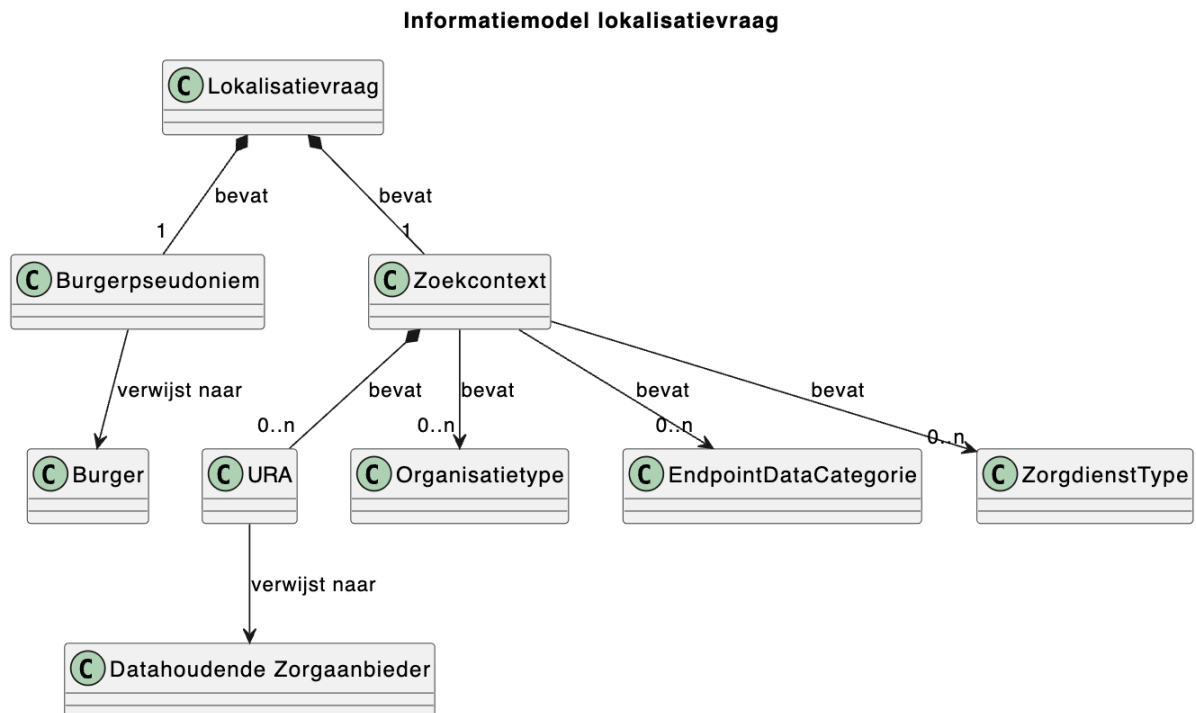
- Een lokalisatie-record bestaat uit vier onderdelen, elk precies één keer aanwezig: het burgerpseudoniem, de lokale patiënt-identificer, het URA van de zorgaanbieder en een identificer van het registrerende systeem.
- Het burgerpseudoniem verwijst naar de burger zonder het BSN te bevatten. De omzetting vindt plaats buiten de NVI, door de de PRS
- De lokale patiënt-identificer is een identificer van een patiënt die specifiek is voor de context van de Datahoudende Zorgaanbieder.
- Het URA identificeert de zorgaanbieder die de gegevens beschikbaar heeft.
- De Localization Registration Client legt vast welk systeem van de Datahoudende Zorgaanbieder de registratie heeft gedaan. Heeft een Datahoudende Zorgaanbieder meerdere systemen, bijvoorbeeld een EPD en een PACS, dan beheert elk systeem uitsluitend de eigen registraties. Het vastleggen van de systeem-identificer voorkomt conflicten wanneer Datahoudende Zorgaanbieders met meerdere systemen aan de NVI koppelen. De systeem-identificer is niet zichtbaar voor Bevragende Zorgaanbieders.
- De combinatie van burger (Betrokkene), Datahoudende Zorgaanbieder en systeem is uniek: dezelfde Datahoudende Zorgaanbieder kan voor dezelfde Betrokkene en hetzelfde systeem niet twee keer voorkomen.

Deze opzet van het lokalisatie-record kent de volgende aandachtspunten:

- Binnen deze datastructuur is bewust geen actualiteitsinformatie opgenomen. Hoewel het opnemen van actualiteitsinformatie zou kunnen helpen om gerichter te kunnen filteren in een lokalisatievraag heeft het ook consequenties voor zowel registratie (moet bij elke actualisatie) en voor de bescherming die een pseudoniem geeft. De consequentie hiervan wordt als acceptabel beschouwd gegeven het feit dat een filter op actualiteit van data ook bij het ophalen van data kan worden toegepast.

9.2. Lokalisatievraag

Een Bevragende Zorgaanbieder bevraagt de NVI met behulp van een lokalisatievraag. De lokalisatievraag modelleert de vraag naar Datahoudende Zorgaanbieders die gezondheidsdata over een specifieke burger aanbieden die voor de context van de Eindgebruiker relevant zijn. Onderstaand informatiemodel toont de onderdelen van een lokalisatievraag en hun onderlinge relaties.



9.2.1 Zoekcontext

Een belangrijk element van de lokalisatievraag is de zoekcontext. De zoekcontext wordt gebruikt bij het zoeken naar Datahoudende Zorgaanbieders in de NVI. De zoekcontext bevat eigenschappen die Datahoudende Zorgaanbieders relevant maken voor de lokalisatievraag van de Eindgebruiker:

- Wat maakt een Datahoudende Zorgaanbieders relevant voor de Eindgebruiker?
 - Voor bijvoorbeeld een patiënt-samenvatting zijn wellicht alleen Datahoudende Zorgaanbieders van type “huisartsenpraktijk”, “apotheek” of “ziekenhuis” relevant.
 - Voor een bepaalde usecase zijn wellicht alleen Datahoudende Zorgaanbieders gevestigd in een bepaalde geografische regio relevant.
- Welke zorgdienst-types zijn relevant voor de Eindgebruiker?
 - Voor een bepaalde usecase zijn wellicht alleen die Datahoudende Zorgaanbieders relevant die een specifiek type zorgdienst aanbieden.
- Welke data-types zijn relevant voor de Eindgebruiker?
 - Voor bijvoorbeeld een actueel medicatieoverzicht zijn wellicht alleen die Datahoudende Zorgaanbieders relevant die beschikken over een endpoint dat het data-type “medicatiegegevens” kan ontsluiten.

Bij het bevragen van de NVI geeft de Bevragende Zorgaanbieder een zoekcontext mee. De NVI gebruikt deze zoekcontext in combinatie met de generieke functie Adressering om de relevante Datahoudende Zorgaanbieders te selecteren. Daarna vraagt de NVI een akkoord aan ieder van deze relevante Datahoudende Zorgaanbieders. De relevante Datahoudende Zorgaanbieders die een akkoord hebben gegeven, worden teruggegeven aan de Bevragende Zorgaanbieder. Bij de registratie van lokalisatie-records in de NVI wordt geen zoekcontext meegegeven.

De zoekcontext filtert op organisatie-eigenschappen (wat een organisatie aanbiedt, zoals het organisatietype, geregistreerde zorgdiensten, geregistreerde endpoints) en niet op de inhoud van de te lokaliseren data. Het filteren op basis van organisatie-eigenschappen in plaats van data-eigenschappen heeft verschillende voordelen:

- Qua change management is een eigenschap op organisatieniveau minder uitdagend dan een eigenschap op dataniveau. Aanpassingen aan categorieën op organisatieniveau zijn meteen te gebruiken zodra partijen deze door middel van de generieke functie Adressering hebben geregistreerd. Hierbij is geen aanpassing en her-aanmelding in/ door de software nodig die wordt gebruikt om met de NVI te communiceren.
- Bij zoeken (en registreren) hoeft aan de data zelf geen categorie te worden gekoppeld. Dit is prettig omdat zorgdata zich moeilijk in vaste categorieën laat onderbrengen.
- Misbruik van zoekcontext is inzichtelijk: een Bevragende Zorgaanbieder kan een zoekcontext gebruiken die veel breder is dan wat nodig is voor de context van de Eindgebruiker. Dit kan van via logging gedetecteerd worden. Dit maakt het mogelijk om bij misbruik op te treden. De Tuchtcolleges voor de Gezondheidszorg en de Inspectie Gezondheidszorg en Jeugd (IGJ) zijn hiervoor de aangewezen instanties.

Het filteren op basis van organisatie-eigenschappen in plaats van data-eigenschappen kent ook een aantal aandachtspunten:

- Een systeem, wat namens Eindgebruiker lokaliseert, kan, bij een match op zoekcontext en lokalisatie-record, Datahoudende Zorgaanbieders in het antwoord geven die, puur vanuit een dataminimalisatieoogpunt, niet nodig zijn voor de vraag van de Eindgebruiker. Dit aandachtspunt wordt als acceptabel beschouwd gegeven het feit dat een Datahoudende Zorgaanbieder via de lokalisatie-accordering-vraag zelf kan bepalen of aan een specifieke Bevragende Zorgaanbieder kenbaar mag worden gemaakt dat die Datahoudende Zorgaanbieder data over een specifieke patiënt beschikbaar stelt. Ook kan het systeem van de Bevragende Zorgaanbieder de filtering op inhoud uitvoeren en op deze wijze de informatie niet delen met de Eindgebruiker.
- Koppeling met de generieke functie Adressering: De zoekcontext van de generieke functie Lokalisatie maakt gebruik van de generieke functie Adressering. Hierdoor ontstaat een afhankelijkheid. Dit maakt dat changemanagement op Adressering potentieel ook gevolgen heeft voor Lokalisatie. In architectuur ermen is er “coupling” tussen de Generieke Functies. Dit aandachtspunt wordt als acceptabel beschouwd omdat het alternatief vereist dat alle zoekvragen via de URA lijst in de zorgcontext worden geplaatst. Dit geeft gevolgen voor het niveau waarop informatie gelogd kan worden (semantiek van een lijst URA’s is anders dan wanneer dat uitgedrukt wordt als organisatie-eigenschappen).

10. Beveiliging

Op het gebied van informatiebeveiliging dient de generieke functie Lokalisatie invulling te geven aan NEN7510, NEN7512 en NEN7513. De uitwerking van de beveiliging wordt nader toegelicht in het technisch ontwerp van de generieke functie Lokalisatie.

