



# IST EN SOLL ONDERZOEK VOOR DE GENERIEKE FUNCTIE ADRESSEREN



Ministerie van Volksgezondheid,  
Welzijn en Sport

**Datum**  
**Versie**

29 augustus 2023  
1.0

**D&A medical group BV**  
Postbus 71  
4180 BB Waardenburg  
[www.dnagroup.nl](http://www.dnagroup.nl)



## INHOUDSOPGAVE

<b>1</b>	<b>OPDRACHTOMSCHRIJVING EN ONDERZOEKSAANPAK .....</b>	<b>4</b>
<b>1.1</b>	<b>OMSCHRIJVING VAN DE OPDRACHT .....</b>	<b>4</b>
<b>1.2</b>	<b>ONDERZOEKSAANPAK.....</b>	<b>5</b>
<b>2</b>	<b>PROBLEEMDEFINITIE EN FUNCTIONELE BEHOEFTE .....</b>	<b>7</b>
<b>2.1</b>	<b>INTRODUCTIE.....</b>	<b>7</b>
<b>2.2</b>	<b>DEFINITIE .....</b>	<b>7</b>
<b>2.3</b>	<b>FUNCTIONELE BEHOEFTE ADRESSEREN .....</b>	<b>8</b>
<b>2.4</b>	<b>SAMENHANG VAN FUNCTIES.....</b>	<b>8</b>
<b>3</b>	<b>IST - BESCHIKBARE OPLOSSINGEN .....</b>	<b>10</b>
<b>3.1</b>	<b>ZORG-AB.....</b>	<b>10</b>
<b>3.2</b>	<b>ZORGDOMEIN .....</b>	<b>13</b>
<b>3.3</b>	<b>NUTS .....</b>	<b>14</b>
<b>3.4</b>	<b>CHIPSOFT .....</b>	<b>16</b>
<b>3.5</b>	<b>EPIC .....</b>	<b>18</b>
<b>3.6</b>	<b>ENOVATION .....</b>	<b>19</b>
<b>3.7</b>	<b>LSP.....</b>	<b>20</b>
<b>3.8</b>	<b>CONCLUSIE HUIDIGE OPLOSSINGEN.....</b>	<b>22</b>
<b>4</b>	<b>TOETSINGSKADER .....</b>	<b>23</b>
<b>5</b>	<b>SOLL – MOGELIJKE SECTOROVERSTIJGENDE OPLOSSINGEN.....</b>	<b>25</b>
<b>5.1</b>	<b>MOGELIJKE OPLOSSINGEN .....</b>	<b>25</b>
<b>5.2</b>	<b>ANALYSE PER OPLOSSING.....</b>	<b>32</b>



<b>6</b>	<b>CONCLUSIE EN ADVIES .....</b>	<b>36</b>
<b>6.1</b>	<b>CONCLUSIE.....</b>	<b>36</b>
<b>6.2</b>	<b>ADVIES EN ROADMAP .....</b>	<b>37</b>
<b>7</b>	<b>BIJLAGEN .....</b>	<b>39</b>
<b>7.1</b>	<b>AFKORTINGEN EN BEGRIPPEN .....</b>	<b>39</b>
<b>7.2</b>	<b>SAMENHANG VAN GENERIEKE FUNCTIES.....</b>	<b>41</b>
<b>7.3</b>	<b>ADRESSEREN VAN PATIËNTEN .....</b>	<b>42</b>
<b>7.4</b>	<b>TOETSINGSKADER .....</b>	<b>43</b>
<b>7.5</b>	<b>IST EN SOLL VISUALISATIES.....</b>	<b>55</b>
<b>7.6</b>	<b>DETAIL ANALYSE SOLL .....</b>	<b>61</b>
<b>7.7</b>	<b>GERAADPLEEGDE BRONNEN.....</b>	<b>65</b>
<b>7.8</b>	<b>GEÏNTERVIEWDE PARTIJEN.....</b>	<b>67</b>



# 1 OPDRACHTOMSCHRIJVING EN ONDERZOEKSAANPAK

## Omschrijving van de opdracht

### 1.1.1 Achtergrond

Om passende zorg te kunnen leveren, moeten zorgverleners op het juiste moment kunnen beschikken over de juiste informatie op de juiste plek. Dat is niet altijd het geval. Daartoe is in het coalitieakkoord van het huidige kabinet een intensivering opgenomen op de standaardisatie van gegevensuitwisseling in de zorg. Dit wil zeggen dat er vergaande afspraken nodig zijn met welke taal er uitgewisseld wordt en op welke wijze.

De Tweede Kamer heeft onlangs een grote stap gezet in dit kader door de Wet elektronische gegevensuitwisseling in de zorg (Wegiz) aan te nemen. Met deze wet maken het zorgveld en leveranciers afspraken over deze taal en techniek. Maar er is meer nodig aan randvoorwaarden om digitale gegevensuitwisseling in de zorg te realiseren waarbij meer regie vanuit de overheid noodzakelijk is. Eén van die voorwaarden is het tot stand komen van generieke functies. Generieke functies zijn functies die zorgbreed voor meerdere toepassingsgebieden nodig zijn om vindbaarheid, toegankelijkheid en maximale interoperabiliteit te kunnen realiseren. De overheid heeft zes generieke functies geprioriteerd: toestemming, identificatie, authenticatie, autorisatie, lokalisering en adressering.

In het Integraal Zorgakkoord (IZA) is afgesproken dat hiertoe 6 generieke functies moeten worden ingevuld met afspraken en/of voorzieningen. Deze generieke functies zijn uiterlijk in 2025 sectoroverstijgend beschikbaar en worden in de praktijk gebruikt. Voor de langere termijn (2035) kijkt de minister naar hoe deze keuzes ook bijdragen aan de doorontwikkeling van generieke functies, waarbij er verschillende oplossingen kunnen bestaan maar dat deze dan wel interoperabel zijn (Integraal Zorgakkoord, 2022). Mede daarom is aanvullend hierop in zomer 2022 opdracht gegeven aan de NEN om voor vier generieke functies een NEN-normeringstraject te starten. Inmiddels zijn deze gestart en worden deze in drie norm trajecten opgepakt te weten: Identificatie en authenticatie, Toestemming, Lokalisatie.

Met bovenstaand in het achterhoofd is de keuze gemaakt om voor de generieke functies lokalisatie, autorisatie en adressering een Opdracht uit te zetten. Dit omdat er op dit moment geen landelijke afspraken zijn over het gebruik van een oplossing en zo niet wordt voldaan aan de afspraken in het IZA. De functie lokalisatie heeft hierin prioriteit, omdat hier een grotere vraag naar is en bij kan dragen aan de ontwikkeling van de eerdergenoemde NEN-norm.

### 1.1.2 De opdracht

De aard van de Opdracht is het in kaart brengen van de huidige situatie op het gebied van oplossingen (afspraken/standaarden en voorzieningen) voor drie generieke functies lokalisatie, autorisatie en adressering en het ontwikkelperspectief van deze oplossingen voor de langere termijn, waarbij interoperabiliteit binnen een federatief gedachtengoed essentieel is. Hierbij wordt tevens een duidelijk focus op de korte termijn, het behalen van de IZA doelstellingen, gevraagd.



Hierbij moeten de volgende vragen beantwoord worden:

1. *Wat is de functionele behoefte van de generieke functie?*
2. *Welke beschikbare oplossingen (standaarden, afspraken en/of voorzieningen) zijn er of zijn in ontwikkeling die invulling geven aan deze functionele behoefte?*
3. *Leiden deze beschikbare oplossingen voor zowel de korte als de lange termijn tot een interoperabele en zorgbrede oplossing voor de functionele behoefte van deze generieke functie?*
4. *Wat zijn de (maatschappelijke) kosten van deze oplossingen en staan die in verhouding tot de baten?*

### 1.1.3 Resultaten

Het resultaat van deze IST-SOLL analyse geeft een overzicht van de huidige situatie en de mogelijke oplossingen, en maakt het mogelijk om op inhoudelijke gronden (o.a. technisch, financieel, operationeel) een keuze te maken voor een werkende (combinatie van) oplossing(en) per 2025 en het ontwikkelperspectief voor de langere termijn.

Voor u ligt het rapport voor de generieke functie adresseren. Het rapport biedt:

- Een overzicht van de beschikbare oplossingen voor de functie Adresseren;
- Een analyse van de organisatorische-, technische- en politieke haalbaarheid per oplossing;
- Een inschatting van de haalbaarheid van een sectoroverstijgende implementatie per 2025;
- Analyse van de eventuele combinatie van oplossingen en gevolgen van deze combinatie(s).
- Visualisatie van elke oplossingsrichting. De visualisaties geven de verschillen weer tussen de verschillende oplossingen per laag van het interoperabiliteitsmodel. Deze visualisaties zijn gemaakt met de IST-SOLL modelleringstool die door VZVZ en BeBright is ontwikkeld.

## Onderzoeksaanpak

Voor het onderzoek naar de functie Adresseren zijn de volgende stappen doorlopen.

### Stap 1. Probleemdefinitie en een analyse van de functionele behoeften.

Ten behoeve van het doorgronden van het probleem en de (functionele) behoeften voor een functie Adresseren hebben een tweetal workshops plaats gevonden met een multidisciplinair team van experts, het expertteam. In deze workshops maken we gebruik van de methode van 'Design Thinking'. Een methode die gebruikt wordt om voor complexe vraagstukken innovatieve oplossingen te genereren en te testen/toetsen. Figuur 1 illustreert een schematische weergave van dit proces.

De eerste 3 stappen in het Design Thinking proces Empathize, Define en Ideate bieden een creatieve en out-of-the-box aanpak om behoeften vanuit het perspectief van toekomstige gebruikers te doorgronden, te definiëren en creatieve oplossingen te bedenken.



*Figuur 1 Design Thinking proces*

Om het vraagstuk vanuit verschillende perspectieven te belichten is een multidisciplinair expertteam samengesteld. Het expertteam bestaat uit zorgverleners (de functionele gebruikers), vertegenwoordiging van de RSO's en van Health-RI (secundair gebruik), systeemarchitecten uit de zorg, systeemleveranciers die de functie in de toekomst zullen moeten gebruiken en/of implementeren en de huidige leveranciers van een adresseringsfunctie. De uitkomsten van deze workshops zijn samengevat in hoofdstuk 2.

Stap 2. Consultatie van partijen die oplossingen voor adressering ontwikkelen en implementeren. Parallel aan de workshops met het expertteam, hebben semigestructureerde interviews plaats gevonden met partijen die (deel)oplossingen ontwikkelen en bieden voor adressering. Zie bijlage 7.8 voor een overzicht van de geïnterviewde partijen.

De oplossingen die we uit deze consultaties ophalen worden op een eenduidige manier beschreven aan de hand van het Nictiz lagenmodel (zie hoofdstuk 3). Tevens is er een visualisatie gemaakt met behulp van de beeldtaal die in het kader van het project "IST en SOLL op basis van model" door VZVZ en BeBright is ontwikkeld (zie bijlage 7.5).

Stap 3. Een analyse van de haalbaarheid van de oplossingen.

Voor de analyse van de functionele, technische, organisatorische en politieke haalbaarheid hebben we het toetsingskader gebruikt dat is ontwikkeld ten behoeve van het onderzoek naar een landelijk netwerk van infrastructuren voor gegevensuitwisseling in de zorg (D&A Medical Group, 2022). De toepassing van het toetsingskader wordt beschreven in hoofdstuk 4 en het volledige toetsingskader is opgenomen in bijlage 7.4.

De analyse en beoordeling van de oplossingen is samengevat in hoofdstuk 5. Zo krijgen we inzichtelijk welke oplossingen functioneel het meest geschikt zijn en in welke mate de oplossingen voldoen aan de leidende principes. In de beoordeling nemen we tevens mee welke oplossing het best passend is bij de beleidslijn van het Ministerie van VWS inzake de ontwikkelrichting voor een landelijke infrastructuur voor gegevensuitwisseling en databeschikbaarheid in de zorg. Een visualisatie van de gewenste oplossingsrichting (SOLL) is opgenomen in bijlage 7.5.

Bovenstaande analyses leiden tot een conclusie wat mogelijke, en vooral ook best passende, oplossingen zijn voor de functie Adresseren, zowel voor de korte als voor de lange termijn, zie hoofdstuk 6.



## 2 PROBLEEMDEFINITIE EN FUNCTIONELE BEHOEFTE

### Introductie

Om tot een goed begrip te komen van het vraagstuk adresseren en de functionele behoeften voor een generieke functie Adresseren zijn een tweetal workshops gehouden met een multifunctioneel team van experts, volgens de methode van Design Thinking.

Om focus te houden op de daadwerkelijke behoeften is vertrokken vanuit 3 zorgprocessen waarbij het delen en beschikbaar zijn van medische en zorgdata essentieel is:

1. Acute zorg, aan de hand van de casus van een mevrouw met een medische voorgeschiedenis die wegens een gebroken heup acuut wordt opgenomen in een ander ziekenhuis dan waar de patiënt onder behandeling is. Dit betreft informatie beschikbaar bij niet-planbare zorg. In dit geval kan op voorhand niet bepaald worden welke specifieke gegevens de zorgverlener van deze patiënt nodig heeft, of waar deze gegevens zich bevinden.
2. Chronische zorg in een netwerk van huisarts, medisch specialist en wijkverpleging, aan de hand van de casus van een man met een ernstige vorm van diabetes type I, die zelfstandig woont met ondersteuning van wijkzorg. Doordat er geen overkoepelende formele (contractuele) afspraken of vooraf afgebakende verantwoordelijkheden tussen de individuele zorgverleners die samenwerken zijn gemaakt, dient er “rondom de patiënt” iets geregeld te worden om gegevensuitwisseling binnen het netwerk mogelijk te maken.
3. Informatieoverdracht over de patiënt van de ene naar een andere zorgverlener. Bijvoorbeeld bij verwijzing of een overdracht van de patiënt (waarbij de verantwoordelijkheid wordt overgedragen naar een andere behandelaar), of het expliciet betrekken van één of meerdere andere zorgverlener(s) (medebehandelaars) bij de behandeling, zonder overdracht van verantwoordelijkheid. Bijvoorbeeld bij consultatie, diagnostiek of bij een (multidisciplinair) overleg.

Voor deze processen hebben we gekeken naar de belemmeringen en problemen die momenteel worden ervaren bij het digitaal adresseren.

Compleetheid van functionele behoeften is niet nagestreefd. Behoeften zullen namelijk evolueren in de tijd omdat er steeds weer nieuwe, andere vormen van samenwerking ontstaan. Flexibiliteit van een oplossingsrichting om met deze veranderende en nieuwe behoeften om te kunnen gaan, is daarom van belang. Dit is verwoord in het leidende principe “Duurzaam” (zie hoofdstuk 4: Toetsingskader).

### Definitie

Gedurende het onderzoek hebben we geconstateerd dat het begrip adresseren niet eenduidig is. Adresseren gaat enerzijds over het bepalen van technische adresgegevens als ook de contactgegevens van zorgaanbieders, zorgverleners en patiënten. In dit onderzoek wordt de onderstaande definitie voor adresseren gehanteerd:

*‘Adressering geeft antwoord op de vraag wat het “digitale adres” van de ontvanger of bron is.’*



Het Uitwisselkompas (VZVZ, 2022) onderscheidt twee situaties waarin adresseren noodzakelijk is: Adressering is noodzakelijk bij het gericht versturen en bij het ongericht beschikbaar stellen van informatie.

- Bij het **gericht versturen van gegevens** (push-verkeer) worden gegevens vanuit het systeem van de dossierhouder direct naar een bekende ontvanger gestuurd, bijvoorbeeld bij een verwijzing. In dit geval moet de functie adresseren antwoord geven op de vraag wat het “digitale adres” van de ontvanger is.
- Het **onggericht beschikbaar stellen van gegevens** (pull-verkeer) gebeurt na lokalisatie. Op het moment dat een zorgverlener (of het systeem) weet waar gegevens van een patiënt bekend zijn, moet de adresseringsfunctie antwoord geven op de vraag wat het “digitale adres” van de bron is. Zo kunnen de gegevens daadwerkelijk opgevraagd worden.