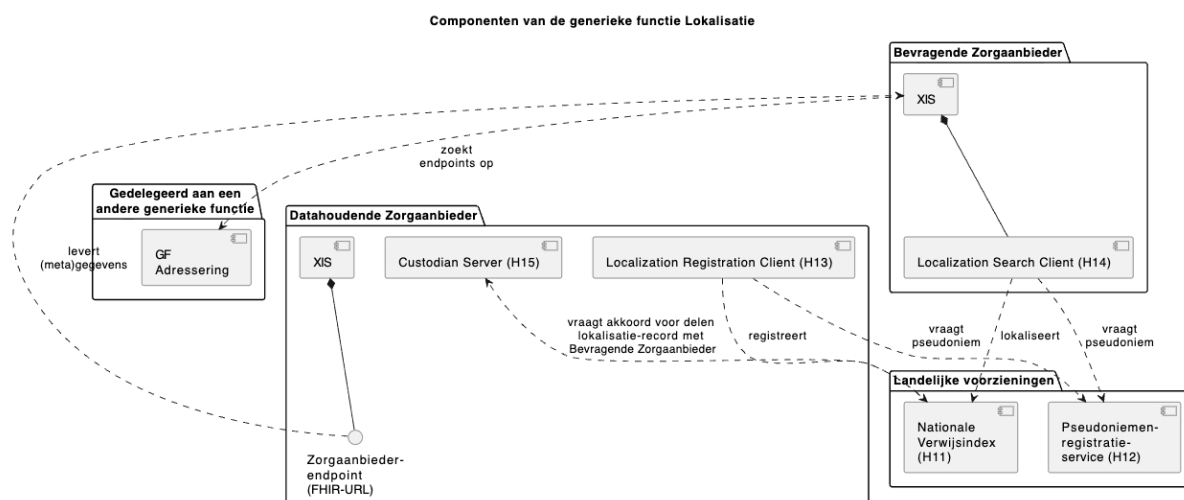
Deel B (informatief): Componenten

LET OP: Deel B is informatief van aard en geen onderdeel van de consultatie.

Deel B beschrijft de componenten die worden gebruikt in de verschillende usecases. Waar deel A de generieke functie Lokalisatie beschrijft vanuit het perspectief van de stakeholders, beschrijft deel B de generieke functie Lokalisatie per component.

Overzicht van de componenten

Onderstaand diagram plaatst de componenten uit dit deel ten opzichte van elkaar. De Localization Search Client draait bij de raadplegende zorgaanbieder; de NVI en de PRS zijn landelijke voorzieningen. Onderin staat de Datahoudende Zorgaanbieder met het endpoint waar het XIS van de Bevragende Zorgaanbieder de (meta)gegevens ophaalt. De lokalisatiefunctie omvat de hele keten van de vraag van de zorgverlener tot en met het resultaatsscherm; het opzoeken van de endpoints is daarbinnen gedelegeerd aan de generieke functie Adressering.



De Implementation Guide geeft dit endpoint geen eigen naam: het beschrijft uitsluitend de registratie bij en bevraging van de NVI. Over de endpoints van de Datahoudende Zorgaanbieders stelt de IG alleen dat “the endpoints of these data holders (e.g. FHIR or DICOM-urls) need to be resolved using a Care service (Query) Directory”. In dit document is het daarom aangeduid als zorgaanbieder-endpoint (FHIR-URL). Het citaat noemt DICOM als mogelijkheid; binnen de lokalisatiefunctie gaat het uitsluitend om FHIR.

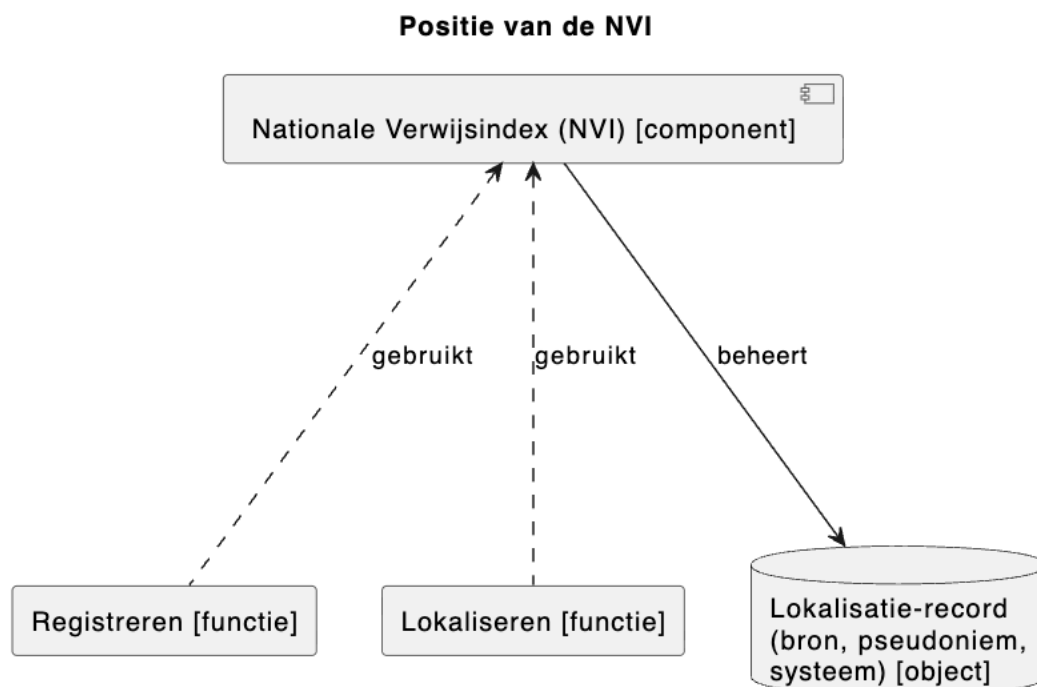
Wat lokalisatie afneemt van de andere generieke functies (identificatie en authenticatie, autorisatie, toestemming en logging) staat in het TO en de Implementation Guide en wordt hier niet uitgewerkt.

11. Nationale Verwijsindex (NVI)

11.1. Rol en doel

De NVI is de landelijke voorziening waarin zorgaanbieders registreren dát zij gegevens over een burger beschikbaar stellen, en waar de systemen van zorgverleners opvragen welke zorgaanbieders dat zijn. De NVI werkt als een landelijke index (Master Patient Index): de NVI legt uitsluitend de verwijzing vast (welke bron, welke burger als pseudoniem, welk systeem). De NVI bevat zelf geen medische gegevens.

623 Zonder centrale index moeten zorgverleners per zorgaanbieder navragen of er gegevens beschikbaar
 624 zijn.



625

626 11.2. Stakeholders

627

Stakeholder	Rol	Omschrijving
Burger	Betrokkene	onderwerp van de registraties. Gegevens zijn vindbaar voor de eigen behandeling; het BSN komt niet in de NVI voor en het gebruik is inzichtelijk.
Zorgverlener	Eindgebruiker	stelt via het XIS de lokalisatievraag. Stelt in één bevraging vast welke zorgaanbiders gegevens hebben, zonder navraag per zorgaanbieder.
Zorgaanbieder	Zorgaanbieder	registreert de beschikbaarheid van gegevens en beheert de eigen registraties. Gegevens zijn landelijk vindbaar zonder eigen lijsten of regionale koppelingen; kan de eigen registraties controleren en corrigeren.
IT-dienstverlener	Dienstverlener Localization- Registration- Client	implementeert registratie bij de NVI het zorginformatiesysteem. Eén koppelvlak op basis van internationale standaarden voor alle klanten.
IT-dienstverlener	Dienstverlener Localization- Search-Client	implementeert bevraging bij de NVI in het zorginformatiesysteem. Eén koppelvlak op basis van internationale standaarden voor alle klanten.
IT-dienstverlener	Dienstverlener Custodian-server	implementeert component dat door NVI kan worden bevraagd om akkoord te geven op het door de NVI ontsluiten van het lokalisatie-record. Eén koppelvlak op basis van internationale standaarden voor alle klanten.

Stakeholder	Rol	Omschrijving
Beheerorganisatie NVI	Dienstverlener NVI	operationeel beheer van de voorziening, beoordeelt aansluitingen. Beschikbaarheid, integriteit en rechtmatig gebruik van landelijke infrastructuur.

11.3. Usecases

11.3.1 UC-NVI-01: Autorisatie van Dienstverlener Localization-Registration-Client/ Dienstverlener Localization-Search-Client

Een Zorgaanbieder maakt gebruik van de generieke functie Lokalisatie via een systeem dat de component Localization Registration Client en/of de component Localization Search Client heeft geïmplementeerd. Deze componenten worden aan een Zorgaanbieder als dienst aangeboden door respectievelijk een Localization-Registration-Client en een Dienstverlener Localization-Search-Client. De Dienstverlener moet eerst door de Zorgaanbieder worden geautoriseerd om namens die Zorgaanbieder lokalisatie-records te kunnen registreren, beheren en/of op te vragen.

Kenmerk	Beschrijving
Rol	Beheerder van Zorgaanbieder
Wanneer	Nieuwe aansluiting, wijziging autorisatie, wissel Dienstverlener Localization-Registration-Client of Dienstverlener Localization-Search-Client
Precondities	Beheerder van Zorgaanbieder heeft toegang tot de autorisatie-interface van de NVI.
Hoofdscenario	De Functioneel beheerder van Zorgaanbieder autoriseert de Dienstverleners die namens die Zorgaanbieder lokalisatie-records mogen registreren, beheren en/of opvragen.
Alternatief scenario	<ul style="list-style-type: none"> - Functioneel beheerder van Zorgaanbieder trekt autorisatie in. - Functioneel beheerder van Zorgaanbieder wijzigt autorisatie.
Postcondities	Dienstverleners Localization-Registration-Client en/of Dienstverleners Localization-Search-Client kunnen namens Zorgaanbieder lokalisatie-records registreren, beheren en opvragen.