## Functionele behoeften adresseren

Zorgverleners formuleren onderstaande essentiële behoeften ten aanzien van de functie Adresseren:

1. Als zorgverlener wil ik onderscheid kunnen maken tussen wie of wat ik adresseer: een zorgaanbieder, een specifieke afdeling of een specifieke zorgverlener.
2. Als zorgverlener wil ik andere zorgverleners/zorgaanbieders niet alleen digitaal kunnen bereiken, maar tevens wil ik dat de (logische) naam en de contactgegevens van de zorgaanbieder/zorgverlener aan het elektronische adres gekoppeld zijn.
3. Als zorgverlener wil ik patiënten digitaal kunnen adresseren, via e-mail of een PGO.

In de workshops met het expertteam en interviews hebben we vastgesteld dat de invulling van de functionele behoeften ten aanzien van het adresseren van patiënten anders is dan die voor het adresseren van zorgaanbieders. Dit vraagt om nader onderzoek. Dit valt buiten de scope van onderhavig onderzoek. De input die we tijdens het onderzoek hebben opgehaald is samengevat in bijlage 7.3, zodat dit niet verloren gaat.

## Samenhang van functies

Dit rapport beschrijft adresseren als een losse (op zichzelf staande) functie, waarbij onderscheid gemaakt wordt tussen (1) het gericht versturen van informatie en (2) het opvragen van informatie, na lokalisatie. In deze paragraaf wordt de samenhang tussen de functies lokaliseren, adresseren, autoriseren en toestemming beschreven aan de hand van het ongericht beschikbaar stellen van informatie door de dossierhouder.

We veronderstellen dat het opvragen van informatie alleen voorkomt na lokalisatie van dossierhouders door de raadplegende zorgverlener. Hierbij stelt de dossierhouder gegevens beschikbaar aan een voor hem onbekende zorgverlener. Het lokaliseren van dossierhouders valt onder de generieke functie lokalisatie. In het rapport “IST en SOLL generieke functie lokalisatie” wordt deze functie als volgt gedefinieerd (D&A Medical Group, 2023):

*“Lokalisatie gaat enerzijds over het bepalen welke zorgaanbieders dossierhouder zijn van een patiënt en anderzijds over welke gegevens deze zorgaanbieders beschikken en wat de actualiteit van deze gegevens is.”*





Om de gegevens te raadplegen bij de gelokaliseerde dossierhouders heeft de raadpleger het digitale adres van de dossierhouders nodig. Met de generieke functie adresseren kunnen de benodigde digitale adressen opgezocht en geraadpleegd worden. Dit zal veelal een geautomatiseerd proces zijn waarin geen extra handelingen van de zorgverlener gevraagd worden.

Alvorens de dossierhouder informatie deelt met de raadpleger dient deze te controleren of de (1) raadplegende zorgverlener bevoegd is om de informatie op te vragen **en** (2) of de patiënt toestemming heeft gegeven voor het delen van (specifieke) gegevens. Het controleren of een zorgverlener bevoegd is om bepaalde informatie in te zien valt onder de generieke functie autoriseren en wordt beschreven in het rapport “IST – SOLL generieke functie autoriseren” (D&A Medical Group, 2023). Zoals in paragraaf 2.2 beschreven, wordt bij het ongericht beschikbaar stellen van informatie verondersteld dat de patiënt reeds toestemming heeft gegeven voor het delen van (medische) informatie. Het registreren van deze (expliciete) toestemming is vervat in de generieke functie toestemmingen en valt buiten de scope van dit onderzoek. In bijlage 7.2 wordt dit proces schematisch weergegeven.



### 3 IST - BESCHIKBARE OPLOSSINGEN

Dit hoofdstuk bevat een beschrijving van de huidige, reeds beschikbare oplossingen voor Adresseren aan de hand van het Nictiz lagenmodel. De volgende oplossingen worden beschreven:

- ZORG-AB
- ZorgDomein
- Nuts
- ChipSoft
- Epic
- Enovation
- LSP

#### **Beveiliging en wet- en regelgeving**

De aspecten ‘beveiliging’ en ‘wet- en regelgeving’ zijn van toepassing op alle lagen van het Nictiz lagenmodel. Voor elk van de oplossingen, beschreven onder IST en SOLL, geldt dat ze moeten passen binnen de huidige wet- en regelgeving.

Een wettelijk uitgangspunt bij Adresseren is het Landelijk Register Zorgaanbieders (LRZa). Dit is het openbare register waarin alle zorgaanbieders verplicht geregistreerd staan. De wettelijke basis van het LRZa is artikel 12 van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) en de wettelijke basis voor opname van zorgaanbieders in het LRZa is de Wet toetreding zorgaanbieders (WTZa). Het doel van het LRZa is om duidelijk te maken wie, waar, welke zorg verleent en met welke bevoegdheid (CIBG, 2022). Het LRZa voorziet dus niet in technische adressen, maar brengt informatie uit diverse relevante basisregistraties samen.

Naast de wettelijke verplichtingen bestaan er ook standaarden en richtlijnen voor gegevensuitwisseling. Een daarvan is Digikoppelingen, gebaseerd op internationale open standaarden van OASIS en W3C. Dit zijn twee wereldwijde standaardisatie-organen voor open standaarden. Digikoppelingen zijn primair bedoeld voor gegevensuitwisseling tussen systemen van overheidsorganisaties, in het bijzonder de basisregistraties en landelijke of intersectorale gegevensdiensten. Digikoppelingen worden echter breder ingezet in de (semi-)publieke sector en zijn ook beschikbaar voor gebruik in de private sector. Voor adresseren en routeren van berichten is de “Digikoppeling Handreiking Adressering en Routering” beschikbaar (Logius, 2023).

#### **ZORG-AB**

ZORG-AB is een digitaal adresboek met daarin de adresgegevens van het merendeel van de zorgaanbieders. Er wordt adresinformatie van verschillende bronnen verzameld en getoond, waaronder het AGB-register, het UZI-register en adressen aangeleverd door de zorgaanbieders zelf. ZORG-AB bevat naast een unieke identificatie (zoals bijvoorbeeld de AGB-code) en contactinformatie ook technische adresgegevens van systemen.



Tabel 1 Samenvatting ZORG-AB

<b>Organisatie</b>	<p>ZORG-AB toont adressen uit verschillende bronnen die bij de bron worden beheerd. Bronnen zijn bijvoorbeeld het AGB-register (Vektis), het applicatieregister van het LSP, de zorgaanbieders zelf.</p> <p>Een zorgaanbieder heeft een UZI-certificaat nodig om zelf gegevens aan te kunnen vullen of te wijzigen in ZORG-AB.</p> <p>XIS-leveranciers doorlopen een acceptatieprocedure om gebruik te kunnen maken van ZORG-AB.</p>
<b>Proces</b>	<p>ZORG-AB wordt geraadpleegd voor de adresgegevens van een zorgaanbieder of zorgverlener. De toepassing is niet use case specifiek.</p> <p>Identificatie middels de AGB-code of het URA-nummer van de zorgaanbieder.</p>
<b>Informatie</b>	<p>ZORG-AB bevat alle type adressen van een zorgaanbieder. In ZORG-AB is ook opgenomen met welke standaarden met welke versie de zorgaanbieder gegevens uit kan wisselen en welk digitaal adres daarbij hoort.</p> <p>ZORG-AB is gebaseerd op onderstaande standaarden:</p> <ul style="list-style-type: none"> <li>- IHE Healthcare Provider Directory (HPD)</li> <li>- HL7 FHIR Argonaut</li> </ul>
<b>Applicatie</b>	<p>Leveranciers koppelen hun systeem aan ZORG-AB. Dit kan op twee manieren:</p> <ol style="list-style-type: none"> <li>1. Op het moment dat een zorgverlener een zorgverlener of zorgaanbieder wil adresseren wordt ZORG-AB geraadpleegd.</li> <li>2. ZORG-AB wordt gesynchroniseerd met het interne adresboek van het XIS.</li> </ol>
<b>Infrastructuur</b>	<p>Raadplegen van ZORG-AB kan via internet, voor het aanpassen van adresgegevens is een aansluiting op Zorgnet, een stelsel van private en beveiligde (niet vanaf het internet te benaderen) landelijk dekkende netwerken, nodig.</p>

### Organisatie

ZORG-AB toont adressen, maar het beheer gebeurt bij de bronnen, dit zijn bijvoorbeeld Vektis, het LSP en de zorgaanbieders zelf. Een zorgaanbieder heeft een UZI-certificaat nodig om gegevens aan te kunnen vullen of te wijzigen in ZORG-AB. Een zorgaanbieder kan bijvoorbeeld locaties, e-mailadressen en (mobiele) telefoonnummers aanleveren. Als een zorgaanbieder niet met een UZI-servercertificaat aansluit kan hij alleen raadplegen.

De leverancier sluit het XIS aan op ZORG-AB. Om aan te mogen sluiten moet de leverancier kunnen aantonen dat ze leverancier in de zorg zijn en er wordt een acceptatieprocedure doorlopen. In deze procedure wordt getoetst of de informatie juist getoond kan worden. Wanneer de leverancier geaccepteerd is, mag ZORG-AB gebruikt worden naar inzicht van de leverancier.

### Proces

ZORG-AB kan volledig geïntegreerd worden in het XIS. Als een zorgverlener gebruik maakt van een XIS dat is aangesloten op ZORG-AB kan er door het systeem landelijk gezocht worden naar andere zorgaanbieders of specifieke zorgverleners. ZORG-AB is geen use case specifieke toepassing en kan



dus voor het versturen van een bericht naar een andere zorgaanbieder of zorgverlener in alle gevallen geraadpleegd worden.

### **Informatie**

ZORG-AB heeft de mogelijkheid om alle typen adressen en identificaties van een zorgaanbieder (afkomstig uit andere bronnen) aan te bieden. In ZORG-AB worden gegevens aan elkaar gekoppeld die van dezelfde zorgaanbieder zijn op basis van het URA-nummer en/of de AGB code. Daarnaast bevat ZORG-AB informatie volgens welke standaard en welke versie een zorgaanbieder gegevens kan ontvangen en welk elektronisch adres daarbij hoort.

Er wordt gebruik gemaakt van het IHE-profiel Healthcare Provider Directory (HPD) voor het datamodel van ZORG-AB en er is een interface beschikbaar op basis van HL7 FHIR Argonaut en Native REST.

### **Applicatie**

XIS'en koppelen aan ZORG-AB. Dit kan door ZORG-AB te raadplegen voor de verzending van een bericht of door ZORG-AB volledig te integreren in het XIS zodat het lokale adresboek gesynchroniseerd wordt met de landelijke informatie in ZORG-AB.

### **Infrastructuur**

Raadplegen van ZORG-AB kan via internet. Voor het aanpassen is er een aansluiting op Zorgnet nodig.



## ZorgDomein

Met ZorgDomein kunnen zorgverleners digitaal verwijzen, diagnostiek aanvragen en informatie sturen naar andere zorgaanbieders. Dit kan naar bijna alle huisartsen, ziekenhuizen, diverse GGZ-instellingen en revalidatiecentra en VVT-instellingen. Hierbij maakt ZorgDomein gebruik van een eigen adressenbestand.

Tabel 2 Samenvatting ZorgDomein

<b>Organisatie</b>	Om gebruik te kunnen maken van ZorgDomein moeten organisaties een AGB-code hebben. Per zorgaanbieder beheert ZorgDomein een lijst met veilige adressen en bestemmingen (b.v. een specifieke polikliniek in een ziekenhuis). Zorginstellingen zijn zelf verantwoordelijk voor het doorgeven van wijzigingen in adressen aan ZorgDomein.
<b>Proces</b>	De oplossing kan sectoroverstijgend ingezet worden voor verwijzen, aanvragen van diagnostiek, versturen van verslagen en overdracht van patiënten. Daarnaast biedt ZorgDomein de mogelijkheid tot inzicht in beschikbare capaciteit.
<b>Informatie</b>	ZorgDomein kent verschillende type technische adressen waaronder <ul style="list-style-type: none"><li>- IP-adressen en poortnummers</li><li>- FHIR-adressen</li><li>- Edifact adressen</li><li>- Nuts DID<sup>1</sup></li></ul>
<b>Applicatie</b>	Applicaties kunnen gekoppeld worden aan ZorgDomein via HL7v2 of FHIR.
<b>Infrastructuur</b>	Er worden geen specifieke eisen gesteld aan de infrastructuur.

### Organisatie

Om gebruik te kunnen maken van ZorgDomein moeten organisaties een AGB-code hebben. Organisaties zonder AGB-code, die gebruik willen maken van de dienstverlening van ZorgDomein, worden individueel beoordeeld. De beoordeling bepaalt of aansluiting mogelijk is. ZorgDomein is verantwoordelijk voor het beheer van het adressenbestand en monitort de berichtenstroom van en naar zorgaanbieders. Wijzigingen worden doorgevoerd op aanvraag van de zorgaanbieder. Dit betreft aanpassingen in adressen naar aanleiding van wijzigingen in bijvoorbeeld berichten, protocollen en zorgaanbod.

### Proces

ZorgDomein kan in elke sector ingezet worden en beschikt over een adressenbestand waarin alle aangesloten zorgaanbieders opgezocht kunnen worden.

---

<sup>1</sup> Decentralized identifiers (DID) stellen individuen en organisaties in staat om hun digitale identiteit te beheren en te beschermen in een gedistribueerde, gedecentraliseerde omgeving.



Het niveau van adressering hangt af van de situatie en is afhankelijk van de bestemming van het bericht. Dit kan per zorgaanbieder worden geconfigureerd. Berichten kunnen geadresseerd worden naar:

- Een individuele zorgverlener, bijvoorbeeld coördinator van een organisatie;
- Een systeem (en of communicatieserver);
- Een afdeling binnen een zorginstelling, bijvoorbeeld een polikliniek;
- Een XIS, waarna het op de werklijst van de juiste personen wordt geplaatst.

### **Informatie**

ZorgDomein kent verschillende typen technische adressen voor het versturen van informatie naar zorgaanbieders. Daarnaast beschikt ZorgDomein ook over een algemene lijst met alle binnen ZorgDomein bekende zorgaanbieders. Dit is ook op zorgverlener niveau beschikbaar. De technische adressen die in ZorgDomein beschikbaar zijn:

- IP-adressen en poortnummers
- FHIR-adressen
- Edifact adressen
- Nuts DID<sup>2</sup>

### **Applicatie**

ZorgDomein kan gekoppeld worden aan alle applicaties. Om te kunnen koppelen met ZorgDomein worden aanvullende eisen gesteld aan het systeem zoals certificering op ISO27001 en NEN7510. Op functioneel niveau wordt gekeken hoe de data binnenkomt en/of wordt verwerkt door het ontvangende systeem. ZorgDomein stelt verschillende API's beschikbaar die leveranciers kunnen gebruiken om met ZorgDomein te integreren. Deze API's zijn beschikbaar voor HL7v2 en FHIR.

### **Infrastructuur**

Er worden geen specifieke eisen gesteld aan de infrastructuur.

## **Nuts**

Nuts is een decentraal communicatienetwerk voor de zorg. Het is een volledig gedistribueerd netwerk, zonder afhankelijkheden van een centrale partij. Nuts definieert adresseren als: 'Het publiceren van kenmerken van een zorgaanbieder op een plek waar anderen erbij kunnen.' Het kan bijvoorbeeld gaan om een technisch adres/endpoint en gevelnaam.

Adresseren binnen het Nuts netwerk vindt plaats op basis van publieke sleutels. Deze sleutels kunnen niet door een andere partij worden gestolen en zijn daardoor niet te vervalsen. De kenmerken van de zorgaanbieder worden gekoppeld aan de sleutel. Dit kan een naam zijn, maar ook een technisch endpoint. De leverancier geeft aan onder welke naam de instelling vindbaar is. Alle adressen worden ondertekend met de cryptografische handtekening. Bij SAAS-leveranciers wordt adressering volledig door de leveranciers geregeld, de endpoints zijn van de leverancier.

---

<sup>2</sup> Decentralized identifiers (DID) stellen individuen en organisaties in staat om hun digitale identiteit te beheren en te beschermen in een gedistribueerde, gedecentraliseerde omgeving.



Tabel 3 Samenvatting Nuts

<b>Organisatie</b>	<p>Nuts is een volledig gedistribueerd netwerk. Er is geen centrale partij, ook niet voor de invulling van de generieke functies.</p> <p>Deelnemende leveranciers tekenen een deelnemersovereenkomst met Nuts, voor ze aansluiten op het Nuts-netwerk.</p>
<b>Proces</b>	<p>Iedere zorgaanbieder publiceert zelf zijn adres binnen het netwerk. Vervolgens heeft ook iedere zorgaanbieder in zijn systeem een eigen adresboek. Er zijn verschillende standaarden voor adresseren, maar er is vrije keuze.</p>
<b>Informatie</b>	<p>Adresseren gebeurt op basis van een technisch endpoint dat bij een zorgaanbieder hoort.</p>
<b>Applicatie</b>	<p>Het is een gedistribueerd register, elke node heeft een register en iedere wijziging bij een andere node wordt naar alle nodes verstuurd. De wijzigingen hebben een cryptografische handtekening zodat de herkomst van de wijziging bevestigd kan worden.</p>
<b>Infrastructuur</b>	<p>Internet</p>

### Organisatie

Nuts is een volledig gedistribueerd netwerk. Er is geen centrale partij, ook niet voor de invulling van de generieke functie adresseren.

De aansluiting op het Nuts netwerk regelt een leverancier zelf door de Nuts-node op te starten in combinatie met een PKI-overheid-certificaat. Deelnemers onderschrijven het Nuts manifest en de leverancier tekent een deelnemersovereenkomst met Nuts voor men aansluit op het Nuts-netwerk. Verplichte tests zijn er niet, maar de leverancier is wel verplicht een risico-inschatting te maken. Het risico op een beveiligingsincident ligt namelijk bij de bronhoudende leverancier.<sup>3</sup>

### Proces

Iedere zorgaanbieder publiceert zelf zijn adres binnen het netwerk. Vervolgens heeft ook iedere zorgaanbieder in zijn systeem een eigen adresboek. Adresseren in Nuts is beperkt tot technische endpoints en cryptografische sleutels. Als er meer adresgegevens nodig zijn kunnen die bij de endpoints worden opgevraagd. Het adresseren binnen Nuts is use case onafhankelijk.

### Informatie

Adresseren gebeurt op basis van een technisch endpoint en cryptografische sleutel, die bij een zorgaanbieder horen. Er zijn verschillende standaarden voor adresseren, maar binnen Nuts is er vrije keuze.

---

<sup>3</sup> <https://nuts.nl/q-and-a/>



## Applicatie

Adressering binnen Nuts vindt plaats op basis van publieke sleutels. De kenmerken (een naam of technisch endpoint) van een zorgaanbieder worden aan de sleutel gekoppeld. De technische endpoint is van de leverancier van de Nuts node. Een leverancier geeft aan onder welke naam een instelling vindbaar is. Een leverancier ontwikkelt een Nuts node. Met de Nuts node wordt een zorginstelling op het Nuts netwerk aangesloten.

## Infrastructuur

Uitwisseling over het openbare internet op een cryptografische basis.

## ChipSoft

Zorgplatform wordt gepositioneerd als een API-gateway voor instellingen die gebruik maken van HiX. Dat zijn naast ongeveer 70 medisch specialistische zorginstellingen (ziekenhuizen & ZBC's) ook ongeveer 125 huisartsenpraktijken en daarnaast nog een aantal apotheken, GGZ-instellingen, revalidatie-instellingen en een VVT-instelling.

Zorgplatform kent alleen alle benodigde (technische) adressen centraal. De minimale adressering wordt daarbij afgestemd met op Zorgplatform aangesloten applicaties of zorgaanbieders.

Binnen de HiX applicatie kunnen instellingen zelf ook contactgegevens van zorgpartners waarmee ze communiceren onderhouden. Er zijn wel mogelijkheden om deze deels geautomatiseerd te vullen vanuit Vektis (AGB-register).

Tabel 4 Samenvatting ChipSoft

<b>Organisatie</b>	Voor de gebruikers van HiX die gebruik maken van Zorgplatform beheert ChipSoft centraal alle benodigde technische adressen. Organisaties moeten een overeenkomst tekenen met ChipSoft om aan te kunnen sluiten op Zorgplatform.
<b>Proces</b>	Zorgplatform kan sectoroverstijgend en voor meerdere use cases ingezet worden (maar wordt vooral in de curatieve zorg gebruikt) voor het adresseren van zowel zorgaanbieders als applicaties.
<b>Informatie</b>	Zorgplatform biedt de mogelijkheid om alle technische adressen vast te leggen die nodig zijn om met andere zorgaanbieders of applicaties te communiceren. Voor het identificeren van zorgaanbieders wordt daarvoor gebruik gemaakt van OID's.
<b>Applicatie</b>	Zorgplatform is de centrale API-gateway waarmee de aangesloten HiX gebruikende organisaties kunnen communiceren met andere zorgaanbieders en applicaties.
<b>Infrastructuur</b>	Er worden geen specifieke eisen gesteld aan de infrastructuur.





## **Organisatie**

Voor de gebruikers van HiX die gebruik maken van Zorgplatform beheert ChipSoft centraal alle benodigde technische adressen. Dit betreft zowel de technische adressen van zorgaanbieders als de technische adressen van aangesloten applicaties. Voorbeelden van applicaties die op Zorgplatform zijn aangesloten zijn o.a. HINQ, ZorgDomein, Point en Luscii.

Organisaties moeten een overeenkomst tekenen met ChipSoft om aan te kunnen sluiten op Zorgplatform. Dit is nodig om randvoorwaarden rondom beveiliging, vertrouwen en verantwoordelijkheden goed te regelen.

## **Proces**

Zorgplatform kan sectoroverstijgend en voor meerdere use cases ingezet worden voor het adresseren van zowel zorgaanbieders als applicaties. Niet alle uitwisselingen waarbij sprake is van adresseren verlopen via Zorgplatform. Sommige uitwisselingen verlopen rechtstreeks vanuit HiX, bijvoorbeeld Zorgmail waarbij gebruik wordt gemaakt van het lokale adresboek in HiX.

## **Informatie**

Zorgplatform biedt de mogelijkheid om alle technische adressen vast te leggen die nodig zijn om met andere zorgaanbieders of applicaties te communiceren. Voor het identificeren van zorgaanbieders wordt daarvoor gebruik gemaakt van OID's.

## **Applicatie**

Zorgplatform is de centrale API-gateway waarmee de aangesloten HiX gebruikende organisaties kunnen communiceren met andere zorgaanbieders en applicaties. Koppelingen dienen hiervoor eenmalig geconfigureerd te worden en zijn daarna door alle aangesloten organisaties te gebruiken.

## **Infrastructuur**

Er worden geen specifieke eisen gesteld aan de infrastructuur.



## Epic

Epic maakt voor de communicatie tussen zorgaanbieders gebruik van Care Everywhere. In Care Everywhere is een adresboek beschikbaar met de contactgegevens van alle Epic ziekenhuizen maar ook van andere zorgaanbieders. Ieder ziekenhuis is zelf verantwoordelijk voor het bijhouden van eigen data in het adresboek.

Tabel 5 Samenvatting Epic

<b>Organisatie</b>	Epic biedt binnen Care Everywhere een adresboek met contactgegevens van alle Epic ziekenhuizen en andere zorgaanbieders. Ieder ziekenhuis is zelf verantwoordelijk voor het bijhouden van de eigen data in het adresboek.
<b>Proces</b>	Care Everywhere kan voor meerdere use cases worden ingezet voor het adresseren van zowel zorgaanbieders als applicaties die door Care Everywhere worden ondersteund.
<b>Informatie</b>	Omdat Epic zich op de internationale markt richt, wordt gebruik gemaakt van internationale standaarden waar dat kan.
<b>Applicatie</b>	Care Everywhere is de oplossing van Epic voor het verwerken van communicatie van en naar andere systemen en organisaties. De ontvangen data wordt daarbij opgenomen in het dossier van de patiënt.
<b>Infrastructuur</b>	Er worden geen specifieke eisen gesteld aan de infrastructuur.

### Organisatie

Epic biedt binnen Care Everywhere een intern adresboek met contactgegevens van alle Epic ziekenhuizen en andere zorgaanbieders. Ieder ziekenhuis is zelf verantwoordelijk voor het bijhouden van de eigen data in het adresboek.

### Proces

Epic ziekenhuizen zijn zelf verantwoordelijk om de contactgegevens in het centrale adresboek up-to-date te houden. Het updaten van het centrale adresboek vindt niet real-time plaats maar met een update per uur.

### Informatie

Omdat Epic zich op de internationale markt richt, wordt gebruik gemaakt van internationale standaarden waar dat kan.



## Applicatie

Care Everywhere is de oplossing van Epic voor het verwerken van communicatie van en naar andere systemen en organisaties. De ontvangen data wordt daarbij opgenomen in het dossier van de patiënt.

## Infrastructuur

Er worden geen specifieke eisen gesteld aan de infrastructuur.

## Enovation

Enovation biedt verschillende oplossingen voor gegevensuitwisseling waarbinnen ook adressering een rol speelt. De volgende oplossingen worden aangeboden:

- LSPConnect / LSPViewer  
Met LSPConnect en LSPViewer biedt Enovation klanten de mogelijkheid om hun informatiesysteem te koppelen met het LSP en actuele medische informatie op te vragen bij het LSP. Hierbij wordt gebruik gemaakt van ZORG-AB om te bepalen welke type bericht (versie) verstuurd moet worden. Dit betreft dus technische adresgegevens.
- XDS  
XDS maakt geen gebruik van een adresboek. De technische adressen zijn geconfigureerd in een XDS-hub en worden gedeeld tussen de verschillende XDS-leveranciers.
- ZorgMail  
ZorgMail maakt gebruik van een eigen (intern) adresboek. Er is met VZVZ gekeken naar de mogelijkheid om de ZorgMailadressen te koppelen met ZORG-AB. In de praktijk kan men hier weinig mee omdat die adressen niet publiekelijk te benaderen zijn. ZorgMail-deelnemers beschikken al over de adressen via het ZorgMail-adresboek en kunnen deze gebruiken.
- POINT  
POINT maakt gebruik van een eigen (intern) adresboek.

Tabel 6 Samenvatting Enovation

<b>Organisatie</b>	Enovation biedt meerdere oplossingen voor gegevensuitwisseling, waarvan enkele gebruik maken van ZORG-AB en andere van een eigen intern adresboek.
<b>Proces</b>	De verschillende oplossingen bieden allen een oplossing voor één of meerdere specifieke use cases.
<b>Informatie</b>	Binnen de verschillende oplossingen wordt gebruik gemaakt van diverse (internationale) standaarden zoals HL7 en FHIR.



<b>Applicatie</b>	Enovation kent verschillende applicaties die gebruik maken van adressering: LSP Connect/LSP Viewer, XDS, ZorgMail en POINT.
<b>Infrastructuur</b>	Er worden geen specifieke eisen gesteld aan de infrastructuur. Met LSPConnect biedt Enovation ook de mogelijkheid om te voldoen aan de eisen van een Goed beheerd Zorg Netwerk (GZN) en daarmee aan te sluiten op het LSP.

### Organisatie

Enovation biedt meerdere oplossingen voor gegevensuitwisseling, waarvan enkele gebruik maken van ZORG-AB en andere van een eigen intern adresboek.

### Proces

De verschillende oplossingen bieden allen een oplossing voor één of meerdere specifieke use cases:

- De functionaliteit van LSPConnect/LSPViewer te gebruiken voor inzage in medicatieverstrekkingen, inzage in intoleranties, contra-indicaties en allergieën.
- De XDS-oplossing is met name in gebruik voor document gebaseerde uitwisseling zoals beelden en de BGZ.
- POINT is een specifieke oplossing voor eOverdracht.
- ZorgMail is een oplossing voor het delen van informatie tussen zorgverleners.

Geen van de oplossingen biedt een volledige, use case onafhankelijke oplossing.

### Informatie

Binnen de verschillende oplossingen wordt gebruik gemaakt van diverse (internationale) standaarden zoals HL7 en FHIR. Enovation kan daarnaast de berichten ook vertalen van en naar de verschillende in gebruik zijnde formaten (FHIR, CDA).

### Applicatie

Enovation kent verschillende applicaties die gebruik maken van adressering: LSP Connect/LSP Viewer, XDS, ZorgMail en POINT.

### Infrastructuur

Er worden geen specifieke eisen gesteld aan de infrastructuur. Met LSPConnect biedt Enovation ook de mogelijkheid om te voldoen aan de eisen van een Goed beheerd Zorg Netwerk (GZN) en daarmee aan te sluiten op het LSP.

## LSP

Het LSP heeft een Applicatieregister waar onder andere de digitale adressen van systemen van zorgaanbieders (endpoints) worden bijgehouden. Via deze endpoints kunnen zorgaanbieders gegevens versturen of raadplegen.



Tabel 7 Samenvatting LSP

<b>Organisatie</b>	Het Applicatieregister is gekoppeld aan ZORG-AB. Via ZORG-AB kunnen (adresserings)gegevens gevonden worden die bij een zorgaanbieder horen.
<b>Proces</b>	De gebruiker kiest het juiste adres aan de hand van een herkenbaar adres dat via ZORG-AB wordt geleverd.
<b>Informatie</b>	Informatie-uitwisseling op basis van informatiestandaarden en zib's.
<b>Applicatie</b>	Het LSP houdt adresgegevens bij in het applicatieregister (APR). Het APR is de centrale component binnen AORTA waarbinnen de gegevens van gekwalificeerde applicaties en GBZ'en zijn vastgelegd.
<b>Infrastructuur</b>	Systemen moeten aangesloten zijn op het LSP en voldoen aan de eisen voor een goed beheerd zorgsysteem (GBZ-eisen) en de gegevensuitwisseling via het netwerk van een leverancier die gekwalificeerd is als zorgserviceprovider (ZSP).

### Organisatie

Het LSP heeft een applicatieregister met daarin o.a. het digitale adres (endpoint) van het systeem van de zorgaanbieders waar gegevens naar toe kunnen worden gestuurd of kunnen worden opgehaald. De zorgaanbieder wordt geïdentificeerd middels de URA (UZI-register abonneenummer). Het applicatieregister is gekoppeld aan ZORG-AB. Via ZORG-AB kunnen onder andere contactgegevens, gevelnamen, etc. worden gevonden die bij de URA horen.

### Proces

De adresseringsfunctie ondersteunt de volgende specifieke use cases:

- Het versturen van een elektronisch 'recept' van de voorschrijver naar een apotheek;
- Dossieroverdracht in de Jeugdgezondheidszorg (JGZ);
- Versturen van het retourbericht van de huisartsenpost (HAP) naar de huisarts.

### Informatie

Er wordt uitgewisseld op basis van specifieke informatiestandaarden, waaronder ketenzorg, medicatieoverdracht, huisartswaarneemgegevens, jeugdgezondheidszorg, etc. Bij een deel van de gegevensuitwisseling wordt reeds gebruik gemaakt van zib's.

### Applicatie

Het LSP houdt adresgegevens bij in het applicatieregister (APR). Het APR is de centrale component binnen AORTA waarbinnen de gegevens van gekwalificeerde applicaties en GBZ'en zijn vastgelegd. Applicatiegegevens zijn uit het APR opvraagbaar door zorgverleners, door middel van het gebruik van de systeemrol Applicatieregister raadplegend systeem. Om te bepalen welke interactie er



uitgezet moet worden naar een bronsysteem, moet het APR bevraagd worden welke interactie het bronsysteem en het opvragende systeem gemeenschappelijk hebben.