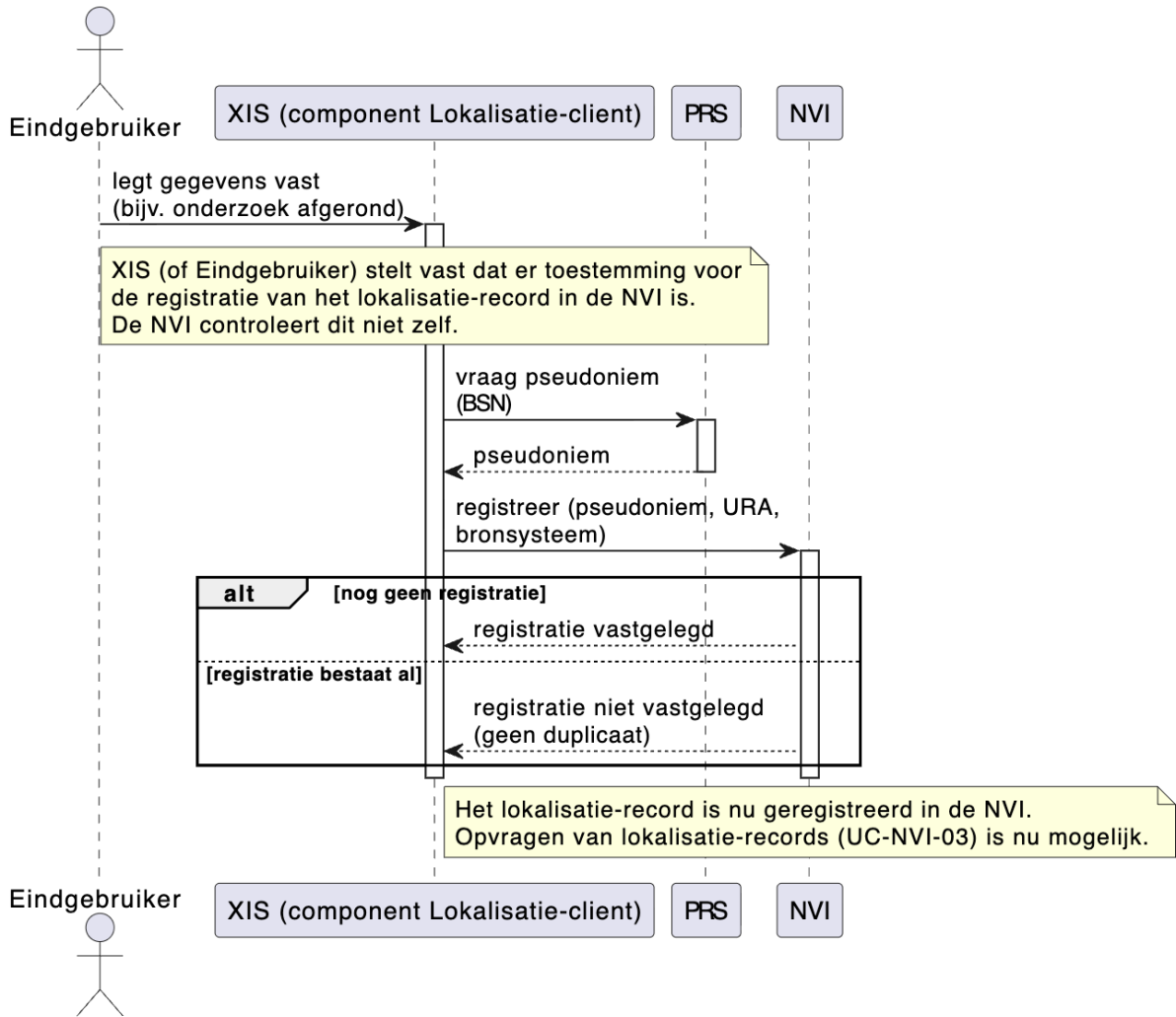
11.3.2 UC-NVI-02: Registratie van lokalisatie-records

Kenmerk	Beschrijving
Rol	Datahoudende Zorgaanbieder / Dienstverlener Localization-Registration-Client
Wanneer	Wanneer gegevens over een Betrokkene beschikbaar komen en toestemming voor registratie van lokalisatie-records in de NVI is vastgesteld

Precondities	Datahoudende Zorgaanbieder is aangesloten en geautoriseerd; toestemming van de Betrokkene voor registratie van lokalisatie-records in de NVI is door de Datahoudende Zorgaanbieder gecontroleerd; pseudoniem is opgehaald bij de PRS
Componenten	Localization Registration Client (Hoofdstuk 13) → PRS (Hoofdstuk 12) → NVI (Hoofdstuk 11)
Hoofdscenario	De Zorgaanbieder registreert bij de NVI het pseudoniem voor deze Betrokkene, de eigen URA, het registrerende systeem. De NVI legt de registratie vast.
Alternatief scenario	De registratie bestaat al: de NVI geeft de bestaande registratie terug en maakt geen duplicaat aan.
Postcondities	De registratie is vindbaar voor geautoriseerde raadplegers.

642
643

UC-NVI-02. Registratie van een lokalisatierecord

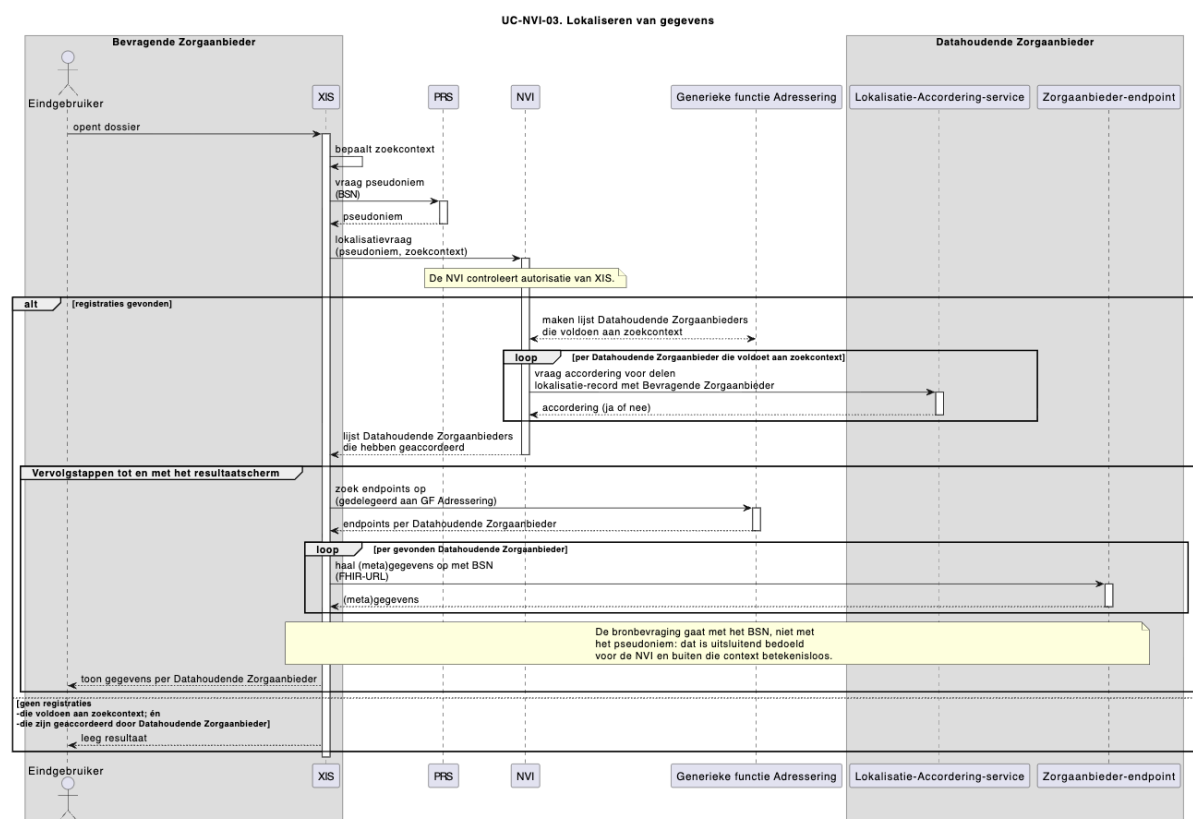


644
645
646
647

11.3.3 UC-NVI-03: Opvraging lokalisatie-records

Kenmerk	Beschrijving
Rol	Eindgebruiker (via Localization Search Client)
Wanneer	Noodzaak voor gegevensuitwisseling over een burger

Precondities	Eindgebruiker is geautoriseerd, pseudoniem is opgehaald bij de PRS
Componenten	Localization Search Client (Hoofdstuk 14) → PRS (Hoofdstuk 12) → NVI (Hoofdstuk 11) → GF Adressering
Hoofdscenario	De raadpleger vraagt lokalisatie-records op aan de hand van pseudoniem en zoekcontext. De NVI antwoordt met een lijst van zorgaanbieders die over relevante gegevens beschikken én die akkoord zijn met het delen van het lokalisatie-record met de raadpleger.
Alternatief scenario	<ul style="list-style-type: none"> - Er zijn geen registraties voor deze Betrokkene, het resultaat is leeg. - Er zijn alleen registraties voor deze Betrokkene van Zorgaanbieders die niet akkoord gaan met het delen van het lokalisatie-record met de Bevragende Zorgaanbieder: het resultaat is leeg.
Postcondities	Het systeem van de Eindgebruiker weet welke zorgaanbieders gezondheidsdata hebben én akkoord zijn met het delen van het lokalisatie-record. Het systeem kan aansluitend GF Adressering gebruiken om de digitale adressen voor elektronische gegevensuitwisseling te verkrijgen.