Op termijn zal het LSP gebruik maken van ZORG-AB voor het raadplegen van formele adresgegevens zoals URA-nummers of zorgaanbiedernaam.

### **Infrastructuur**

Een zorgaanbieder kan alleen gebruikmaken van het LSP via de AORTA-infrastructuur als hij voldoet aan de eisen van een Goed Beheerd Zorgsysteem (GBZ). Daarvoor moet zijn zorginformatiesysteem (XIS) gekwalificeerd en geaccepteerd zijn.

## **Conclusie huidige oplossingen**

De oplossingen in de huidige situatie voldoen niet volledig aan de functionele behoeften, zoals beschreven in paragraaf 2.3. De belangrijkste oorzaken hiervan zijn:

- Adressen staan versnipperd: verschillende technische endpoints zijn op verschillende plekken vindbaar en contactgegevens (email-adressen, telefoonnummers etc.) zijn weer op andere plekken vindbaar.
- De consequentie hiervan is dat zorgaanbieders adressen op verschillende plekken bij moeten houden.
- De versnippering van adressen brengt ook met zich mee dat de relatie tussen de verschillende adressen niet altijd duidelijk is. Hoe verhoudt een URA-code zich bijvoorbeeld tot een AGB-adres.
- Op dit moment zijn er verschillende registers met identificerende gegevens en digitale adressen. Deze zijn allemaal incompleet.

Deze pijnpunten leiden tot twee uitgangspunten voor de SOLL-oplossingen:

1. De adresgegevens moeten gestandaardiseerd worden, zodat er eenduidigheid komt in het vastleggen van adressen en het gebruik en beheer ervan.
2. Het is wenselijk dat adresgegevens aan de bron kunnen worden bijgehouden. Voor contactgegevens zijn de zorgaanbieders dit zelf. Voor technische adresgegevens kan dit bij de leverancier liggen.



## 4 TOETSINGSKADER

De mogelijke sectoroverstijgende (SOLL) oplossingen die beschreven worden in hoofdstuk 5 worden beoordeeld ten opzichte van een toetsingskader. Dit toetsingskader bestaat uit 3 onderdelen:

1. Functionele behoeften,
2. Leidende principes,
3. Haalbaarheid en draagvlak.

Dit toetsingskader is ontwikkeld ten behoeve van het onderzoek naar landelijke infrastructuren voor gegevensuitwisseling in de zorg (D&A Medical Group, 2022). In dit hoofdstuk lichten we toe hoe het toetsingskader is toegepast in de beoordeling van de SOLL-oplossingen. De functionele behoeften uit het toetsingskader zijn voor deze beoordeling vervangen door de functionele behoeften die voort zijn gekomen uit de werksessies, zie hoofdstuk 2.

Voor de leidende principes is vastgesteld welke relevant zijn om mogelijke oplossingen voor Adresseren aan te toetsen. De reden dat een principe niet getoetst kan worden, is bijvoorbeeld dat oplossingen zich er niet op kunnen onderscheiden, het buiten scope van de definitie van Adresseren valt of niet van toepassing is. In bijlage 7.3 is bij het principe aangegeven als dit het geval is.

Elke oplossing is langs het toetsingskader gelegd. Voor het beoordelen van de functionele behoeften, leidende principes en haalbaarheid van een oplossing is per categorie een vraag geformuleerd om te beoordelen of de oplossing in meer of mindere mate kan voldoen.

De onderdelen uit het toetsingskader zijn als volgt beoordeeld:

- *Voor de functionele behoeften*

Adresseren is randvoorwaardelijk om invulling te geven aan een aantal functionele behoeften. De vraag die bij de functionele behoeften gesteld is: Is het mogelijk om met deze oplossing de functionele behoefte te realiseren? De mogelijke antwoorden zijn:

- Ja, met deze oplossing kunnen de functionele behoeften volledig gerealiseerd worden.
- Het is mogelijk, maar één of meerdere randvoorwaarden zullen nog ingevuld moeten worden.
- Gedeeltelijk: de functionele behoeften kunnen voor een deel ingevuld worden, bijvoorbeeld omdat de oplossing tot specifieke sectoren beperkt is.
- Onmogelijk: de functionele behoeften zijn met deze oplossing niet te realiseren.

- *Voor de leidende principes*

Ondersteunt de oplossing dit principe 'by design'? De mogelijke antwoorden zijn:

- Ja: de oplossing voldoet 'by design'.
- Nee, de oplossing voldoet op onderdelen niet. Hierbij wordt onderscheid gemaakt tussen twee antwoordopties:
  - Nee, de oplossing voldoet op één aspect/onderdeel van het principe niet.
  - Nee, de oplossing voldoet op meerdere aspecten/onderdelen niet aan het principe.



- Nee: de oplossing voldoet niet 'by design' en kan met aanpassingen ook niet voldoen.
- *Voor haalbaarheid*  
Hoe beoordelen we de haalbaarheid van en het draagvlak voor de oplossing? Mogelijke antwoorden zijn:
  - Hoog: De oplossing is technisch en organisatorisch haalbaar; het draagvlak is groot.
  - Gemiddeld: er zijn bezwaren of moeilijkheden, maar deze zijn overkomelijk.
  - Laag: De oplossing is technisch of organisatorisch slecht haalbaar; de impact is zeer groot, er is weinig draagvlak.
  - Heel laag: De oplossing is eigenlijk niet haalbaar; de impact is heel erg groot, er is geen draagvlak.





## 5 SOLL – MOGELIJKE SECTOROVERSTIJGENDE OPLOSSINGEN

In dit hoofdstuk beschrijven we mogelijke oplossingen voor een sectoroverstijgende, interoperabele oplossing (SOLL) voor de functie adresseren. We toetsen deze mogelijke oplossingen aan het toetsingskader.

### Mogelijke oplossingen

Voor alle SOLL-oplossingen geldt dat ze moeten passen in het wettelijk kader, zoals beschreven in hoofdstuk 3.

Voor de SOLL-oplossingen ziet de invulling van de proces-, informatie- en infrastructuurlaag uit het Nictiz lagenmodel er hetzelfde uit. Om deze reden worden deze één keer beschreven. Tijdens de werksessies zijn er, zoals in hoofdstuk 3 beschreven, twee uitgangspunten naar voren gekomen die randvoorwaardelijk zijn om de pijnpunten rondom Adresseren op te lossen. Dit zijn:

1. De adresgegevens moeten gestandaardiseerd worden, zodat er eenduidigheid komt in het vastleggen van adressen en het gebruik ervan.
2. Het is wenselijk dat zorgaanbieders zelf, op één plek, hun eigen adresgegevens kunnen bijhouden.

Dit zijn uitgangspunten geweest bij het formuleren van de SOLL-oplossingen.

#### 5.1.1 SOLL overstijgend

Tabel 8 Samenvatting alle SOLL-oplossingen

Organisatie	<i>Invulling verschilt per oplossing.</i>
Proces	De toepassing van de SOLL-oplossingen is niet use case specifiek. Daarmee wordt bedoeld dat de adresseringsfunctie generiek en sectoroverstijgend toepasbaar is binnen de verschillende use cases van gegevensuitwisseling.
Informatie	Alle type adressen van een zorgaanbieder worden ondersteund, waaronder: <ul style="list-style-type: none"><li>- Technische endpoints,</li><li>- Overige adressen, zoals telefoonnummers of e-mailadressen,</li><li>- Demografische gegevens, zoals plaats en postcode,</li><li>- Organisatie-eenheden,</li><li>- Individuele zorgverleners.</li></ul> Beschikbare standaarden: <ul style="list-style-type: none"><li>- IHE Healthcare Provider Directory (HPD)</li><li>- HL7 FHIR Argonaut (gebaseerd op HPD)</li></ul>
Applicatie	<i>Invulling verschilt per oplossing.</i>



## Infrastructuur

Beveiligde verbindingen via het internet.

### Organisatie

*Zie specifieke SOLL-beschrijvingen.*

### Proces

De SOLL-oplossingen voor Adresseren zijn niet use case specifiek. De oplossingen ondersteunen alle typen use cases waarin Adresseren voorkomt. Het startpunt van Adresseren is dat bekend is wie de ontvanger van het bericht is. Het kan bijvoorbeeld om een verwijzing of overdracht gaan of het opvragen van gegevens. De wijze waarop Adresseren plaatsvindt verschilt per SOLL-oplossing en wordt onder applicatie beschreven.

### Informatie

De informatie die nodig is om te Adresseren is allereerst een technisch endpoint. Daarnaast is er ook een behoefte om telefoonnummers op te kunnen halen en informatie over de zorgaanbieder, zoals het specialisme of specifieke adresgegevens. Dit kunnen een locatie, het e-mailadres of telefoonnummer van een zorgverlener zijn. De SOLL-oplossingen geven hier op twee mogelijke manieren invulling aan:

- In één keer de juiste gegevens opvragen: één plek waar de vraag om adresgegevens gesteld kan worden en ook beantwoord wordt. Dit kan gaan om een (of meerdere) technisch(e) endpoint(s), maar dus ook om andere gegevens, zoals contactgegevens.
- Adresseren in twee stappen: er is een technisch endpoint van een zorgaanbieder bekend dat bevestigd kan worden om nadere gegevens. In de tweede stap kunnen ook aanvullende technische adressen worden opgehaald.

Per SOLL-oplossing wordt beschreven welke manier van Adresseren er wordt toegepast.

De internationale standaarden die gebruikt kunnen worden om invulling te geven aan Adresseren zijn:

- Het IHE-profiel Healthcare Provider Directory (HPD)
- HL7 FHIR Argonaut (gebaseerd op HPD).

Het IHE-profiel Healthcare Provider Directory (HPD)<sup>4</sup> bevat de gegevens om invulling te kunnen geven aan de functionele behoeften. Het profiel beschrijft welke gegevens vastgelegd worden. De toepassing van het profiel kan verschillen en past in beide manieren van adresseren, zoals hiervoor beschreven. Daarop aanvullend moet er een keuze worden gemaakt voor een communicatiestandaard om de adresseringsfuncties te raadplegen. Zowel het HPD-profiel als HL7 FHIR Argonaut bieden hier een mogelijke invulling voor.

### Applicatie

*Zie specifieke SOLL-beschrijvingen.*

---

<sup>4</sup> IHE Healthcare Provider Directory



## Infrastructuur

Adresgegevens kunnen met beveiligde verbindingen via het internet geraadpleegd en aangepast worden.

### 5.1.2 SOLL 1 Centraal adresboek

SOLL 1 beschrijft een centraal adresboek, waarin alle adresgegevens op één plek beschikbaar zijn. Dit is vergelijkbaar met ZORG-AB.

Tabel 9 Samenvatting SOLL 1 Centraal adresboek

<b>Organisatie</b>	Leveranciers en zorgaanbieders sluiten aan op het adresboek. Ze doorlopen een acceptatieprocedure om te mogen aansluiten.
<b>Proces</b>	<i>Invulling onder 5.1.1</i>
<b>Informatie</b>	<i>Invulling onder 5.1.1</i>
<b>Applicatie</b>	Er is één centraal adresboek dat alle gegevens voor adresseren bevat; de hele inhoud van het HPD.
<b>Infrastructuur</b>	<i>Invulling onder 5.1.1</i>

#### Organisatie

Er is een centraal adresboek, waar alle adressen beschikbaar zijn. ICT-leveranciers, zorgaanbieders en bronnen van adresgegevens sluiten hierop aan. Om aan te sluiten moeten er aansluitvoorwaarden worden opgesteld. Deze aansluitvoorwaarden zijn nodig om te borgen dat de bronnen van adressen authentiek zijn. Het is van belang om zeker te weten dat een bron van adresgegevens de juiste gegevens aanlevert en dat zeker is dat de adresgegevens horen bij de juiste organisatie. Hiervoor zijn maatregelen nodig die opgenomen worden in de aansluitvoorwaarden.

#### Applicatie

Er is één centraal adresboek dat alle gegevens voor adresseren bevat. Deze gegevens zijn afkomstig uit verschillende mogelijke bronnen van adresgegevens; dit kunnen bestaande registers zijn, adresgegevens van specifieke oplossingen en uit het bronsysteem van een zorgaanbieder zelf. Welke registers en systemen bron kunnen zijn voor het centrale adresboek dient verder bepaald te worden. Door alle gegevens op één centraal punt bij elkaar te brengen kunnen ze daar ook aan elkaar gekoppeld worden (alles wat bij één zorgaanbieder hoort) en verrijkt worden. Vanuit het bronsysteem kunnen eigen adresgegevens aan het centrale adresboek worden aangeleverd en kan het centrale adresboek geraadpleegd worden.

Het adresboek kan op twee manieren gebruikt worden. Namelijk door het te raadplegen voor de verzending van een bericht of door het volledig te integreren in het XIS zodat het lokale adresboek gesynchroniseerd wordt met de landelijke informatie uit het centrale adresboek.



Alle gegevens, zoals beschreven op de informatielaag worden in deze SOLL op één plek bij elkaar gebracht. Hierdoor is het mogelijk dat een gebruiker specifieke adresgegevens opvraagt, zoals een e-mailadres, maar het adresboek kan ook geraadpleegd worden voor een technisch endpoint.

#### Aandachtspunten voor implementatie

- Opstellen van aansluitvoorwaarden: zowel voor de bronnen van adresgegevens als de gebruikende systemen. Het doel is om eenduidigheid in gegevens af te dwingen, maar ook om de security goed te borgen.
- Om het centrale adresboek te vullen zijn bronnen nodig. Hiervoor moet vastgesteld worden wat mogelijke bronnen voor het centraal adresboek zijn. Een mogelijke bron voor contactgegevens kan het LRZa zijn, zie hoofdstuk 3.
- Besluit welke standaard er gebruikt wordt om adresgegevens vast te leggen en uit te wisselen.

### 5.1.3 SOLL 2 gedistribueerde oplossing

SOLL 2 gaat uit van een volledig gedistribueerd netwerk, zoals bijvoorbeeld Nuts. Een gedistribueerd netwerk bestaat uit een netwerk van deelnemers, zoals bijvoorbeeld zorgaanbieders en (regionale) dataplatformen. Deze deelnemers worden nodes genoemd. De nodes vormen samen een gedistribueerd adresboek, waarin elke node het adres of de adressen van de andere nodes kent. Wanneer een node aan het netwerk wordt toegevoegd, publiceert deze node zijn eigen identiteit en adres op het netwerk. Iedere node houdt een eigen kopie van het adressenbestand bij, dat automatisch wordt geüpdatet bij wijzigingen in het netwerk.

Tabel 10 Samenvatting SOLL 2

<b>Organisatie</b>	Deze oplossing past in een volledig gedistribueerd netwerk. Er is geen centrale partij, ook niet voor de invulling van de generieke functies.  Er is vertrouwen nodig om aan te sluiten op het netwerk. Dit kan geregeld worden door een convenant.
<b>Proces</b>	<i>Invulling onder 5.1.1</i>
<b>Informatie</b>	<i>Invulling onder 5.1.1</i>
<b>Applicatie</b>	Het is een gedistribueerd register, elke node heeft een register en iedere wijziging bij een andere node wordt naar alle nodes verstuurd. De wijzigingen hebben een cryptografische signature zodat de herkomst van de wijziging bevestigd kan worden.
<b>Infrastructuur</b>	<i>Invulling onder 5.1.1</i>

#### Organisatie

Deze oplossing past in een volledig gedistribueerd netwerk. Er is geen centrale partij, ook niet voor de invulling van de generieke functies.

Er is vertrouwen nodig om aan te sluiten op het netwerk. Dit kan geregeld worden door een convenant. Daarnaast zijn er waarborgen nodig bij het verspreiden van een adres over het netwerk. Deze waarborgen moeten de garantie bieden dat het adres dat over het netwerk bekend gemaakt wordt, hoort bij de betreffende zorgaanbieder.



## Applicatie

Het is een gedistribueerd register, elke node heeft een register en iedere wijziging bij een andere node wordt naar alle nodes verstuurd. De wijzigingen hebben een cryptografische signature zodat de herkomst van de wijziging bevestigd kan worden. In de praktijk betekent dit dus als zorginstelling A een wijziging in een technisch endpoint heeft, alle overige nodes in het netwerk hiervan op de hoogte worden gebracht. En als zorginstelling B een bericht naar zorginstelling A wil versturen, zij altijd over het actuele adres (technische endpoint) beschikt. Het beheer van de technische endpoint kan zowel door een zorgaanbieder zelf, als door een leverancier voor meerdere zorgaanbieders worden uitgevoerd.

Het is van belang om onderscheid te maken tussen adressen van nodes en adressen van organisaties en personen. Dit zouden bijvoorbeeld telefoonnummers of e-mailadressen kunnen zijn. Deze gegevens kunnen in een gedistribueerd netwerk via API's op alle nodes worden aangeboden. Dus de node van de opvrager benadert de node van de zorgaanbieder waarvan de opvrager gegevens wil ontvangen. In deze SOLL-oplossing is er dus geen centraal punt waar gegevens opgeslagen worden.

## Aandachtspunten voor implementatie

- Afspraken maken waarmee het vertrouwen geborgd wordt op het netwerk. Dit kan op landelijk niveau door middel van een convenant of contract dat organisaties tekenen voordat er gegevens uitgewisseld kunnen worden.
- Deze oplossing past in een volledig gedistribueerd netwerk, zoals scenario D (een standaard datamodel voor elke zorgaanbieder) en scenario F (een volledig gedistribueerd netwerk) uit het onderzoek 'een landelijk dekkend netwerk van infrastructuren voor gegevensuitwisseling in de zorg' (D&A Medical Group, 2022), waar alle zorgaanbieders op zijn aangesloten. Daarnaast moet dit netwerk door alle leveranciers ondersteund worden om het te laten werken.
- Besluit welke standaard er gebruikt wordt om adresgegevens vast te leggen en uit te wisselen.

### 5.1.4 SOLL 3 Combineren van adresseringsfuncties

SOLL 3 is het combineren van verschillende oplossingen voor Adresseren. In deze oplossing wordt er geen keuze gemaakt tussen een volledig gedistribueerde oplossing of een centraal adresboek. Adresseringsfuncties zijn nu vaak gekoppeld aan een uitwisselingsinfrastructuur. SOLL 1 en SOLL 2 vragen beide aanpassingen ten opzichte van de huidige situatie. In dit scenario kunnen bestaande functies in stand blijven. Het is dan wel noodzakelijk om uitgevers/beheerders van adressen te kunnen koppelen. Een belangrijk aandachtspunt hierbij is dat adresgegevens gestandaardiseerd moeten kunnen worden opgezocht en uitgewisseld en dat er niet voor elke use case/koppeling afspraken gemaakt moeten worden. Daarnaast is ook de betrouwbaarheid van de adresgegevens een belangrijk uitgangspunt.

In het gezamenlijk groeipad TwiinxNuts (Tesink & Spee, 2022) wordt deze oplossing beschreven.



Tabel 11 Samenvatting SOLL 3

<b>Organisatie</b>	Afspraken om betrouwbaarheid van de adresseringsfuncties te waarborgen.
<b>Proces</b>	<i>Invulling onder 5.1.1</i>
<b>Informatie</b>	<i>Invulling onder 5.1.1</i>
<b>Applicatie</b>	De adresseringsfunctie kan in verschillende oplossingen ingebouwd worden. Dit kan een centraal adresboek zijn, adresboeken gekoppeld aan dataplatforms of op het niveau van een individuele zorgaanbieder. Deze adresseringsfuncties worden aan elkaar gekoppeld, zodat met één uitvraag om adresgegevens verschillende adresseringsfuncties geraadpleegd kunnen worden.
<b>Infrastructuur</b>	<i>Invulling onder 5.1.1</i>

### Organisatie

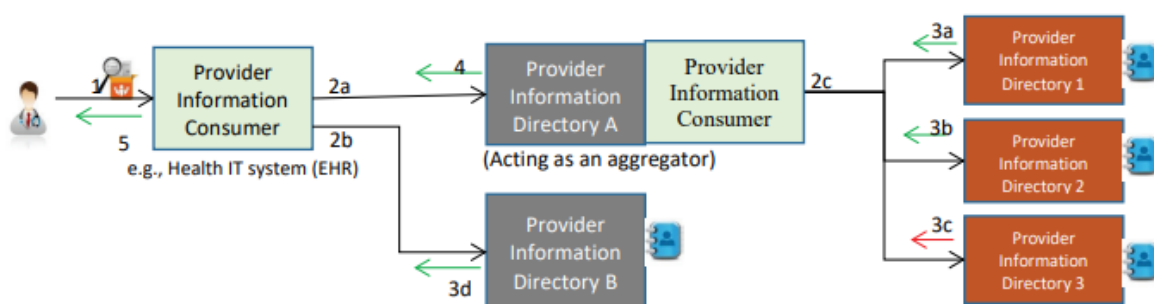
Afspraken om betrouwbaarheid van de adresseringsfuncties te waarborgen.

### Applicatie

De adresseringsfunctie kan in verschillende oplossingen ingebouwd worden. Dit kan een centraal adresboek zijn, adresboeken gekoppeld aan dataplatforms, een adresboek van een leverancier of op het niveau van een individuele zorgaanbieder. Deze adresseringsfuncties worden aan elkaar gekoppeld, zodat met één uitvraag om adresgegevens verschillende adresseringsfuncties geraadpleegd kunnen worden.

Elke adresseringsfunctie die gekoppeld wordt, bouwt het IHE profiel Healthcare Provider Directory (HPD) in.

Een gebruiker stelt een vraag om bepaalde adresgegevens. Deze vraag gaat vervolgens naar alle Provider Information Directories, zoals in onderstaande afbeelding weergegeven. De directories bevatten de informatie zoals in het profiel beschreven staat. Een directory kan een centraal adresboek zijn, een dataplatform, geaggregeerd adresboek of een individuele zorgaanbieder.



Figuur 2 Bron IHE (IHE, 2020)

### Aandachtspunten voor implementatie

- Deze SOLL oplossing gaat over het combineren van verschillende oplossingen. Er zullen dus overstijgend afspraken nodig zijn om deze oplossingen aan elkaar te koppelen. Deze afspraken zullen zowel organisatorisch van aard zijn als technisch. De afspraken zijn nodig



om het vertrouwen tussen partijen te boren, maar ook om de oplossing technisch te laten werken. Met betrekking tot adresseren kan het gaan over welke waarborgen er nodig zijn om de bron van de adresseringsgegevens te valideren.

- In aanvulling op het voorgaande punt zullen er aansluitvoorwaarden opgesteld moeten worden. Dit zijn voorwaarden waar zowel de bronnen van adresgegevens als de gebruikende systemen aan moeten voldoen. Uiteraard kunnen de voorwaarden verschillen.
- Besluit welke standaard er gebruikt wordt om adresgegevens vast te leggen en uit te wisselen.
- In deze oplossing kunnen alle beschikbare technische endpoints bevroegd worden. Het aantal technische endpoints kan met verschillende oplossingen (van één voor een centraal adresboek tot een endpoint per zorgaanbieder) oplopen tot een groot aantal. Bij de implementatie dient rekening gehouden te worden met het risico op performance issues.



## Analyse per oplossing

In deze paragraaf worden de drie SOLL-oplossingen beoordeeld aan de hand van het toetsingskader, zoals in hoofdstuk 4 is beschreven.

De gedetailleerde beoordeling van de oplossingen per functionele behoefte, principe en aspect van haalbaarheid is opgenomen in bijlage 7.6. In deze paragraaf wordt per oplossing de conclusie van de beoordeling op hoofdlijnen beschreven.

Een algemene conclusie is dat **geen enkele** oplossing aan alle behoeften en principes voldoet. Elke oplossing voldoet aan een deel van de principes en/of functionele behoeften. Ze maken het wel alle drie mogelijk om invulling te geven aan de functionele behoefte voor het adresseren van zorgaanbieders. Bij de keuze voor een oplossing is het dus van belang om principes en criteria af te wegen en te bepalen wat het zwaarst weegt en écht leidend moet zijn.

### 5.1.5 SOLL 1 Centraal adresboek

#### Functionele behoeften

SOLL1 voldoet aan twee van de drie functionele behoeften. Met een centraal adresboek is het mogelijk om onderscheid te maken tussen wie er geadresseerd wordt: een zorgaanbieder of een specifieke afdeling of zorgverlener (F1). Het adresboek kan zo ingericht worden dat deze gegevens beschikbaar zijn. Dit geldt ook voor verschillende typen adressen. Het centraal adresboek kan ook gebruikt worden om contactgegevens (F2) op te halen.

Met een centraal adresboek is de derde functionele behoefte, het adresseren van patiënten, moeilijker te realiseren. Het ligt niet voor de hand om ook patiënten met hun adressen (e-mail/PGO) aan een centraal adresboek toe te voegen. Om deze functionele behoefte in te vullen zijn aanvullende maatregelen nodig (zie bijlage 7.3).

#### Leidende principes

Deze oplossing maakt het mogelijk om gebruik te maken van open internationale standaarden (P6). De invulling van het adresboek kan bijvoorbeeld conform het HPD IHE-profiel ingericht worden. Als er gebruik gemaakt wordt van open internationale standaarden kan de oplossing ook duurzaam (P2) opgezet worden. Functionaliteit en data kan op deze manier gescheiden worden. Hierdoor is er geen afhankelijkheid van een specifieke leverancier en kan elke XIS-leverancier in zijn eigen functionaliteit de gegevens aanbieden. Het principe dat een oplossing federatief tot stand komt (P3) is in deze oplossing lastiger te realiseren, omdat er een centrale voorziening gebruikt wordt waar de informatie-uitwisseling van afhankelijk is.

Op het gebied van privacy en security zijn de principes in deze oplossing niet volledig geborgd. Er zijn uiteraard wel maatregelen mogelijk om de risico's te beperken. Het grootste risico in deze oplossing is het risico op spoofing. Spoofing wil zeggen dat een component (fysiek of software) of een menselijke actor zich voordoeft als een ander (bijvoorbeeld door het plegen van identiteitsfraude). Deze partij doet zich bijvoorbeeld voor als zorgaanbieder, staat vervolgens in het adresboek en kan dus patiëntgegevens opvragen en ontvangen. Het risico op spoofing kan beperkt worden door gebruik van sterke authenticatie van zowel mens als machine, inclusief de veilige distributie van beveiligingscertificaten. Daarnaast is er in deze oplossing een single point of failure. Als het adresboek niet beschikbaar is kunnen zorgverleners/-aanbieders niet geadresseerd worden.





## Haalbaarheid

Deze oplossing kent een aantal beperkingen met betrekking tot de haalbaarheid. De belangrijkste oorzaak hiervan is dat er weerstand is bij leveranciers tegen de manier van het tot stand komen van gemeenschappelijke voorzieningen. Om het centrale adresboek goed te kunnen gebruiken in het zorgproces is het van belang dat het gevuld wordt en dat zorgaanbieders, via hun leverancier, aangesloten zijn. Om dit te realiseren is er draagvlak bij leveranciers nodig. Dit kan impact hebben op de realisatietermijn. De oplossing is technisch realiseerbaar. Er wordt gebruik gemaakt van bestaande oplossingen.

Tabel 12 Haalbaarheid SOLL 1 Centraal adresboek

H1	<b>Technisch realiseerbaar</b> Ja, dit scenario kan met bestaande technologieën worden gerealiseerd. Er moeten maatregelen genomen worden om het risico op spoofing te beperken.
H2	<b>Gebruik bestaande oplossingen</b> Gemiddeld, er kan gebruik gemaakt worden van ZORG-AB, maar dit moet dan nog verder doorontwikkeld worden.
H3	<b>Impact</b> Gemiddeld, omdat er een kleine aanpassing nodig is en alle zorgaanbieders aan moeten sluiten.
H4	<b>Draagvlak bij de leveranciers</b> Laag, er is weerstand bij leveranciers tegen de manier waarop gemeenschappelijke voorzieningen tot stand komen.
H5	<b>Maatschappelijk en politiek draagvlak</b> Hoog, er zijn geen maatschappelijke of politieke bezwaren.

## 5.1.6 SOLL 2 Gedistribueerde oplossing

### Functionele behoeften

In SOLL2 vindt adresseren plaats in twee stappen. In stap 1 wordt de technische endpoint bevraagd, waarna in stap 2 de vervolgvraag gesteld kan worden aan een specifieke endpoint. De technische endpoint, dat bij een zorgaanbieder hoort, is bekend bij elke node en kan bevraagd worden om de specifieke adresgegevens. Bijvoorbeeld adressen van een specifieke afdeling of zorgverlener, of de vraag om contactgegevens. Voor beide functionele behoeften (F1 en F2) is een API nodig om de gegevens op te kunnen vragen. Dit betekent dat het zoeken naar een nog niet bekende zorgaanbieder of zorgverlener, bijvoorbeeld op basis van kenmerken, complexer kan zijn dan met een centrale oplossing.

In deze oplossing is het eenvoudiger om patiënten te adresseren. Het is een mogelijkheid dat een patiënt met een node in het netwerk zich bekend maakt. Alle andere nodes, van zorgaanbieders, nemen het adres over. Vervolgens moet een zorgaanbieder een patiënt alleen kunnen benaderen als er een behandelrelatie is (zie bijlage 7.3).

### Leidende principes

SOLL 2 voldoet aan alle leidende principes. Er is scheiding van data en functionaliteit en hiermee is de oplossing duurzaam (P2). Elke leverancier biedt de gegevens aan op het netwerk. De oplossing is ook volledige federatief (P3), er is geen centrale voorziening nodig in de gegevensuitwisseling en



geen impact op de interne werking van systemen. De oplossing kan gebaseerd worden op open internationale standaarden. De data kan aangeboden worden conform het HPD-profiel, maar blijft bij de bron staan. Ook op het gebied van privacy en security voldoet deze oplossing aan de principes. Doordat er geen centrale component is, is er ook geen single point of failure.

### Haalbaarheid

Terwijl deze oplossing aan alle leidende principes voldoet zijn er wel een aantal uitdagingen rondom de haalbaarheid. De belangrijkste oorzaak hiervan is dat de huidige systemen en infrastructuur nog niet volledig zijn voorbereid op een gedistribueerde oplossing. Deze oplossing vraagt dus aanpassingen aan de huidige systemen. Deze oplossing past goed in een gedistribueerde infrastructuur en past daarmee op de langere termijn in een gedistribueerd netwerk van zorgsystemen. Binnen de bestaande infrastructuur is dit nog moeilijk realiseerbaar.

Omdat deze oplossing weinig privacy risico's met zich meebrengt is de verwachting dat hier maatschappelijk en politiek draagvlak voor zal zijn.

Tabel 13 Haalbaarheid SOLL 2 Gedistribueerde oplossing

H1	<b>Technisch realiseerbaar</b> Ja, technisch is dit mogelijk, het wordt op kleine schaal al toegepast.
H2	<b>Gebruik bestaande oplossingen</b> Gemiddeld, elk systeem zou de vereisten met betrekking tot deze functie kunnen inbouwen, maar dit vraagt aanpassingen.
H3	<b>Impact</b> Hoog, als gevolg van de benodigde aanpassingen in veel systemen is de impact hoog en de realisatietermijn lang.
H4	<b>Draagvlak bij de leveranciers</b> Gemiddeld, het draagvlak is wisselend onder de leveranciers.
H5	<b>Maatschappelijk en politiek draagvlak</b> Hoog, er zijn geen maatschappelijke of politieke bezwaren.

## 5.1.7 SOLL 3 Combineren van adresseringsfuncties

### Functionele behoeften

SOLL 3 is een combinatie van SOLL 1 en 2; er worden adresseringsfuncties aan elkaar gekoppeld, met daarbij de mogelijkheid om ook andere oplossingen te koppelen, zoals bijvoorbeeld een geaggregeerd adresboek. Dit betekent dat er voldaan kan worden aan de functionele behoeften, mits de adresseringsfuncties gestandaardiseerd zijn en gekoppeld worden. Het kan verschillen per functie of de adresgegevens in één stap beschikbaar zijn of dat er een tussenstap nodig is, zoals beschreven onder SOLL 2.