648

649 11.3.4 UC-NVI-04: Verwijderen van registraties

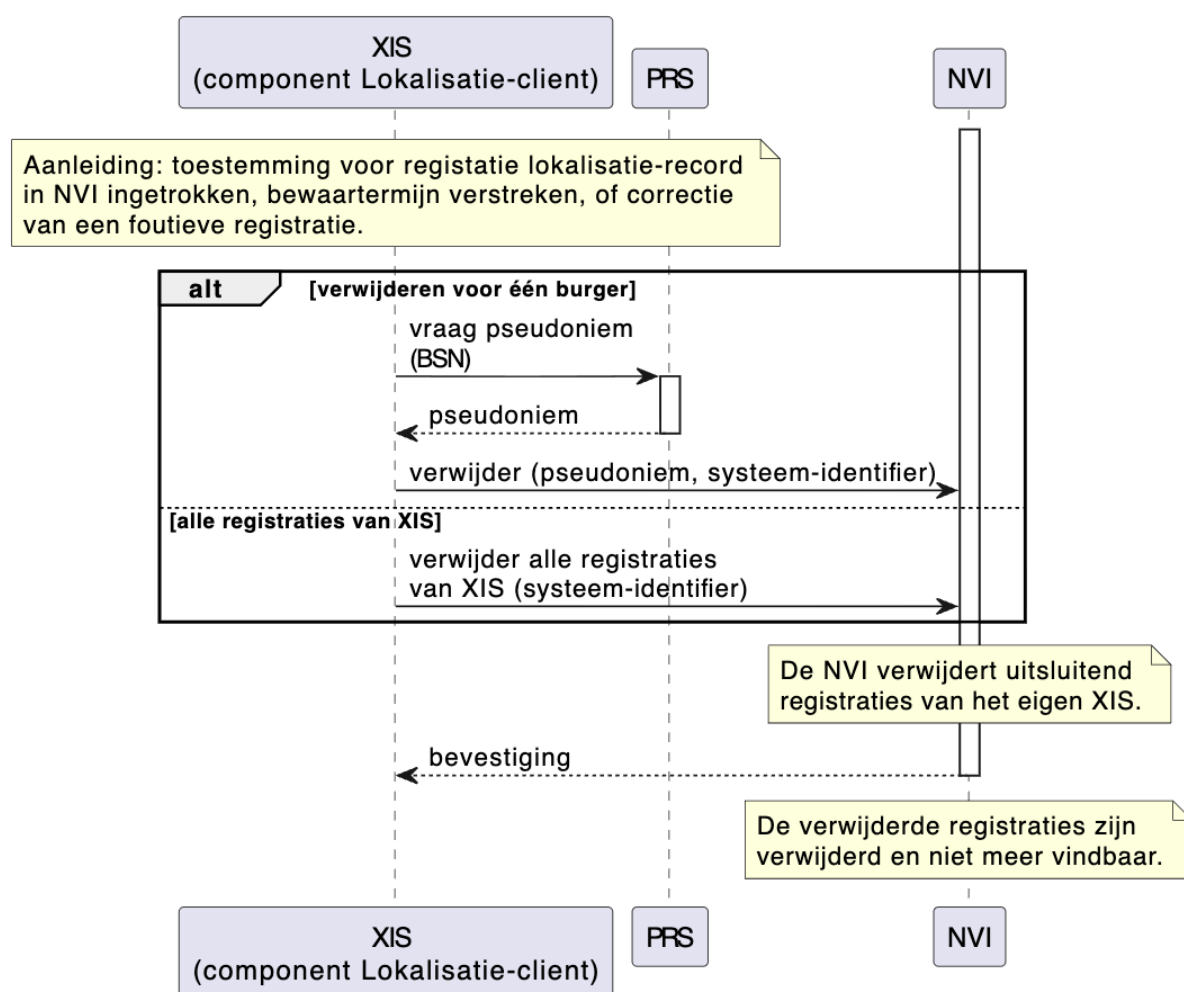
650

Kenmerk	Beschrijving
Rol	Zorgaanbieder / Dienstverlener Zorginformatiesysteem (via Dienstverlener Localization-Registration-Client)

Wanneer	Toestemming voor de registratie van lokalisatie-records in de NVI ingetrokken, gegevens vernietigd conform bewaartermijn, of correctie van een foutieve registratie
Precondities	De registratie is van de eigen bron
Componenten	Localization Registration Client (hoofdstuk 13) → NVI (hoofdstuk 11)
Hoofdscenario	De Zorgaanbieder verwijdert een specifieke registratie, alle registraties voor één Betrokkene, of al haar registraties.
Postcondities	De verwijderde registraties zijn niet meer vindbaar voor raadplegers.

651

UC-NVI-04. Verwijderen van registraties



652

653

654 11.3.5 UC-NVI-05: Raadplegen eigen registraties

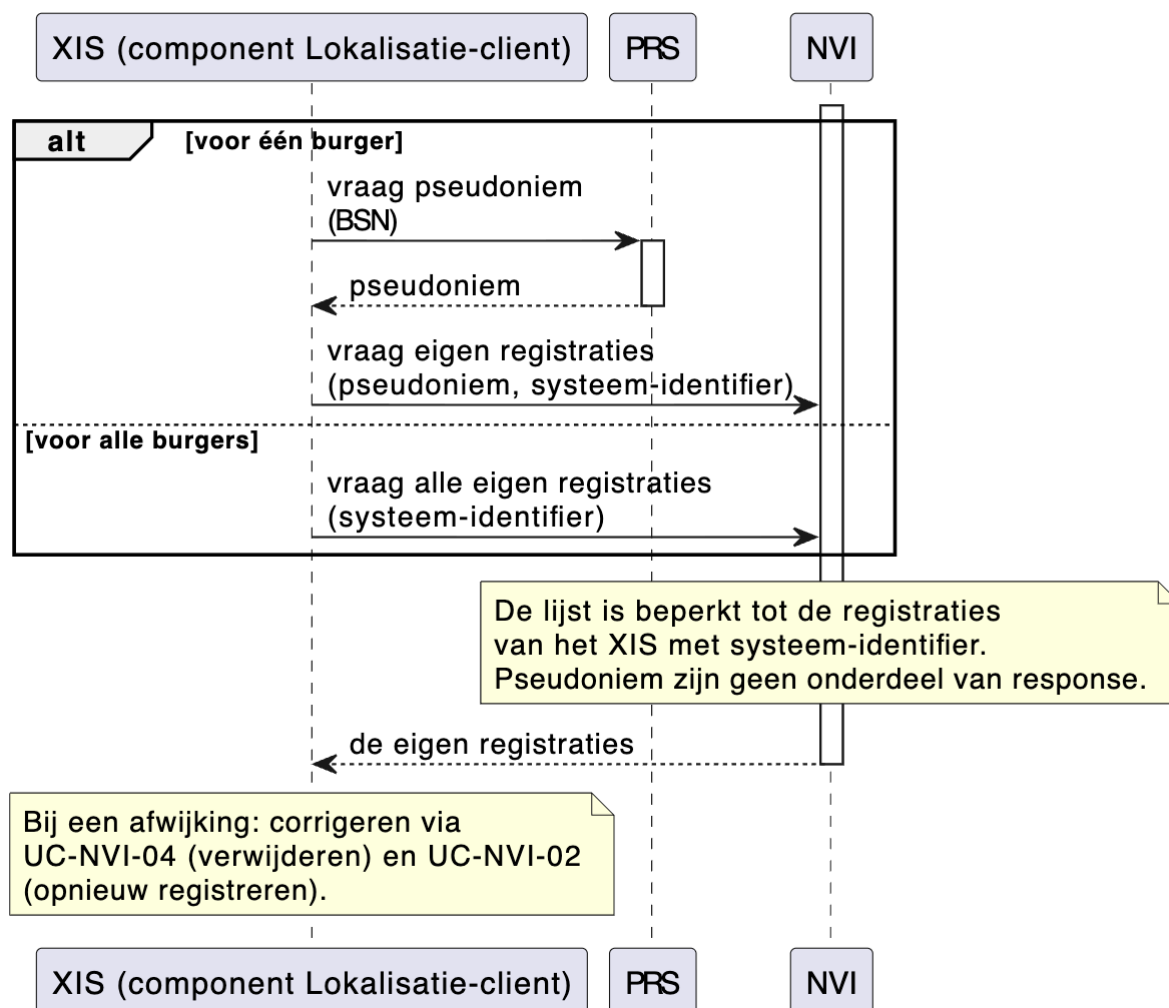
655

Kenmerk	Beschrijving
Rol	Zorgaanbieder / Dienstverlener Localization-Registration-Client
Wanneer	Controle of de eigen registraties juist en actueel zijn
Precondities	Zorgaanbieder is aangesloten en geautoriseerd
Componenten	Localization Registration Client, NVI

Hoofdscenario	De Zorgaanbieder vraagt haar eigen registraties op, voor één Betrokkene of voor alle Betrokkenen.
Postcondities	De Zorgaanbieder kan verschillen constateren en zo nodig corrigeren via verwijderen en opnieuw registreren.

656

UC-NVI-05. Raadplegen van de eigen registraties

657
658

659 11.4. Requirements applicatielaag- en IT-infrastructuurlaag

660 De NVI biedt de volgende functionaliteit:

- 661 - Registreren van gegevensbeschikbaarheid. Een Datahoudende Zorgaanbieder legt vast dat zij
- 662 gegevens van een Betrokkene heeft, met het pseudoniem voor deze Betrokkene, de eigen
- 663 URA en het systeem dat de gegevens beschikbaar stelt.
- 664 - Verwijderen van registraties. Een Datahoudende Zorgaanbieder kan haar registraties per
- 665 systeem verwijderen, gericht op één Betrokkene of breder.
- 666 - Raadplegen van eigen registraties. Een Datahoudende Zorgaanbieder kan opvragen welke
- 667 registraties van haarzelf in de NVI staan, zodat zij kan verifiëren of deze juist zijn. De lijst is
- 668 beperkt tot de eigen registraties.

- Lokaliseren van bronnen. Een Bevragende Zorgaanbieder kan opvragen welke Datahoudende Zorgaanbieders gegevens hebben over een Betrokkene in een bepaalde zoekcontext. Het resultaat is een lijst van datahoudende Zorgaanbieders.
- Geen directe BSN-kennis. De NVI beschikt niet over het BSN, niet in het berichtenverkeer en niet in de opslag. Zie hoofdstuk 9.
- Isolatie tussen bronsystemen. Heeft een zorgaanbieder meerdere bronsystemen (bijvoorbeeld een XIS én een PACS), dan beheert elk systeem uitsluitend zijn eigen registraties, ook binnen dezelfde zorgaanbieder.
- Technische autorisatiecontrole. De NVI controleert zelfstandig of de raadpleger een aangesloten zorgaanbieder is. Dit is een technische controle, geen inhoudelijke toets van de behandelrelatie: die blijft de verantwoordelijkheid van de zorgaanbieder.

11.5. Data/gegevens

Een lokalisatie-record in de NVI bevat op logisch niveau:

- de Datahoudende Zorgaanbieder: de Zorgaanbieder die de gegevens heeft, geïdentificeerd met de URA;
- het burgerpseudoniem: het BSN komt niet in de NVI voor (zie hoofdstuk 9);
- het registrerende systeem: welk bronsysteem van de zorgaanbieder de registratie heeft gedaan, zodat bronsystemen van elkaar gescheiden blijven.

De combinatie van deze gegevens is uniek: dezelfde Datahoudende Zorgaanbieder kan voor dezelfde Betrokkene en hetzelfde systeem niet twee keer voorkomen.

Het zoekresultaat is een lijst van Datahoudende Zorgaanbieders: de raadpleger bevraagt de NVI voor een specifieke zoekcontext en krijgt terug welke Datahoudende Zorgaanbieders daarvoor hebben geregistreerd én akkoord zijn met het delen van hun lokalisatie-record met de Bevragende Zorgaanbieder. Het pseudoniem wordt nooit teruggegeven in een antwoord van de NVI.

11.6. Gedrag en randgevallen

Garanties

- Herhaalde registratie is idempotent. Registreert een Datahoudende Zorgaanbieder dezelfde combinatie nogmaals, dan ontstaat geen duplicaat; de bestaande registratie blijft gelden.
- Een Datahoudende Zorgaanbieder ziet en beheert alleen de eigen registraties. Een Datahoudende Zorgaanbieder kan de registraties van andere Datahoudende Zorgaanbieders niet raadplegen, wijzigen of verwijderen, en kan niet namens een andere Datahoudende Zorgaanbieder registreren.
- Het pseudoniem verlaat de NVI niet.

Randgevallen

De NVI is niet beschikbaar.

Er kan niet worden gelokaliseerd of geregistreerd. Directe gegevensuitwisseling tussen zorgaanbieders gaat door: lokalisatie is geen voorwaarde voor uitwisseling. De voorziening is opgezet als landelijke infrastructuur; beschikbaarheid voor de raadpleger weegt daarbij zwaarder dan het kunnen aanpassen van registraties, dat binnen grenzen tijdelijk onbeschikbaar mag zijn. De technische maatregelen staan in het TO.