Om patiënten te adresseren kan er een specifieke adresseringsfunctie voor patiënten ingericht worden. De specifieke invulling hiervan vraagt om meer uitwerking (zie bijlage 7.3). De functionele mogelijkheden hangen sterk samen met implementatiekeuzes die gemaakt worden en de mogelijkheden van de specifieke oplossingen.



## Leidende principes

Deze oplossing gaat ervan uit dat adresseringsfuncties met elkaar gecombineerd kunnen worden. Dit kunnen bestaande oplossingen en nieuwe oplossingen zijn. Door de oplossingen op basis van open internationale standaarden (P6) te koppelen wordt er scheiding van data en functionaliteit gerealiseerd. Daarnaast is SOLL 3 toekomstbestendig, de functie Adresseren kan door verschillende typen oplossingen ingevuld worden. Het is dus een duurzame oplossing (P2). Hieraan gerelateerd is de oplossing federatief (P3): de interne werking van de bronsystemen en uitwisselsystemen wordt niet voorgeschreven en is grotendeels decentraal. Ook nieuwe oplossingen (zoals dataplatforms) kunnen relatief eenvoudig aansluiten met een eigen adresseringsfunctie. Deze oplossing biedt in principe een gelijk speelveld voor leveranciers (15). Nieuwe leveranciers kunnen met een eigen systeem aansluiten of gebruik maken van een centraal adresboek.

Met betrekking tot privacy en security worden de risico's uit SOLL 1 meegenomen in deze oplossing, maar wel op kleinere schaal omdat er in SOLL 3 geen totale afhankelijkheid is van één systeem.

## Haalbaarheid

Dit scenario kan met bestaande systemen en hun adresseringsfuncties gerealiseerd worden. De uitdaging ligt in het koppelen van de verschillende functies. Op dit moment is er nog geen standaard in gebruik voor adresgegevens en voor de uitwisseling ervan in gebruik in Nederland. Daarnaast is er complexiteit in het koppelen van functies, omdat ze nu in verschillende infrastructuren gebruikt worden. Deze infrastructuren stellen verschillende eisen, met name op het gebied van vertrouwen. Als adresseringsfuncties gecombineerd worden is het van belang om het vertrouwen tussen de functies goed te borgen om zo mogelijk te maken dat adresgegevens ook daadwerkelijk bij de zorgaanbieder horen die geadresseerd wordt. Als gevolg hiervan verwachten we niet dat deze oplossing op korte termijn gerealiseerd kan worden.

De oplossing kan wel op draagvlak bij leveranciers rekenen, omdat zij hun eigen functies kunnen behouden. De verwachting is ook dat er maatschappelijk en politiek draagvlak zal zijn.

Tabel 14 Haalbaarheid SOLL 3 Combinatie van adresseringsfuncties

H1	<b>Technisch realiseerbaar</b> Moeilijk, omdat bestaande functies aan elkaar gekoppeld moeten worden, brengt dit complexiteit met zich mee.
H2	<b>Gebruik bestaande oplossingen</b> Gemiddeld, elk systeem kan de huidige oplossing in stand houden. Er zullen wel aanpassingen nodig zijn aan de bestaande oplossingen om ze te kunnen koppelen.
H3	<b>Impact</b> Hoog, er moet een oplossing gevonden worden voor het kunnen combineren van verschillende adresseringsfuncties.
H4	<b>Draagvlak bij de leverancier</b> Hoog, elke leverancier kan een eigen keuze maken.
H5	<b>Maatschappelijk en politiek draagvlak</b> Hoog, er zijn geen maatschappelijke of politieke bezwaren.



## 6 CONCLUSIE EN ADVIES

### Conclusie

De drie besproken oplossingen voor Adresseren kunnen in principe allemaal aan de functionele behoeften voldoen.

De belangrijkste verschillen tussen de oplossingen zitten in de haalbaarheid, security (zoals gedefinieerd in het toetsingskader) en het draagvlak. Deze verschillen zijn samengevat in tabel 15. De volledige analyse is opgenomen in bijlage 7.6.

- SOLL 1 is een centrale voorziening. Er is weerstand, met name, bij leveranciers tegen de manier waarop centrale voorzieningen tot stand komen. De manier van tot stand komen van de centrale voorziening is dus bepalend voor het draagvlak. Daarnaast kent SOLL 1 een aantal security risico's die in deze oplossing groter zijn dan in de andere twee oplossingen. Het gaat bijvoorbeeld om het risico op spoofing. Daarnaast ontstaat er met een centrale voorziening een kwetsbaarheid, een single point of failure. Vanuit de huidige situatie verwachten we dat SOLL 1 op de korte termijn, technisch gezien, de meest haalbare oplossing is.
- SOLL 2 voldoet het beste aan de leidende principes, maar vereist de grootste aanpassingen aan de bronsystemen en past niet één op één in de huidige infrastructuur. De oplossing gaat uit van een volledig gedistribueerde infrastructuur. Dit maakt de oplossing minder haalbaar. In SOLL 2 moeten alle leveranciers in alle sectoren dezelfde oplossing ondersteunen. Het draagvlak voor deze oplossing, onder leveranciers, wisselt.
- SOLL 3 is een combinatie van verschillende adresseringsfuncties en neemt dus voor een deel de risico's van SOLL 1 over, maar op kleinere schaal. De complexiteit van SOLL 3 zit in het koppelen van verschillende oplossingen voor Adresseren over verschillende infrastructuren. SOLL 3 kan op het meeste draagvlak rekenen, omdat bestaande oplossingen naast elkaar gebruikt kunnen worden.

Tabel 15 Grootste verschillen tussen SOLL 1, 2 en 3

	<i>SOLL 1 - Centraal adresboek</i>	<i>SOLL 2 – Gedistribueerde oplossing</i>	<i>SOLL 3 – combineren van adresseringsfuncties</i>
<i>Haalbaarheid</i>			
<i>Security</i>			
<i>Draagvlak</i>			

In alle SOLL-oplossingen zullen er op organisatorisch vlak afspraken gemaakt moeten worden, zodat het vertrouwen geborgd wordt. Dit kan op landelijk niveau door middel van een convenant of contract, dat organisaties tekenen, voordat er gegevens uitgewisseld kunnen worden. In een dergelijk convenant kunnen afspraken over het gebruik van de voorziening(en) en de verantwoordelijkheden van de verschillende deelnemers en leveranciers worden vastgelegd.

Vanuit de interviews blijkt dat de functionele behoeften, voor het digitaal adresseren van andere zorgaanbieders, met de bestaande oplossingen al ingevuld worden. Op dit moment zit de pijn met name in de versnippering van adressen, onvolledigheid en de beheerlast om op alle plekken de adressen te beheren. Met één zorgbrede adresseringsfunctie wordt dit eenvoudiger. Vanuit



zorgverleners neemt de behoefte voor een adresseringsfunctie toe als er een oplossing voor de generieke functie lokalisatie beschikbaar komt. Op dit moment is de zorgaanbieder die geadresseerd wordt in de meeste gevallen bekend. Maar, als er een vooraf onbekende zorgaanbieder gelokaliseerd kan worden, is het wenselijk dat deze na lokalisatie direct geadresseerd kan worden.

### **Kosten en baten**

In de analyse van de verschillende SOLL-oplossingen is beschreven in hoeverre de oplossing kan voldoen aan de functionele behoeften en de principes. De baten die met de oplossing gerealiseerd kunnen worden zijn hier nauw aan verbonden. De kosten die per SOLL-oplossing gemaakt moeten worden zijn van veel verschillende factoren afhankelijk, zoals de exacte aanpassingen die nodig zijn aan de systemen, tot welke wijzigingen dit leidt, hoe groot de impact op het proces is, hoe de oplossing beheerd gaat worden, de kosten van een centrale voorziening, etc. Hiermee is het niet mogelijk om een accurate inschatting van de verwachte kosten te geven.

## **Advies en roadmap**

Naar aanleiding van de analyse is het advies om op korte termijn te werken aan de realisatie van de generieke functie lokalisatie. Ontwikkel tegelijkertijd een solide basis ter ondersteuning van adressering oplossingsrichting SOLL 3 (het combineren van meerdere adresseringsfuncties).

Om een solide basis te bouwen voor het (gecombineerd) ondersteunen van meerdere adresfuncties (adresboeken) dienen de onderstaande twee belangrijkste uitgangspunten nagestreefd te worden. Deze uitgangspunten vormen het startpunt van de sectorbrede afspraken die gemaakt dienen te worden, maar zijn niet uitputtend voor de realisatie van SOLL 3.

Belangrijkste uitgangspunten voor de realisatie van SOLL 3:

### **1. Stimuleer, volg en omarm de ontwikkelingen van het landelijk vertrouwensmodel (voorheen TwiinxNuts)**

Om de verschillende uitwisselingsinfrastructuren en adresfuncties aan elkaar te koppelen moeten eenduidige implementatie afspraken gemaakt worden. Het landelijk vertrouwensmodel heeft voor 2025 als doelstelling het gestandaardiseerd opzoeken en uitwisselen van technische adressen uit verschillende bronnen.

Op dit moment worden de mogelijkheden verkent in een PoC tussen Nuts en ZORG-AB. De uitkomsten van de PoC kunnen de basis vormen van de implementatie afspraken voor uitwisseling van technische adressen.

### **2. Standaardiseer de registratie en uitwisseling van adresgegevens met internationale standaarden**

Digitale adressen, zowel technische adressen als contactgegevens, moeten eenvoudig uitwisselbaar en raadpleegbaar zijn voor alle systemen. Om dit te bewerkstelligen is het van belang om adresgegevens op eenduidige manier te registreren. Hiervoor dienen sector overstijgende afspraken gemaakt te worden over de registratie van (1) niveaus van adresseren (zorgaanbieder, specifieke afdeling of zorgverlener) en (2) (logische) naam en



de contactgegevens van de zorgaanbieder en/of zorgverlener gekoppeld aan het digitaal adres. Door gebruik te maken van internationale standaarden zoals het IHE-profiel Healthcare Provider Directory (HPD) en HL7 FHIR Argonaut (gebaseerd op HPD) wordt eenduidige registratie aan de bron afgedwongen. Het standaardiseren van de registratie en uitwisseling van adresgegevens kan verder door de NEN-werkgroep adresseren uitgewerkt worden.



## 7 BIJLAGEN

### Afkortingen en begrippen

#### 7.1.1 Afkortingenlijst

Afkorting	Definitie
API	Application Programming Interface
AVG	Algemene Verordening Gegevensbescherming
BSN	Burgerservicenummer
CDA	Clinical Document Architecture
DIZRA	Duurzaam Informatiestelsel in de Zorg Referentie Architectuur
EHDS	European Health Data Space
GGZ-instelling	Geestelijke Gezondheidszorg instelling
HAP	Huisartsenpost
HPD	Healthcare Provider Directory
ISO	International Organization for Standardization
IST	"Ist-Zustand" in het Duits, wat letterlijk betekent "huidige situatie"
IZA	Integraal Zorgakkoord
LRZa	Landelijk Register Zorgaanbieders
LSP	Landelijk Schakelpunt
NEN	Stichting Koninklijk Nederlands Normalisatie Instituut
OID	Wereldwijde Unieke Object Identificatie
PGO	Persoonlijke gezondheidsomgeving
RSO	Regionale Samenwerkings Organisatie
SEH	Spoedeisende hulp
SOLL	"Soll-Zustand" in het Duits, wat letterlijk betekent "gewenste situatie"
TA	Technische afspraken
URA	UZI Registratie Abonneenummer
UZI	Unieke Zorgverlener Identificatie
VVT-instelling	Verpleeg- en Verzorgingshuizen en Thuiszorg instelling
Wabvpz	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
Wegiz	Wet elektronische gegevensuitwisseling in de zorg
WGBO	Wet geneeskundige behandelingsovereenkomst
Wkkgz	Wet kwaliteit, klachten en geschillen zorg
XDS	Cross-enterprise Document Sharing