Het resultaat is leeg.

Er zijn geen registraties voor deze Betrokkene of voor de registraties die er zijn ontbreekt het akkoord van de Datahoudende Zorgaanbieder voor het delen met de Bevragende Zorgaanbieder. In het laatste geval wordt geen melding getoond dat er wél gegevens zijn maar geen akkoord, omdat dat alsnog het bestaan van gegevens zou onthullen.

Onjuiste registratie.

Een registratie wordt niet gewijzigd: een correctie bestaat uit verwijderen en opnieuw registreren.

Toestemming voor de registratie van lokalisatie-records in de NVI wordt ingetrokken.

De Datahoudende Zorgaanbieder verwijdert haar registraties (UC-NVI-04).

Aansluiting van een Datahoudende Zorgaanbieder wordt ingetrokken.

De registraties van die Datahoudende Zorgaanbieder vervallen mee: gegevens van die Datahoudende Zorgaanbieder worden daarmee in één keer onvindbaar. Intrekken kan voorlopig alleen door de beheerorganisatie.

11.7. Beheer, verantwoordelijkheden en verwijzingen

De NVI wordt beheerd door de beheerorganisatie, die ook aansluitingen beoordeelt en toekent. Dat aansluitproces verloopt buiten de voorziening om en is verder uitgewerkt in het TO. Wie deze beheerorganisatie wordt, is nog niet vastgesteld.

De Datahoudende Zorgaanbieder is verantwoordelijk voor de juistheid en actualiteit van haar eigen registraties, en voor het vaststellen van toestemming vóórdat zij registreert. De NVI controleert die toestemming niet zelf.

De NVI gebruikt van de andere generieke functies: Adressering (voor het opzoeken van type en endpoints van zorgaanbieders na lokalisatie), Identificatie & Authenticatie, Autorisatie en Logging. Hoe die functies technisch worden afgenomen staat in het TO en de Implementation Guide. Daarnaast is de NVI afhankelijk van de PRS (hoofdstuk 9) en van het LRZa als centrale index van zorgaanbieders.

Bewust niet in dit FO: het datamodel, de koppelvlakken en berichtprofielen, de cryptografische uitwerking, de beschikbaarheids- en replicatiemaatregelen en de rate limiting. Die staan in het TO en de Implementation Guide.

12. Pseudoniemenregistratieservice (PRS)

12.1. Rol en doel

De PRS is de privacyvoorziening van de lokalisatiefunctie. De PRS zet het BSN van een Betrokkene om in een pseudoniem, zodat de NVI nooit over het BSN zelf beschikt: niet in het berichtenverkeer en niet in de opslag.

12.2. Stakeholders en hun belang

De PRS wordt aangeroepen door systemen: het XIS of PACS roept de PRS aan bij het registreren van een lokalisatie-record (UC-GFL-01) en bij elke lokalisatievraag (UC-GFL-02).

Stakeholder	Rol	Omschrijving
IT-dienstverlener	Dienstverlener Localization-Registration-Client	Integreert de aanroep in XIS/PACS. Kan registreren en lokaliseren zonder het BSN aan de NVI te hoeven verstrekken.
IT-dienstverlener	Dienstverlener Localization-Search-Client	Integreert de aanroep in XIS/PACS. Kan registreren en lokaliseren zonder het BSN aan de NVI te hoeven verstrekken.
Beheerorganisatie PRS	Dienstverlener PRS	Beheert de voorziening. Verantwoordelijk voor beschikbaarheid en correcte werking van een dienst waarvan zowel registratie als bevraging afhangt.
Burger	Betrokkene	Onderwerp van de pseudonimisering. Het BSN is niet bekend bij de NVI; gegevens zijn bij een eventueel datalek niet tot personen herleidbaar.
Zorgaanbieder (Bronhouder), Zorgverlener	Datahoudende Zorgaanbieder, Eindgebruiker	Indirecte stakeholders die de PRS via hun systeem gebruiken. Registratie en bevraging leiden tot hetzelfde pseudoniem, zodat lokalisatie-records vindbaar zijn.

12.3. usecases

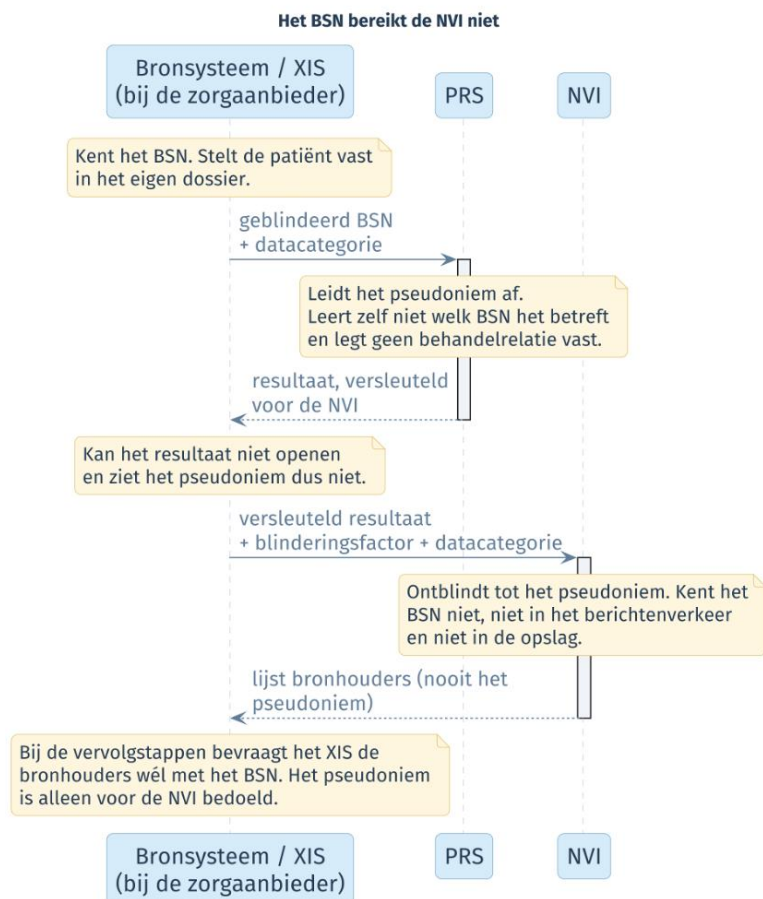
De PRS heeft geen eigen usecase: hij is een ondersteunende stap binnen UC-GFL-01 (registratie) en UC-GFL-02 (lokalisatie). In deze use cases haalt respectievelijk de Localization Registration Client en de Localization Search eerst een pseudoniem op bij de PRS, en pas daarna volgt de aanroep van de NVI.

Wat de PRS functioneel biedt.

Dezelfde Betrokkene leidt bij registratie en bevraging tot hetzelfde pseudoniem, zodat lokalisatie-records vindbaar zijn zonder dat het BSN de NVI bereikt. Een pseudoniem is buiten deze context betekenisloos: ook bij een onverhoopt datalek uit de NVI zijn de gegevens niet tot personen herleidbaar.

Het pseudoniem is bovendien zo opgezet dat de PRS zelf niet weet welke BSN's worden verwerkt, en dat pseudoniemen niet tussen verschillende bronnen of voorzieningen te correleren zijn. De cryptografische werking hiervan staat in het TO en de PRS-specificatie.

Onderstaand diagram laat zien welke identificatie waarheen gaat. Richting de NVI gaat uitsluitend het pseudoniem; het BSN gaat in geblindeerde vorm naar de PRS en verder niet (zie het hoofdstuk Blinding via OPRF in het technisch ontwerp voor een uitleg over blinding). Bij de vervolgstappen bevraagt het XIS de Datahoudende Zorgaanbieders wél met het BSN: het pseudoniem is alleen voor de NVI bedoeld en is daarbuiten betekenisloos.



12.4. Requirements applicatielaag- en IT-infrastructuurlaag

- Geen directe BSN-kennis in de NVI. Een pseudoniem is specifiek voor de NVI, niet bruikbaar in andere systemen en niet direct herleidbaar naar het BSN.
- Consistentie. Dezelfde Betrokkene levert bij registratie en bij bevraging hetzelfde pseudoniem op, anders zijn lokalisatie-records niet vindbaar.
- Onlinkbaarheid. Pseudoniemen zijn niet te correleren tussen bronnen, en de PRS leert zelf niet welke BSN's worden verwerkt.
- Dataminimalisatie. De functie verwerkt alleen gegevens op persoonsniveau voor zover strikt noodzakelijk.

12.5. Data/gegevens

De PRS ontvangt het BSN niet: de Localization Registration Client of Localization Search Client blindeert het voordat het de deur uit gaat, zodat de PRS rekent op een waarde waaruit het BSN niet af te leiden is. De PRS slaat geen behandelinformatie op en legt geen relatie vast tussen Bevragende/Datahoudende Zorgaanbieder en Betrokkene.

12.6. Gedrag en randgevallen

De PRS is niet beschikbaar.

Er kan niet worden geregistreerd en niet worden bevragd; beide vereisen een pseudoniem. Directe gegevensuitwisselingen tussen zorgaanbieders kunnen wel doorgaan. Voor de zorgverlener betekent

dit dat de lokalisatiefunctie tijdelijk geen resultaat kan geven; het XIS moet dit onderscheiden van een leeg resultaat (zie §10.6).

De omzetting mislukt.

De aanroep levert geen bruikbaar pseudoniem op; het XIS behandelt dit als een technische storing, niet als “geen gegevens gevonden”.

De PRS voert geen controle uit op het BSN: de zorgaanbieder is wettelijk verplicht het BSN in het dossier te gebruiken, en de vaststelling en verificatie ervan vinden plaats in het XIS, buiten de lokalisatiefunctie. De PRS zet aan wat wordt aangeboden.

12.7. Beheer, verantwoordelijkheden en verwijzingen

De PRS is een afzonderlijke voorziening onder verantwoordelijkheid van VWS, iRealisatie. De technische werking van de pseudonimisering staat in het TO en het PRS-aansluitdocument.

13. Localization Registration Client

13.1. Rol en doel

De Localization Registration Client is de functionaliteit in het XIS van de Datahoudende Zorgaanbieder waarmee lokalisatie-records worden geregistreerd (bronrol). De Localization Registration Client verbergt de samenwerking tussen de voorzieningen voor de rest van het systeem: hij haalt het pseudoniem op bij de PRS en registreert het lokalisatie-record bij de NVI.

13.2. Stakeholders en hun belang

Stakeholder	Rol	Omschrijving
Zorgverlener	Eindgebruiker	legt data vast in het eigen systeem. De data kan vindbaar worden gemaakt zonder handmatige actie, zonder apart systeem of aparte inlog.
Zorgaanbieder (Bronhouder)	Datahoudende Zorgaanbieder	registreert via het eigen bronsysteem. Registratie verloopt automatisch in het zorgproces, zonder extra handelingen.
IT-dienstverlener	Dienstverlener Localization-Registration-Client	bouwt en beheert de Localization Registration Client. Eén manier van aansluiten, gebaseerd op internationale standaarden, herbruikbaar over klanten.

13.3. Usecases

De Localization Registration Client is de uitvoerende kant van UC-GFL-01 (registratie), UC-GFL-02 (lokalisatie), UC-GFL-04 (verwijderen) en UC-GFL-03 (raadplegen eigen registraties). De usecase-tabellen staan in hoofdstuk 5; hier gaat het om wat de Localization Registration Client daarin doet:

Registreren

Neemt het BSN uit het dossier, haalt het pseudoniem op bij de PRS en registreert bij de NVI namens de eigen URA en het eigen bronsysteem.

Verwijderen

Verwijdert registraties van de eigen bron, bijvoorbeeld wanneer de Betrokkene de toestemming voor het registreren van lokalisatie-records in de NVI intrekt, of een correctie.

Raadplegen

Vraagt de eigen registraties op ter controle.

De journeys in deel A (radioloog registreert beelden, cardioloog zoekt beelden) illustreren deze handelingen vanuit de gebruiker.

13.4. Requirements applicatielaag- en IT-infrastructuurlaag

- Eén manier om lokalisatie-records te registreren.
- Koppelvlakken op basis van internationale standaarden.
- Implementeerbaar voor zorgaanbieders.
- Registreren in het zorgproces. De Localization Registration Client registreert de beschikbaarheid van gegevens op het moment dat die ontstaan, zonder dat de zorgverlener daar een aparte handeling voor hoeft te doen.

13.5. Data/gegevens

De Localization Registration Client verwerkt:

- het BSN: om bij de PRS een pseudoniem op te halen, en bij de vervolgstappen om de gegevens bij de Datahoudende Zorgaanbieders op te vragen. Het BSN gaat niet naar de NVI;
- het pseudoniem: kortstondig, voor de aanroep van de NVI;
- de lokale patiënt-identificer: kortstondig, voor de aanroep van de NVI;

13.6. Gedrag en randgevallen

NVI of PRS niet beschikbaar.

De Localization Registration Client meldt dit als storing. Het zorgproces gaat door en directe gegevensuitwisseling blijft mogelijk.

Geen autorisatie.

Is de aansluiting niet (meer) geldig, dan wordt de vraag afgewezen. De Localization Registration Client toont dit als een probleem met de aansluiting, niet als een leeg resultaat.

Registratie mislukt.

De gegevens zijn wel vastgelegd in het bronsysteem maar niet vindbaar via de NVI. De IT-dienstverlener zorgt dat dit wordt opgemerkt en de registratie alsnog plaatsvindt; herhaalde registratie is idempotent.

Meerdere bronsystemen binnen één zorgaanbieder.

Een XIS en een PACS kunnen beide registreren zonder elkaars registraties te raken.

13.7. Beheer, verantwoordelijkheden en verwijzingen

De Dienstverlener Localization-Registration-Client ontwikkelt en beheert de Localization Registration Client en is verantwoordelijk voor een correcte implementatie van de specificaties. De Datahoudende Zorgaanbieder blijft verantwoordelijk voor wat er namens haar wordt geregistreerd, inclusief het vaststellen van toestemming voor de registratie van lokalisatie-records in de NVI.

Bewust niet in dit FO:

- de schermen en werkwijze in het systeem van de Eindgebruiker: deze zijn leveranciersspecifiek.
- de berichtprofielen, verplichte velden, foutcodes en het conformiteits- en testtraject: Deze staan in de Implementation Guide.

14. Localization Search Client

14.1. Rol en doel

De Localization Search Client is de functionaliteit in het XIS van de Bevrage Zorgaanbieder waarmee lokalisatievragen worden gesteld (raadpleegrol). De Localization Search Client verbergt de samenwerking tussen de voorzieningen voor de rest van het systeem: hij haalt het pseudoniem op bij de PRS, bepaalt de zoekcontext, bevroagt de NVI en levert de URA's van de Datahoudende Zorgaanbieders en de identifiers van de bronsystemen op aan het aanroepende systeem. Het aanroepende systeem vraagt per gevonden Datahoudende Zorgaanbieder met behulp van de generieke functie Adressering (component Query Client) de endpoints op, initieert de elektronische gegevensuitwisseling en presenteert het resultaat aan de Eindgebruiker. Daarmee heeft de Localization Search Client een centrale rol in de keten van de vraag van de Eindgebruiker tot en met het resultaatsscherm.

14.2. Stakeholders en hun belang

Stakeholder	Rol	Omschrijving
Zorgverlener	Eindgebruiker	gebruikt de functie in het eigen systeem. Kan lokaliseren binnen de vertrouwde werkomgeving, zonder apart systeem of aparte inlog.
Zorgaanbieder (Bevragend)	Bevragende Zorgaanbieder	De Localization Search Client handelt namens de Bevragende Zorgaanbieder.
IT-dienstverlener	Dienstverlener Localization-Registration-Client	bouwt en beheert de Localization Search Client. Eén manier van aansluiten, gebaseerd op internationale standaarden, herbruikbaar over klanten.

14.3. Usecases

De Localization Search Client is de uitvoerende kant van UC-GFL-01 (registratie), UC-GFL-02 (lokalisatie), UC-GFL-04 (verwijderen) en UC-GFL-03 (raadplegen eigen registraties). De usecase-tabellen staan in hoofdstuk 5; hier gaat het om wat de Localization Search Client daarin doet:

Lokaliseren

Haalt het pseudoniem op bij de PRS, bepaalt de zoekcontext, stelt de lokalisatievraag, levert de URA's van de Datahoudende Zorgaanbieders en de identifiers van de bronsystemen op aan het aanroepende systeem. Het aanroepende systeem vraagt per gevonden Datahoudende Zorgaanbieder met behulp van de generieke functie Adressering (component Query Client) de endpoints op, initieert de elektronische gegevensuitwisseling en presenteert het resultaat aan de Eindgebruiker.

14.4. Requirements applicatielaag- en IT-infrastructuurlaag

- Eén manier om de lokalisatievraag te stellen. De zorgverlener heeft één manier om te lokaliseren, ongeacht welke voorzieningen de vraag afhandelen.
- Koppelvlakken op basis van internationale standaarden.
- Implementeerbaar voor zorgaanbieders.
- Zoekcontext meegeven. Bij lokaliseren gebruikt de Localization Search Client een zoekcontext om de lokalisatievraag te beperken tot Datahoudende Zorgaanbieders die voor de context van de Eindgebruiker relevant zijn.
- Endpoints opzoeken via GF Adressering. De Localization Search Client zoekt de endpoints van de gevonden Datahoudende Zorgaanbieders niet zelf op maar delegeert dat aan het aanroepende systeem dat hiervoor de generieke functie Adressering gebruikt. Het daadwerkelijk uitvoeren van een elektronische gegevensuitwisseling met een via de generieke functie Lokalisatie gevonden Datahoudende Zorgaanbieder is daarmee afhankelijk van de beschikbaarheid en juistheid van de generieke functie Adressering.
- (Meta)gegevens ophalen en tonen. Het systeem dat de Localization Search Client aanroept, haalt de (meta)gegevens op bij de gevonden Datahoudende Zorgaanbieders en presenteert het resultaat aan de Eindgebruiker.
- Aanvullende presentatie is aan de leverancier van het aanroepende systeem. Extra filtering, sortering of groepering van het resultaat is functionaliteit die deze leverancier zelf ontwikkelt.

14.5. Data/gegevens

De Localization Search Client verwerkt:

- het BSN: om bij de PRS een pseudoniem op te halen, en bij de vervolgstappen om de gegevens bij de Datahoudende Zorgaanbieders op te vragen. Het BSN gaat niet naar de NVI;
- het pseudoniem: kortstondig, voor de aanroep van de NVI;
- de zoekcontext: een lijst van eigenschappen van - voor de context van de Eindgebruiker relevante - Datahoudende Zorgaanbieders;
- het zoekresultaat: de lijst van gevonden Datahoudende Zorgaanbieders.

Wat het aanroepende systeem daarna met het resultaat doet: het opzoeken van de endpoints (gedelegeerd aan GF Adressering), het ophalen van de (meta)gegevens bij de Datahoudende Zorgaanbieders en het tonen daarvan aan de zorgverlener. Die bronbevraging gaat met het BSN: het pseudoniem is uitsluitend bedoeld voor de NVI en is buiten die context betekenisloos.

14.6. Gedrag en randgevallen

Leeg resultaat versus storing.

De Localization Search Client moet onderscheid maken tussen “er zijn geen registraties gevonden die voldoen aan de gegeven zoekcontext én die door de Datahoudende Zorgaanbieder zijn geaccordeerd voor delen met de Bevragende Zorgaanbieder” en “de vraag kon niet worden gesteld” (NVI of PRS onbereikbaar). Voor de zorgverlener zijn dit verschillende situaties: in het eerste geval is vastgesteld dat er niets gevonden is, in het tweede geval is niets vastgesteld.

NVI of PRS niet beschikbaar.

De Localization Search Client meldt dit als storing. Het zorgproces gaat door en directe gegevensuitwisseling blijft mogelijk.

Een Datahoudende Zorgaanbieder geeft geen akkoord op delen lokalisatie-record

Bij een bevraging neemt de NVI alleen de Datahoudende Zorgaanbieders in het antwoord op die

- voldoen aan de zoekcontext; én
- akkoord hebben gegeven op het delen van het lokalisatie-record met de Bevragende Zorgaanbieder.

Voor de Localization Search Client is niet zichtbaar welke Datahoudende Zorgaanbieders wel voldoen aan de zoekcontext en geen akkoord hebben gegeven op het delen van het lokalisatie-record met de Bevragende Zorgaanbieder.

Generieke functie Adressering niet beschikbaar.