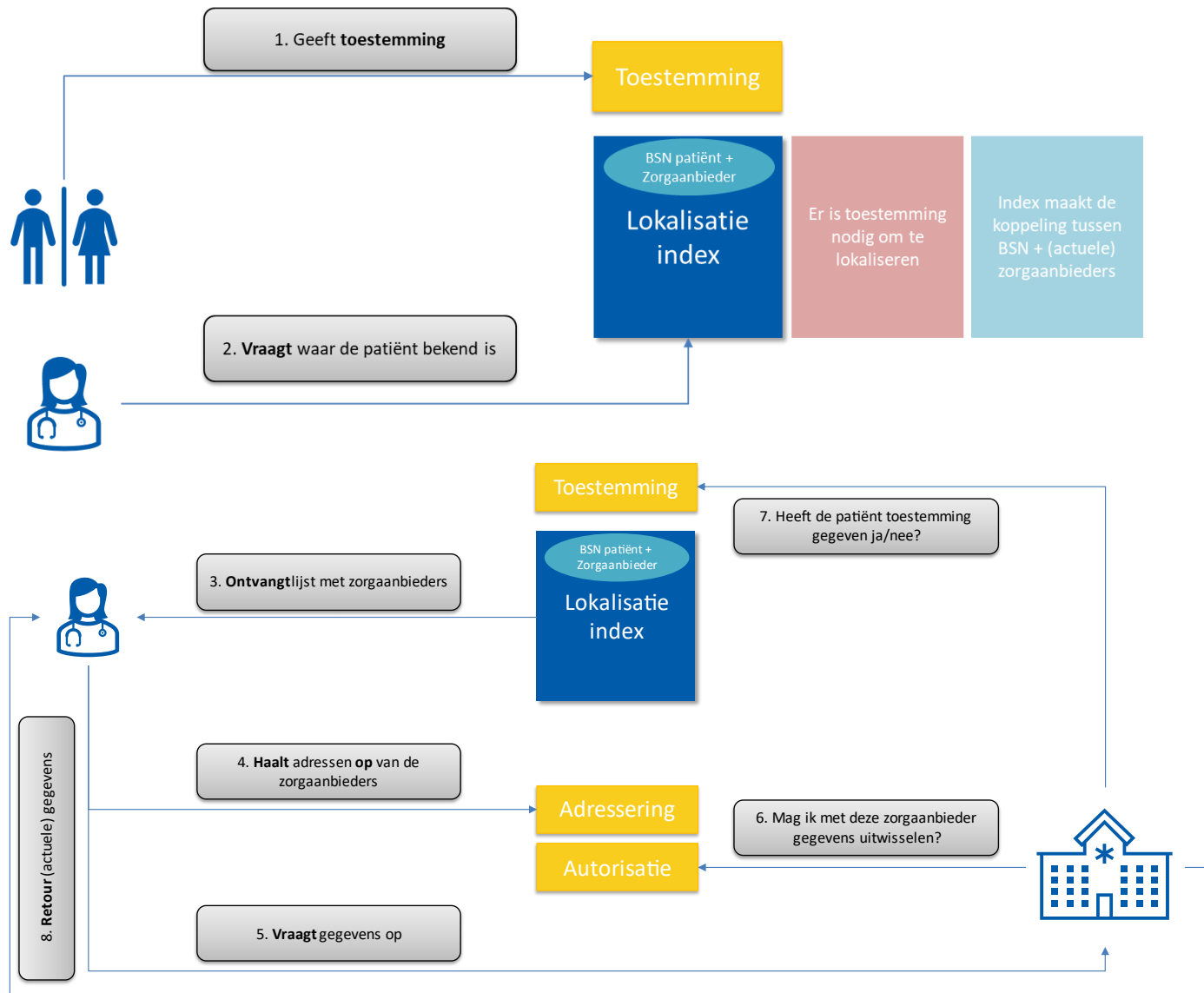
## 7.1.2 Begrippenlijst

Begrip	Definitie
API	Een API biedt een toegangspoort tot een programma. Deze poort zorgt ervoor dat clients van buitenaf bepaalde requests (vragen) kunnen stellen aan het programma.
DIZRA	Referentiearchitectuur van een duurzaam informatiestelsel in de zorg.
FHIR	HL7-standaard om digitaal gegevens uit te wisselen binnen en tussen zorgaanbieders onderling en tussen zorgaanbieders en zorggebruikers.
IST – SOLL-model	Het IST-SOLL model is een methodiek waarmee de huidige situatie (IST) kan worden vergeleken met de gewenste situatie (SOLL). Hierbij wordt gekeken naar verschillende aspecten. Door deze aspecten te vergelijken, kan een “gap” worden geïdentificeerd tussen de huidige situatie en de gewenste situatie. Dit geeft inzicht in welke verbeteringen er nodig zijn om de doelstellingen te bereiken.
Mitz	Veilige onlinetoestemmingsvoorziening waarmee een patiënt zelf zijn toestemmingskeuzes kan beheren en vastleggen
Nuts	Samenwerkingsverband van partijen in de zorg om digitale gegevensuitwisseling tussen zorgorganisaties te faciliteren op basis van een decentraal en open source communicatienetwerk.
OMOP	Een open community datastandaard, ontworpen om de structuur en inhoud van observatiegegevens te standaardiseren en om efficiënte analyses mogelijk te maken die betrouwbaar bewijs kunnen opleveren.
OpenEHR	OpenEHR is een non-profitorganisatie die technische standaarden publiceert voor een EPD-platform samen met in het domein ontwikkelde klinische modellen om inhoud te definiëren.
STRIDE-categorisatie	STRIDE is een classificatieschema voor het karakteriseren/meten van bekende bedreigingen/kwetsbaarheden op basis van het soort misbruik dat wordt gebruikt (of de motivatie van de aanvaller). Het richt zich ook op de eindresultaten van mogelijke aanvallen in plaats van op de identificatie van elke specifieke aanval.
UZI	Het Unieke Zorgverlener Identificatienummer (UZI) wordt gebruikt om een bij het zorgproces betrokken persoon te identificeren. Het nummer is gekoppeld aan het gebruik van de UZI-pas met als doel veilige elektronische uitwisseling van patiëntgegevens.
URA	Een uniek nummer dat een zorgaanbieder heeft voor elektronische communicatie van zorgdata.
XDS	Standaard voor het delen van medische documenten en beelden tussen samenwerkende zorginstellingen.
Zorgnet	Zorgnet is een stelsel van private en beveiligde, niet vanaf het internet te benaderen, landelijk dekkende netwerken





## Samenhang van generieke functies



Figuur 3 Schematische weergave ongericht beschikbaar stellen van gegevens



## Adresseren van patiënten

Eén van de functionele behoeften is het digitaal kunnen adresseren van patiënten via een PGO of via e-mail. Bij de uitwerking van de SOLL-oplossingen werd duidelijk dat een oplossing om patiënten te kunnen adresseren aan andere criteria moet voldoen.

Allereerst is een belangrijk verschil dat bij het adresseren van een zorgaanbieder of zorgverlener het meestal om publiek aanwezige adresgegevens gaat. Adresgegevens van patiënten zijn dit niet, dit zijn persoonsgegevens. Voor adresgegevens van zorgaanbieders zijn er standaarden beschikbaar, voor patiënten is dit er nog niet en dit moet dit nog ontwikkeld worden.

In hoofdstuk 5 worden de SOLL-oplossingen beschreven. Het adresseren van patiënten past niet één op één in deze oplossingen. Er zullen dus aanvullende maatregelen nodig zijn of een aparte functie.

In het geval van een centraal adresboek ligt het niet voor de hand om hier ook patiënten in op te nemen. Het gaat om persoonsgegevens en deze blijven bij voorkeur bij de bron.

Het adresseren van patiënten in een gedistribueerd netwerk kent ook aandachtspunten, waar onder:

- Een patiënt zou zich, met zijn node, in het netwerk bekend kunnen maken. Alle andere nodes, van zorgaanbieders, nemen het adres over. De consequentie is dan dat de adresgegevens van patiënten bij elke zorgaanbieder bekend kunnen zijn.
- Los van de adresgegevens zullen er ook maatregelen genomen moeten worden waarmee vastgesteld kan worden dat gegevens ook daadwerkelijk horen bij de patiënt, zodat de juiste persoon geadresseerd wordt.
- Een zorgverlener zou ook niet zomaar elke patiënt moeten kunnen adresseren, maar alleen als er een behandelrelatie of een andere grondslag is.



## Toetsingskader

Deze bijlage bevat het toetsingskader dat is gebruikt voor de analyse van scenario's voor een landelijk dekkend netwerk voor gegevensuitwisseling in de zorg. We gebruiken hetzelfde toetsingskader voor de analyse van de generieke functies lokalisatie, adressering en autorisatie.

Het toetsingskader is opgebouwd uit 3 delen:

### 1. *Functionele behoeften*

De functionele behoeften ten aanzien van gegevensuitwisseling zijn uiteraard veel breder dan specifieke behoeften m.b.t. lokalisatie. De functionele behoeften voor een lokalisatie-functie zijn beschreven in hoofdstuk 2 van dit rapport.

### 2. *Leidende principes*

Het tweede deel van het toetsingskader bestaat uit leidende principes. Voor elk van deze principes kan worden aangegeven in hoeverre een oplossing eraan kan voldoen. Om een principe leidend te laten zijn moet het aan een aantal voorwaarden voldoen. Dit zijn:

- Het principe is onomstreden, dit houdt in dat het voortkomt uit onomstreden bronnen. Een onomstreden bron is een publiek toegankelijke publicatie (dus geen persoon of organisatie) die aan één van de volgende voorwaarden voldoet:
  - Landelijke of Europese regelgeving: de AVG, de WGBO, de Wabvz en de EHDS;
  - De bron is vastgesteld door het Informatieberaad Zorg: DIZRA;
  - De bron is vastgesteld door het Ministerie van VWS of door een substantieel deel van de veldpartijen: het Integraal Zorgakkoord, de Nationale visie en strategie op het zorginformatiestelsel.

In dit onderzoek zijn er geen nieuwe leidende principes ontwikkeld.

- Het principe is onafhankelijk van een bepaald type architectuur, een specifieke technologie of een specifiek paradigma.
- Het principe is duurzaam. Dit betekent dat het dusdanig is geformuleerd dat het onafhankelijk is van de huidige stand van de techniek (e.g. concrete performance-eisen), bestaande standaarden of de huidige (minimale) functionele behoeften.
- Het principe is eenduidig en vereist geen specialistische voorkennis. Dit betekent dat het principe dusdanig wordt beschreven dat er geen interpretatieverschillen kunnen zijn en dat het principe goed te begrijpen is, ook door niet-architecten.

### 3. *Haalbaarheid*

Een beoordeling van haalbaarheid in termen van financiën (kosten en baten), technische leverbaarheidsrealisatie, realisatie- en implementatetermijn, organisatie en governance, politiek draagvlak.



### Functionele behoeften

De functionele behoeften voor adresseren zijn geformuleerd in hoofdstuk 2. Daarnaast vereisen een aantal functionele behoeften uit het onderzoek naar scenario's voor gegevensuitwisseling in de zorg een adresseringsfunctie. Deze zijn onderstaand weergegeven.

Zorgverleners formuleren onderstaande essentiële behoeften ten aanzien van adresseren.

Functionele behoeften adresseren	
F1	Als zorgverlener wil ik <b>onderscheid kunnen maken tussen wat ik adresseer</b> : een zorgaanbieder, een specifieke afdeling of een specifieke zorgverlener.
F2	Als zorgverlener wil ik andere zorgverleners/zorgaanbieders niet alleen digitaal kunnen bereiken, maar tevens wil ik dat de <b>(logische) naam en de contactgegevens</b> van de zorgaanbieder/zorgverlener aan het elektronische adres gekoppeld zijn.
F3	Als zorgverlener wil ik <b>patiënten digitaal kunnen adresseren</b> , via e-mail of een PGO.

### Leidende principes

Onderstaande leidende principes zijn gedestilleerd uit de volgende onbetwiste bronnen:

- DIZRA 2020
- Integraal Zorgakkoord (IZA) 2022
- EHDS
- Visie op het zorginformatiestelsel, oktober 2022
- Geldende wetgeving.

De principes die niet gebruikt zijn in de beoordeling van lokalisatie zijn in onderstaande tabel grijs gemaakt.

Algemene principes	
1.	Het scenario vervult de <b>functionele behoeften</b> van patiënten en zorgverleners. Niet getoetst: Zie functionele behoeften.
2.	Het informatiestelsel is <b>duurzaam</b> doordat het relevant is en blijft. Het omarmt voor nu en in de toekomst de complexiteit van meerdere standaarden in een stelsel waarin verandering en innovatie welkom is. (DIZRA, 2020)
3.	In het informatiestelsel wordt <b>federatief</b> samengewerkt aan afspraken voor data en voor services. Iedereen implementeert deze afspraken en is aanspreekbaar op het nakomen van de afspraken en de kwaliteit van de implementatie (DIZRA, 2020).
4.	De <b>data blijft bij de bron</b> , onder de verantwoordelijkheid van de bronhouder, voor een veilig en vertrouwd informatiestelsel waarin het voor cliënten transparant is welke bronhouders welke gezondheidsgegevens registreren en wie het raadpleegt. (DIZRA, 2020)  Niet getoetst: het DIZRA-principe gaat over patiëntgegevens. Dit gaat over adresgegevens van zorgaanbieders en zorgverleners.
5.	Er wordt gebruik gemaakt van de zes <b>generieke functies</b> (lokalisatie, identificatie, authenticatie, autorisatie, toestemming en adressering) als deze van toepassing zijn op het scenario (Integraal Zorgakkoord, 2022).



	Niet getoetst: de oplossing gaat specifiek over de generieke functie adresseren.
<b>Afspraken</b>	
Niet getoetst: de principes rondom afspraken zijn aanvullend op de oplossing. In elke oplossing is het mogelijk te kiezen voor open internationale standaarden, machineleesbare data en een gemeenschappelijke taal.	
6.	Semantische en technische interoperabiliteit wordt in het informatiestelsel gerealiseerd door te kiezen voor <b>open internationale standaarden</b> . Iedere deelnemer aan het stelsel moet voldoen aan de standaarden die zijn afgesproken (DIZRA, 2020).
7.	Data is <b>machineleesbaar</b> , machines begrijpen de data, zonder daarbij de leesbaarheid van deze data voor mensen uit het oog te verliezen. Dit opent de mogelijkheden van data-analyse en data-science (DIZRA, 2020).  Niet getoetst: Het principe is aanvullend op de oplossing. In elke oplossing is het mogelijk te kiezen voor machineleesbare data.
8.	In het informatiestelsel spreken we een <b>gemeenschappelijke taal</b> en hanteren gemeenschappelijke terminologie, waarbij we de contextuele verschillen omarmen (DIZRA, 2020).  Niet getoetst: Het principe is aanvullend op de oplossing. In elke oplossing is het mogelijk te kiezen voor machineleesbare data.
<b>Databeschikbaarheid</b>	
9.	Data is beschikbaar voor patiënten en de door de patiënt gemachtigde informele zorgverleners en zij hebben de regie; In het informatiestelsel hebben <b>cliënten regie op hun eigen gezondheidsgegevens</b> en kunnen deze gegevens meenemen en delen in hun reis door het zorglandschap en in het netwerk van zorgverleners en ondersteuners dat zich rondom hen vormt (DIZRA, 2020)  Niet getoetst: de beschikbaarheid van data kan volgen na adresseren, in dit geval van een patiënt, het is geen functie van adresseren zelf.
10.	Informatie dient, ongeacht de elektronische bron, tijd en plaats, <b>beschikbaar</b> te zijn voor zorgverleners die de informatie nodig hebben voor het verlenen van goede zorg (Integraal Zorgakkoord, 2022). Data is beschikbaar voor alle betrokkenen in het zorgnetwerk van een persoon (Visie op het zorginformatiestelsel, 2022).  Niet getoetst: de beschikbaarheid van data volgt na adresseren, het is geen functie van adresseren zelf.
11.	Data worden digitaal, eenduidig en gestandaardiseerd geregistreerd in het zorgproces en beschikbaar gesteld voor diverse <b>secundaire doelen</b> (Integraal Zorgakkoord, 2022). Zorgdata is beschikbaar voor secundaire processen die bijdragen aan verbetering van zorg, met minimale registratielast voor zorgprofessionals (Visie op het zorginformatiestelsel, 2022).  Niet getoetst: de beschikbaarheid van data volgt na adresseren, het is geen functie van adresseren zelf.
12.	Systemen zijn open (Integraal Zorgakkoord, 2022).  Niet getoetst: De zorgaanbieders moeten geadresseerd worden. Vervolgens zijn systemen open om ook daadwerkelijk gegevens op te kunnen vragen. Dit is geen onderdeel van de



	lokalisatie functie.
13.	Data wordt enkelvoudig geregistreerd bij de bron en vervolgens beschikbaar gesteld voor meervoudig gebruik in verschillende toepassingen. Hiervoor hanteert het informatiestelsel de <b>FAIR-data</b> principes (DIZRA, 2020).  Niet getoetst: Dit is een principe dat gesteld kan worden aan bronsystemen, het is niet onderscheidend voor de adresseringsfunctie.
14.	Data uit <b>verschillende bronnen kan gecombineerd</b> worden; zowel uit de bronsystemen van zorgverleners als data die een patiënt zelf verzamelt.  Niet getoetst: dit vraagt functionaliteit van de systemen.
<b>Mededinging</b>	
15.	Het informatiestelsel hanteert een <b>gelijk speelveld voor alle leveranciers</b> . Afspraken worden gemaakt over het gebruik van standaarden, niet over het gebruik van een product of dienst. Iedere organisatie kiest haar eigen leveranciers voor het implementeren van de standaarden (DIZRA, 2020).
<b>Wettelijke eisen</b>	
16.	De functie voldoet aan <b>privacy by design</b> (AVG)
17.	De functie betracht <b>standaard maximale privacy</b> (privacy by default) (AVG).
18.	De functie voldoet aan <b>secure by design</b> (AVG)
19.	De functie dient te voorzien in/ te kunnen samenwerken met een 'national contact point' in de <b>MyHealth@EU infrastructuur</b> , voor toegang tot- en uitwisseling van zorginformatie. (EHDS)  Niet getoetst: Dit principe is niet onderscheidend voor de adresseringsfunctie.

Onderstaand worden de leidende principes nader toegelicht.

## ALGEMENE PRINCIPES

### 1. De functie vervult de functionele behoeften van patiënten en zorgverleners

Zie de eerder beschreven functionele behoeften.

### 2. Het informatiestelsel is duurzaam doordat het relevant is en blijft. Het omarmt voor nu en in de toekomst de complexiteit van meerdere standaarden in een stelsel waarin verandering en innovatie welkom is (DIZRA, 2020)

DIZRA definieert duurzaamheid<sup>5</sup> als volgt: Een duurzaam stelsel gaat niet alleen over gegevensuitwisseling en de standaarden die we daarvoor gebruiken. Duurzaamheid bereik je alleen als we ook de informatiesystemen weten te integreren en weten zorg te dragen voor een optimale informatievoorziening. Om dat mogelijk te maken moeten mensen, processen en technologie op elkaar zijn afgestemd.

De definitie van- en nadere toelichting op het principe 'Duurzaamheid' wordt onverkort overgenomen uit DIZRA. Ten behoeve van de beoordeling van de scenario's wordt het DIZRA-principe met de

<sup>5</sup> Zie <https://dizra.gitbook.io/dizra/perspectieven/motivation/duurzaam>



onderstaande toelichting uitgebreid.