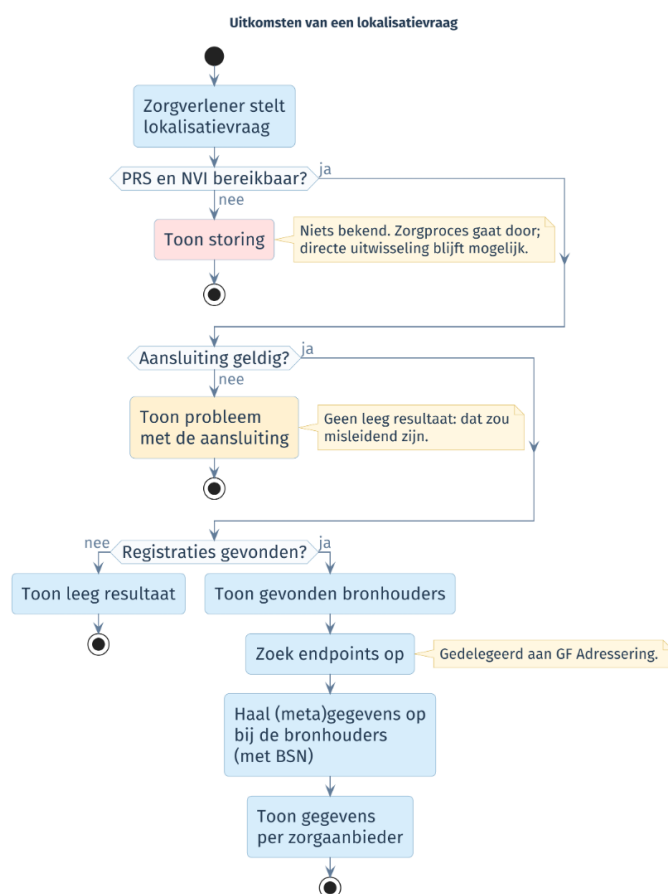
De Datahoudende Zorgaanbieders zijn wel gevonden, maar de endpoints kunnen niet worden opgezocht en de gegevens dus niet worden opgehaald. De Localization Search Client levert een lijst van welke Datahoudende Zorgaanbieders zijn gevonden. Het ophalen van Endpoints en data is buiten scope van de Localization Search Client.

Een Datahoudende Zorgaanbieder is niet bereikbaar.

Bij de overige Datahoudende Zorgaanbieders worden wel gegevens opgehaald. Het systeem van de Eindgebruiker maakt zichtbaar van welke Datahoudende Zorgaanbieders geen gegevens zijn verkregen, zodat het overzicht niet ten onrechte als volledig wordt gelezen.

Geen autorisatie.

Is de aansluiting niet (meer) geldig, dan wordt de vraag afgewezen. De Localization Search Client toont dit als een probleem met de aansluiting, niet als een leeg resultaat.



14.7. Beheer, verantwoordelijkheden en verwijzingen

De Dienstverlener Localization-Search-Client ontwikkelt en beheert de Localization Search Client en is verantwoordelijk voor een correcte implementatie van de specificaties. De Bevrage Zorgaanbieder blijft verantwoordelijk voor wat er namens haar wordt bevestigd, inclusief het ontsluiten van behandelrelaties aan relevante Datahoudende Zorgaanbieders.

Het opzoeken van endpoints van door de Localization Search Client gevonden Datahoudende Zorgaanbieders valt buiten de scope van de Localization Search Client en is afhankelijk van de generieke functie Adressering. Het ophalen van gegevens bij de gevonden Datahoudende Zorgaanbieders valt buiten de scope van de Localization Search Client en is afhankelijk van de beschikbaarheid van de endpoints van de Datahoudende Zorgaanbieders.

Bewust niet in dit FO:

- de schermen en werkwijze in het systeem van de Eindgebruiker: deze zijn leveranciersspecifiek.
- de berichtprofielen, verplichte velden, foutcodes en het conformiteits- en testtraject: Deze staan in de Implementation Guide.

15. Custodian server

15.1. Rol en doel

De Custodian server is de component (in het XIS) van de Datahoudende Zorgaanbieder die antwoordt op de vraag van de NVI: "Gaat de Datahoudende Zorgaanbieder akkoord met het delen met de Bevrage Zorgaanbieder B van het lokalisatie-record aangaande de Betrokkene met lokaal pseudoniem P?". Om te bepalen of dat akkoord kan worden gegeven, toetst (een systeem van) de Datahoudende Zorgaanbieder of er een grondslag en/of beperking van toepassing is.

15.2. Stakeholders en rollen

Stakeholder	Rol	Omschrijving
Zorgverlener	Eindgebruiker	kan alleen data inzien van Datahoudende Zorgaanbieders die akkoord hebben gegeven op het delen van het lokalisatie-record met de Bevrage Zorgaanbieder
Zorgaanbieder (Bronhouder)	Datahoudende Zorgaanbieder	<ul style="list-style-type: none"> - heeft door de Custodian Server regie over het ontsluiten van eerder in de NVI geregistreerde lokalisatie-records aan een specifieke Bevrage Zorgaanbieder. - bepaalt zelf of er een grondslag (bijvoorbeeld een OTV- of DHTV-toestemming) en/of beperking van toepassing is
Zorgaanbieder (Bevrage)	Bevrage Zorgaanbieder	krijgt alleen inzage in lokalisatie-records die zijn geaccordeerd.
IT-dienstverlener	Dienstverlener Custodian-server	bouwt en beheert de Custodian server. Een manier van aansluiten, gebaseerd op internationale standaarden, herbruikbaar over klanten.

15.3. Usecases

De Custodian server heeft een rol in UC-GFL-02 (lokalisatie). De usecase-tabel staat in hoofdstuk 5; hier gaat het om wat de Custodian server in die usecase doet.

Lokaliseren

De Custodian server ontvangt een verzoek van de NVI "Gaaf de Datahoudende Zorgaanbieder akkoord met het delen met de Bevragefde Zorgaanbieder B van het lokalisatie-record aangaande de Betrokkene met lokaal pseudoniem P?". Om te bepalen of dat akkoord kan worden gegeven, toetst een systeem van de Datahoudende Zorgaanbieder of er een grondslag en/of beperking van toepassing is. Op basis van deze toets antwoordt de Custodian server aan de NVI "Akkoord" of "Niet akkoord".

15.4. Requirements applicatielaag- en IT-infrastructuurlaag

- De NVI ondersteunt 1 manier om de lokalisatie-accordering-vraag te stellen en de Datahoudende Zorgaanbieder ondersteunt één manier om de lokalisatie-accordering-vraag te ontvangen en beantwoorden.
- Koppelvlakken op basis van internationale standaarden.
- Implementeerbaar voor zorgaanbieders.
- Systeemkoppeling. De Custodian server accordeert op het moment dat een vraag binnenkomt, zonder dat een zorgverlener daar een aparte handeling voor hoeft te doen.
- Aanvullende presentatie is aan de leverancier van het aanroepende systeem. Extra filtering, sortering of groepering van het resultaat is functionaliteit die deze leverancier zelf ontwikkelt.

15.5. Data

De Custodian server ontvangt het BSN niet. De vraag aan de Custodian server bevat het lokale pseudoniem van de burger dat onderdeel is van het in de NVI geregistreefde lokalisatie-record. De Custodian server is een dienst van een verwerker van de Datahoudende Zorgaanbieder.

15.6. Gedrag en randvoorwaarden

Authenticatie van NVI faalt

Alleen de NVI mag de lokalisatie-accordering-vraag stellen. Indien de authenticatie van een client die een lokalisatie-accordering-vraag stelt, faalt, mag de Custodian server geen antwoord geven dat informatie over de Betrokkene onthult.

15.7. Beheer, verantwoordelijkheden en verwijzingen

De Dienstverlener Custodian-server ontwikkelt en beheert de Custodian server en is verantwoordelijk voor een correcte implementatie van de specificaties. De Datahoudende Zorgaanbieder blijft verantwoordelijk voor het accorderen van het delen van lokalisatie-records met specifieke Bevragefde Zorgaanbieders, inclusief het vaststellen of er een grondslag en/of beperking van toepassing is.

16. LMR (optioneel)

NEN 7519

NEN 7519 bevat eisen voor het vastleggen en uitwisselen van gegevens die beschrijven waar bepaalde lokaliseerbare datasets beschikbaar en opvraagbaar zijn. In de architectuur van de generieke functies

is de NEN 7519 bedoeld als de normatieve basis voor de inrichting van Lokalisatie Metadata Registers (LMR's).

De norm beschrijft daarmee de informatiestructuur van de gegevens die als antwoord op een lokalisatievraag vanuit een LMR kunnen worden verstrekt. Na bevraging van een LMR worden de resultaten volgens de informatiestructuur van NEN 7519 teruggegeven aan de zorgmedewerker die de lokalisatievraag stelt. De NEN 7519 is daarmee vooral gericht op wat aan gegevens moet worden vastgelegd en uitgewisseld vanuit een LMR.

Lokalisatie Metadata Registers

Binnen de generieke functie Lokalisatie zijn LMR's voorzien als optionele decentrale componenten. De NVI (in samenhang met de PRS) is daarbij de centrale component en geeft op hoofdlijnen antwoord op de vraag waar bij welke zorgaanbieder relevante gezondheidsgegevens beschikbaar zijn. LMR's zijn bedoeld om hierboven op een fijnmazigere lokalisatie mogelijk maken.

Een LMR kan bijvoorbeeld aanvullende metadata bevatten over radiologische beelden, zoals het type onderzoek, de datum van het onderzoek, de gebruikte modaliteit of de relatie met een bepaalde diagnose. Daarmee kan een zorgmedewerker op basis van metadata bepalen welke gegevens mogelijk relevant zijn, voordat de onderliggende gegevens daadwerkelijk worden opgevraagd.

LMR's zijn niet bedoeld als verplichte voorzieningen, maar bieden ruimte voor sectorale, regionale of private initiatieven en innovatie vanuit het zorgveld. VWS heeft daarnaast geen rol in de ontwikkeling of bouw van LMR's. In de opzet van de generieke functie Lokalisatie wordt dus aan het zorgveld ruimte geboden voor het ontwikkelen van een LMR, in het geval dat er vanuit het zorgveld een concrete behoefte is aan fijnmaziger lokaliseren voor specifieke use-cases.

Een LMR kan op verschillende manieren worden ingericht. Een eerste mogelijkheid is een component binnen of als uitbreiding van het bronsysteem van een zorgaanbieder. Een tweede mogelijkheid is het positioneren een LMR op een andere plaats dan bij de bron. Een mogelijk voorbeeld hiervan is een index voor het faciliteren van fijnmazig lokaliseren van beeldvormende onderzoeken.

Ongeacht de gekozen inrichting moeten de lokalisatiegegevens die door een LMR worden verstrekt, voldoen aan de informatiestructuur van de NEN 7519 en aan de informatiestandaard Lokalisatie.

Informatiestandaard

Om de interactie met LMR's verder te standaardiseren is aan Nictiz gevraagd om een informatiestandaard voor Lokalisatie op te stellen. Deze informatiestandaard bouwt voort op NEN 7519 en werkt de interacties met LMR's nader uit.

Waar NEN 7519 de eisen en informatiestructuur voor het vastleggen en uitwisselen van lokalisatiegegevens beschrijft, moet de informatiestandaard van Nictiz dit vertalen naar de praktische uitwisseling tussen systemen en voorzieningen. Daarmee wordt de wijze waarop een LMR kan worden bevraagd en waarop een antwoord wordt teruggegeven verder gestandaardiseerd.

Bijlage 1: Requirements

Dit hoofdstuk bevat de volledige lijst van requirements van Github. Deze is te vinden op <https://github.com/orgs/minvws/projects/60/views/1>.

Functionele requirements

Gerealiseerde functionele requirements

Onderstaande requirements worden gerealiseerd in deze versie van de generieke functie Lokalisatie.

#	Titel	Status	Type
54	Als bronhouder moet ik lokalisatiegegevens kunnen aan- en afmelden alsmede updaten.	Beoordeeld	Functioneel
50	Als zorgverlener heb ik 1 manier om de lokalisatievraag te stellen, deze kan dan via verschillende voorzieningen worden afgehandeld.	Beoordeeld	Functioneel
31	Als zorgverlener kan ik gegevens lokaliseren op basis van het BSN van de patiënt/burger	Beoordeeld	Functioneel
67	Als zorgverlener wil ik lokaliseren op basis van datasets	Beoordeeld	Functioneel
28	De bronhouder wil alleen relevante lokalisatiegegevens beschikbaar stellen.	Beoordeeld	Functioneel
37	De functie verwerkt alleen gegevens op persoonsniveau indien strikt noodzakelijk	Beoordeeld	Functioneel
38	De lokalisatiefunctie kan gebruikt worden voor uitwisselingen waarbij gegevens gericht beschikbaar worden gesteld	Beoordeeld	Functioneel
40	Een raadplegende zorgverlener wil alle relevante bronhouders kunnen lokaliseren	Beoordeeld	Functioneel
29	Niemand mag beschikken over lokalisatiegegevens waar hij niet voor geautoriseerd is.	Beoordeeld	Functioneel
55	Als bronhouder, die lokalisatiegegevens deelt, moet je ook zelf kunnen aangeven welke zorgverleners er over mogen beschikken.	Beoordeeld	Functioneel

Niet-gerealiseerde functionele requirements

De volgende functionele requirements zijn nog niet beschikbaar in deze versie van Lokalisatie.

#	Titel	Status	Type
35	Als PGO/MGO wil ik gebruik kunnen maken van de lokalisatiefunctie om bronnen te vinden.	Beoordeeld	Functioneel
32	Als burger wil ik kunnen zien wie mijn lokalisatieinformatie heeft geraadpleegd.	Beoordeeld	Functioneel
45	Als persoon wil ik dat gegevens die ik zelf beheer, bijvoorbeeld in mijn PGO, lokaliseerbaar kunnen worden voor zorgverleners.	Beoordeeld	Functioneel
42	Als persoon wil ik een overzicht van mijn (zorg)netwerk kunnen gebruiken om gegevens te lokaliseren.	Beoordeeld	Functioneel
68	Als zorgverlener wil ik dat er achteraf aangetoond kan worden welke gegevens op welk moment voor mij beschikbaar zodat ik mijn beslissingen kan verantwoorden	Beoordeeld	Functioneel
43	Als zorgverlener wil ik een overzicht van een (zorg)netwerk kunnen gebruiken om gegevens te lokaliseren.	Beoordeeld	Functioneel
51	Casus netwerkzorg: Alle zorgaanbieders inzichtelijk binnen het netwerk, vervolgens een filter welke zorgaanbieders toestemming om te delen en welke data/gegevens er dan beschikbaar zijn.	Afgewezen	Functioneel
52	De lokalisatiefunctie moet voldoen aan de NEN-norm 7513 voor logging.	Beoordeeld	Functioneel
30	De lokalisatiefunctie onthult de informatievraag van de raadpleger alleen aan relevante bronhouders.	Beoordeeld	Functioneel
44	Naast de landelijke lokalisatievoorziening moeten er in de lokalisatiefunctie ook andere manieren mogelijk zijn om patiëntgegevens te lokaliseren.	Beoordeeld	Functioneel

1089 Niet-functionele requirements

#	Titel	Status	Type
57	Als ICT leverancier van een zorgapplicatie wil ik met koppelvlakken o.b.v. internationale standaarden gegevens kunnen lokaliseren (opvrager) en lokaliseerbaar maken (bron)	Beoordeeld	Niet functioneel
26	Bij het onbeschikbaar zijn van de lokalisatie functie moeten directe gegevensuitwisselingen door kunnen gaan	Beoordeeld	Niet functioneel
53	De adressen die in de volle breedte na lokalisatie en adressering nodig zijn moeten aan eisen voor persistentie voldoen.	Beoordeeld	Niet functioneel
27	De lokalisatie functie moet implementeerbaar zijn voor zorgaanbieders	Beoordeeld	Niet functioneel

#	Titel	Status	Type
56	De lokalisatiefunctie moet voldoen aan security en privacy by design	Beoordeeld	Niet functioneel
39	De werking van de lokalisatiefunctie moet rekening houden met (Europese) wetgeving en programmas.	Beoordeeld	Niet functioneel

1090

1091

1092

1093

Bijlage 2: Definities

Onderstaande lijst beschrijft de belangrijkste begrippen en afkortingen die in dit document worden gebruikt. De lijst is bedoeld om consistent woordgebruik binnen de generieke functies te ondersteunen en sluit aan op de terminologie van het FO van de generieke functie Adressering.

Begrip / afkorting	Definitie
Adressering	De generieke functie Adressering maakt het mogelijk om digitale en fysieke adressen, organisatieonderdelen en zorgdiensten van zorgaanbieders op een gestandaardiseerde wijze te registreren, beheren en raadplegen.
Autorisatie	De generieke functie Autorisatie bepaalt welke gegevens een persoon, systeem of organisatie mag bekijken, gebruiken of wijzigen. De functie zorgt ervoor dat toegang aansluit bij de rol, verantwoordelijkheid en betrokkenheid van een persoon, systeem of organisatie.
Beheerorganisatie	Organisatie die verantwoordelijk is voor het functioneel en technisch beheer van de NVI.
Datahoudende Zorgaanbieder	Zorgaanbieder die gegevens van een patiënt onder zich heeft en de aanwezigheid daarvan registreert in de NVI.
BSN	Burgerservicenummer; wettelijk persoonsnummer waarmee een patiënt wordt geïdentificeerd. Wordt in het verkeer met en de opslag van de NVI uitsluitend gepseudonimiseerd gebruikt.
Burger	Burger wordt in dit document gebruikt als brede, niet-juridische overkoepelende term voor de natuurlijke persoon aan de vraagzijde van gezondheid en zorg, waaronder afhankelijk van de context ook patiënt, cliënt en zorgvrager vallen. Bron: GISA
Datacategorie	Gestandaardiseerde code voor het type gegevens dat via een endpoint van een Datahoudende Zorgaanbieder beschikbaar wordt gesteld. De codes komen uit een landelijk beheerde waardelijst, gebaseerd op een gereduceerde set zorginformatiebouwstenen (ZIB's). De volledige codelijst staat in de Implementation Guide.
EHDS	European Health Data Space; Europees kader voor gezondheidsdata waarmee de werking van de lokalisatiefunctie rekening houdt.
Generieke functies	Het samenhangende stelsel van zes functies — Identificatie & Authenticatie, Autorisatie, Toestemming, Lokalisatie, Adressering en Logging — dat elektronische gegevensuitwisseling in de zorg ondersteunt.
FO	Functioneel Ontwerp; beschrijft de functionaliteit, zonder technische implementatiedetails.
TO	Technisch Ontwerp; technische uitwerking van het FO.
Gezondheidsdata	Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven

	Dit is een juridische term: op het moment dat data volledig geanonimiseerd is of geen betrekking heeft op een persoon, valt deze niet onder de AVG. Bron: GISA
Identificatie & Authenticatie	Generieke functie die zorgt voor een veilige manier van inloggen van de zorgverlener.
Implementation Guide (IG)	Document met de technische specificaties waarmee leveranciers de functionaliteit implementeren.
IT-dienstverlener	Partij die namens een zorgaanbieder technisch beheer uitvoert en, na autorisatie door de zorgaanbieder, lokalisatie-records registreert en beheert.
LDN	Programma Landelijk Dekkend Netwerk, uitgevoerd onder regie van het Ministerie van VWS.
Logging	Generieke functie die vastlegt wie welke gegevens heeft opgevraagd of gewijzigd.
Lokalisatie	Generieke functie die inzichtelijk maakt welke zorgaanbieders beschikken over relevante gegevens van een patiënt.
Lokalisatievraag	Bevraging van de NVI met een gepseudonimiseerd BSN en een zoekcontext, met als resultaat een lijst van Datahoudende Zorgaanbieders die akkoord hebben gegeven op het delen van het lokalisatie-record met de Bevragende Zorgaanbieder.
Lokalisatie-record	Registratie in de NVI waarmee een Datahoudende Zorgaanbieder vastlegt dat hij gegevens over een patiënt beschikbaar heeft.
NEN 7513	Nederlandse norm voor het loggen van toegang tot patiëntgegevens.
NVI	Nationale Verwijsindex; de gemeenschappelijke voorziening binnen de generieke functie Lokalisatie waarin lokalisatie-records worden geregistreerd en bevroegd.
PACS	Picture Archiving and Communication System; systeem voor het opslaan en uitwisselen van beeldmateriaal.
PGO / MGO	Persoonlijke respectievelijk medische gezondheidsomgeving waarin een persoon zelf gegevens beheert.
PKIoverheid-certificaat	Digitaal certificaat waarmee een organisatie of beheerder zich tegenover een voorziening authenticceert.
PRS	Pseudoniemenregistratieservice; afzonderlijke dienst die het pseudonimiseren van het BSN uitvoert.
Pseudonimisering	Beveiligingsmaatregel waarbij het BSN wordt omgezet in een pseudoniem zodat de gegevens niet door derden tot een persoon herleidbaar zijn.
Raadpleger	Zorgverlener of zorgtoepassing die lokalisatiegegevens opvraagt.
Toestemming	Generieke functie die de toestemming van de patiënt voor het delen van gegevens beheert.
URA	Unieke Zorgaanbiedersidentificatie waarmee de bronhoudende zorgorganisatie wordt aangeduid.
Wegiz	Wet elektronische gegevensuitwisseling in de zorg.

XIS	Zorginformatiesysteem van een zorgaanbieder (bijvoorbeeld een EPD of PACS) waarmee lokalisatie-records worden geregistreerd en lokalisatievragen worden uitgevoerd.
Zorgaanbieder	Organisatie die zorg verleent en, als Datahoudende Zorgaanbieder, lokalisatiegegevens registreert en beheert.
Zorgverlener	Professional die zorg verleent en gegevens van een patiënt lokaliseert ten behoeve van gegevensuitwisseling.

1099