Een onomstreden uitwerking van het begrip duurzaamheid, in de vorm van ontwerpstrategieën of ontwerp patronen, bestaat niet binnen de Nederlandse zorg-ICT. Het DIZRA-principe van duurzaamheid wijst in de richting van **flexibiliteit** en **toekomstbestendigheid**. Bertrand Meyer (Meyer, 1988) stelt dat de flexibiliteit van systemen en architecturen groter is, naarmate de opzet van het systeem/ de architectuur meer modulair is. Dat komt omdat componenten makkelijker kunnen worden gecombineerd (modular composability) en makkelijker kunnen worden aangepast of vervangen (modular continuity). Toegepast op de scenario's betekent dit dat:

- Een scenario is meer duurzaam als de verschillende onderdelen in vrijheid kunnen worden gecombineerd om nieuwe use cases te ondersteunen, die anders zijn dan de use cases waarvoor het scenario oorspronkelijk werd ontwikkeld (modular composability).
- Een scenario is meer duurzaam als een wijziging in de (functionele) requirements of ondersteunde use cases, slechts leidt tot aanpassing van één of hooguit een klein aantal onderdelen (modular continuity).

Voor de beoordeling van de scenario's wordt in dit onderzoek gebruik gemaakt van de volgende 3 strategieën die modulariteit (en dus flexibiliteit en duurzaamheid) verhogen:

- Scheiding van data en functionaliteit (Nictiz, 2022)
- Law of Demeter (Holland, 1987) of 'principle of least knowledge'. Ieder onderdeel (module) van het scenario heeft slechts zeer beperkte kennis van andere onderdelen: uitsluitend kennis van enkele sterk gerelateerde onderdelen (zoals generieke functies)
- Minimale koppeling  
Gerelateerd aan LoD maar meer gericht op communicatie tussen modules: die dient minimaal te zijn. De topologie binnen het scenario bevat zo weinig mogelijk verschillende koppelingen tussen onderdelen, de interfaces van die koppelingen zijn zo klein mogelijk (dataminimalisatie) en asynchrone communicatie waar mogelijk

### **3. In het informatiestelsel wordt federatief samengewerkt aan afspraken voor data en voor services. Iedereen implementeert deze afspraken en is aanspreekbaar op het nakomen van de afspraken en de kwaliteit van de implementatie (DIZRA, 2020).**

Verdere toelichting op [federatief](#) is te vinden bij DIZRA.

De definitie van- en nadere toelichting op het principe 'federatief' wordt onverkort overgenomen uit DIZRA. Ten behoeve van de beoordeling van de scenario's wordt het DIZRA-principe met de onderstaande toelichting uitgebreid:

Federatief afspraken maken is gebaat bij een gelijke uitgangspositie van alle betrokken partijen en bij een zekere mate van autonomie van betrokken partijen over de wijze waarop zij hun rol/ verantwoordelijkheden uitvoeren. Van een scenario wordt daarom gesteld dat zij in mindere mate voldoet aan het principe federatief indien:

- De functie afhankelijk is van centrale partijen voor de uitwisseling van informatie
- En/of De functie in hoge mate de interne werking van systemen voorschrijft.

### **4. De data blijft bij de bron, onder de verantwoordelijkheid van de bronhouder, voor een veilig en vertrouwd informatiestelsel waarin het voor cliënten transparant is welke bronhouders welke gezondheidsgegevens registreren en wie het raadpleegt (DIZRA, 2020)**

DIZRA definieert data bij de bron <sup>6</sup> als volgt: 'Data bij de bron betekent dat we gegevens bij de bron

---

<sup>6</sup> Zie: <https://dizra.gitbook.io/dizra/perspectieven/motivation/data-bij-de-bron>



ophalen en niet door kopiëren. Soms is een kopie noodzakelijk vanuit wettelijke verplichtingen, maar het principe is dat we zo weinig mogelijk kopiëren en zoveel mogelijk gegevens direct bij de bron ophalen. Data bij de bron betekent dat we dezelfde databron hebben voor meerdere ketens. Hierdoor ontstaat een netwerk van data en services. Iedere deelnemer in het netwerk kan zowel afnemer als aanbieder van data en services zijn. Gegevens kunnen hergebruikt en meervoudig gebruikt worden omdat de betekenis van data formeel en machine leesbaar is beschreven. Iedere keten kan op basis van de betekenis bepalen wat zij nodig heeft in haar keten. Eenzelfde databron heeft daardoor vele afnemers in vele ketens.'

De definitie van- en nadere toelichting op het principe 'Data bij de bron' wordt onverkort overgenomen uit DIZRA.

**5. Er wordt gebruik gemaakt van de zes generieke functies (lokalisatie, identificatie, authenticatie, autorisatie, toestemming en adressering) als deze van toepassing zijn op het scenario (Integraal Zorgakkoord, 2022)**

Het is van belang onderscheid te maken tussen generieke functies en gemeenschappelijke voorzieningen. Een generieke functie is een functionele rol binnen een scenario (zoals adressering) die losstaat van een specifieke implementatie van die rol. De generieke functie wordt eenduidig gespecificeerd op zulke wijze dat iedereen een systeem kan implementeren dat in de functie voorziet. Een gemeenschappelijke voorziening implementeert een generieke functie in een systeem voor gemeenschappelijk gebruik. Een gemeenschappelijke voorziening wordt geëxploiteerd door een specifieke partij; de leverancier van die gemeenschappelijke voorziening.

Verplichting van het gebruik van een specifieke gemeenschappelijke voorziening van overheidswege, staat op gespannen voet met het mededingingsrecht. Door generieke functies gedistribueerd te ontwerpen kan worden voorkomen dat een specifieke implementatie (gemeenschappelijke voorziening) dient te worden verplicht. Verplichting van de implementatie en/of het gebruik van generieke functies is mogelijk via de Wegiz. In dat kader worden NEN-normen voor de generieke functies ontwikkeld.

Scenario's kunnen worden beoordeeld in de mate waarin zij een oplossing bieden voor de zes generieke functies en de mate waarin deze functies gedistribueerd ontworpen zijn.

## AFSPRAKEN

**6. Semantische en technische interoperabiliteit wordt in het informatiestelsel gerealiseerd door te kiezen voor open internationale standaarden. Iedere deelnemer aan het stelsel moet voldoen aan de standaarden die zijn afgesproken (DIZRA, 2020)**

De keuze voor het gebruik van open, internationale standaarden wordt breed gedragen. Ook in het Integraal Zorgakkoord en de Visie op het informatiestelsel wordt hiernaar verwezen. DIZRA hanteert de kenmerken van Forum Standaardisatie om open standaarden <sup>7</sup>te definiëren:

- De benodigde documentatie moet laagdrempelig beschikbaar zijn.
- Er mogen geen hindernissen zijn op het terrein van intellectueel eigendomsrecht.
- Er moeten voldoende inspraakmogelijkheden zijn voor stakeholders tijdens de (door)ontwikkeling van de standaard.
- De onafhankelijkheid en duurzaamheid van de standaardisatieorganisatie moeten verzekerd zijn.

De definitie van- en nadere toelichting op het principe 'open standaarden' wordt onverkort overgenomen uit DIZRA.

---

<sup>7</sup> Zie <https://dizra.gitbook.io/dizra/perspectieven/motivation/open-standaarden>





**7. Data is machine leesbaar, machines begrijpen de data, zonder daarbij de leesbaarheid van deze data voor mensen uit het oog te verliezen. Dit opent de mogelijkheden van data-analyse en data-science (DIZRA, 2020)**

Verdere toelichting op Machine leesbaar<sup>8</sup> is te vinden bij DIZRA.

De definitie van- en nadere toelichting op het principe 'machine leesbaar' wordt onverkort overgenomen uit DIZRA.

**8. In het informatiestelsel spreken we een gemeenschappelijke taal en hanteren gemeenschappelijke terminologie, waarbij we de contextuele verschillen omarmen (DIZRA, 2020)**

Een gemeenschappelijke taal is nodig voor het realiseren van interoperabiliteit. Verdere toelichting op de gemeenschappelijke taal<sup>9</sup> is te vinden bij DIZRA. Het gebruik van een gemeenschappelijke taal maakt het mogelijk om dit ook te vertalen naar een taal die door patiënten begrepen wordt. Met het Integraal Zorgakkoord wordt 'passende zorg' nagestreefd. Onderdeel van passende zorg is dat de zorg samen met en rondom de patiënt tot stand komt en wordt ondersteund door informatie passend bij de vaardigheden van de patiënt. Eenheid van taal is randvoorwaarden om aan te kunnen sluiten bij de vaardigheden van de patiënt. De definitie van- en nadere toelichting op het principe 'gemeenschappelijke taal' wordt onverkort overgenomen uit DIZRA.

## DATABESCHIKBAARHEID

**9. Data is beschikbaar voor patiënten en de door de patiënt gemachtigde informele zorgverleners en zij hebben de regie; In het informatiestelsel hebben cliënten regie op hun eigen gezondheidsgegevens en kunnen deze gegevens meenemen en delen in hun reis door het zorglandschap en in het netwerk van zorgverleners en ondersteuners dat zich rondom hen vormt (DIZRA, 2020)**

Databeschikbaarheid voor patiënten is onomstreden, het wordt in verschillende bronnen onderschreven:

- a. Inwoners van Nederland hebben digitaal toegang tot en de beschikking over hun eigen zorggegevens op één plek. Zij kunnen zo desgewenst meer eigen regie nemen op hun gezondheid en zorg en invulling geven aan het samen beslissen met hun zorgverlener. (Integraal Zorgakkoord, 2022).
- b. De persoon zelf heeft beschikking over relevante data, zodat hij in staat is regie te voeren over zijn gezondheidsgegevens (Nictiz, 2022);
- c. Informatie dient, ongeacht elektronische bron, tijd en plaats, beschikbaar te zijn voor de patiënt (EHDS, 2022).

De definitie van- en nadere toelichting op het principe wordt onverkort overgenomen uit DIZRA.

**10. Informatie dient, ongeacht de elektronische bron, tijd en plaats, beschikbaar te zijn voor zorgverleners die de informatie nodig hebben voor het verlenen van goede zorg (Integraal Zorgakkoord, 2022).**

In het Integraal Zorgakkoord (2022) wordt verwezen naar databeschikbaarheid van een kernset voor zorgverleners. De set kerngegevens volgens het IZA betreft de EU-patiëntensamenvatting, lab uitslagen, beelden, verslagen en zorgplannen die nodig zijn voor het verlenen van netwerkzorg. Het IZA sluit hierin aan op de EHDS. In de Visie op het zorginformatiestelsel (2022) wordt beschreven dat het erom gaat dat zorgverleners beschikking hebben over relevante data, zodat zij in staat zijn om hun zorgtaak optimaal te

---

<sup>8</sup> Zie: <https://dizra.gitbook.io/dizra/perspectieven/motivation/machineleesbaar>

<sup>9</sup> Zie: <https://dizra.gitbook.io/dizra/perspectieven/motivation/gemeenschappelijke-taal>



vervullen. Naast het beschikbaar stellen van gegevens gaat het ook over de mogelijkheid om cross-sectoraal gegevens uit te wisselen tussen zorgverleners (offerte aanvraag VWS).

#### **11. Data worden digitaal, eenduidig en gestandaardiseerd geregistreerd in het zorgproces en beschikbaar gesteld voor diverse secundaire doelen (Integraal Zorgakkoord, 2022)**

In de visie op het informatiestelsel (2022) is data beschikbaarheid als volgt beschreven: '...data op het juiste moment, op de juiste plaats en op een eenduidige manier beschikbaar komt en gebruikt wordt (of kan worden), zowel in het kader van preventie als binnen het primaire zorgproces en in secundaire processen, door patiënten, professionals en toepassingen die daartoe gerechtigd zijn.'. Om deze reden is, naast databeschikbaarheid, voor patiënten (en hun gemachtigde informele zorgverleners) zorgverleners een derde toepassing als criterium opgenomen; databeschikbaarheid voor secundair gebruik.

#### **12. Systemen zijn open (IZA)**

De 'openheid' van systemen is veelvuldig onderwerp van (publieke) discussie. In het Integraal Zorgakkoord van 2022 wordt gesteld: De gestandaardiseerde API-strategie van Nictiz is leidend in de wijze van openstelling van systemen. Een onomstreden uitwerking van het principe van 'Openheid' of 'openstelling' is echter in de Nederlandse zorg-ICT niet voorhanden.

In de context van dit onderzoek wordt onder 'openheid' van een systeem verstaan: 'de mate waarin informatie die is vastgelegd door een systeem, toegankelijk is binnen andere systemen en processen'.

Er zijn globaal genomen twee belangrijke ontwerpstrategieën die openheid van systemen bevorderen:

1. Gestandaardiseerde 'vendor neutral' opslag van zorginformatie  
Wanneer alle zorginformatie in een standaardformaat wordt opgeslagen, is deze informatie onafhankelijk van specifieke systemen en per definitie interoperabel. Voorbeelden van een dergelijke strategie in de zorg-ICT zijn openEHR en OMOP.  
  
Deze strategie wordt vaak 'data-centric genoemd'. Het voordeel van deze strategie is dat alle data, onafhankelijk van een specifieke use case, benaderbaar is voor lezen en schrijven. Melius Health Informatics noemt deze strategie 'fundamenteel open' en in contrast met API-led integraties die 'reactief' of 'proactief' open worden genoemd<sup>10</sup>.
2. Gestandaardiseerde API's voor het benaderen van informatie  
Zelfs al is informatie in een vendor-specifiek formaat opgeslagen, kunnen gestandaardiseerde API's toegang bieden tot die informatie. HL7 FHIR is een voorbeeld van een dergelijke strategie. Steeds vaker wordt een dergelijke strategie 'application centric' of 'API-led integration' genoemd. Het bevorderen van deze strategie is onderwerp van de in het IZA benoemde Nictiz API-strategie.

Deze strategie leidt tot beperkte openheid omdat API's niet tot alle in het systeem opgeslagen informatie toegang geven, maar alleen tot informatie waarvoor specifieke API's zijn ontwikkeld.

Scenario's kunnen worden getoetst op 'openheid' door te beoordelen in hoeverre vendor neutrale opslag (zeer open) of gestandaardiseerde API's (beperkt open) een substantieel onderdeel van het scenario zijn.

---

<sup>10</sup> Zie: <https://www.meliushealthinformatics.nl/post/waarom-is-een-pgo-koppelen-moeilijker-dan-een-stopcontact-vervangen>



**13. Data wordt enkelvoudig geregistreerd bij de bron en vervolgens beschikbaar gesteld voor meervoudig gebruik in verschillende toepassingen. Hiervoor hanteert het informatiestelsel de FAIR-data principes (DIZRA, 2020)**

[FAIR data](#) staat voor Findable, Accessible, Interoperable en Reusable. DIZRA heeft dit verder omschreven.

De definitie van- en nadere toelichting op het begrip FAIR-data wordt onverkort overgenomen uit DIZRA.

**14. Data uit verschillende bronnen kan gecombineerd worden; zowel uit de bronsystemen van zorgverleners als data die een patiënt zelf verzamelt.**

Eén van de kenmerken van Passende Zorg is dat het gaat over **preventie** en **gezondheid** in plaats van ziekte. In het kader hiervan is het wenselijk dat het scenario de mogelijkheid ondersteunt om data uit bronnen van professionele zorgverleners te combineren met data buiten het ZorgDomein, zoals het sociale domein, en met data van de patiënt zelf en van niet-professionele zorgverleners.

## MEDEDINGING

**15. Het informatiestelsel hanteert een gelijk speelveld voor alle leveranciers. Afspraken worden gemaakt over het gebruik van standaarden, niet over het gebruik van een product of dienst. Iedere organisatie kiest haar eigen leveranciers voor het implementeren van de standaarden (DIZRA, 2020)**

Een gelijk speelveld <sup>11</sup> wordt door DIZRA als volgt gedefinieerd, waarbij zij de definitie van de Autoriteit Consument en Markt gebruiken: ‘Een eerlijk speelveld is een speelveld waarin de kansen en keuzes van consumenten en andere bedrijven niet worden belemmerd. Een gelijk speelveld zien we ook als een marktsituatie (een speelveld) waar dezelfde regels gelden voor alle leveranciers, waardoor zij een gelijke uitgangspositie hebben om met elkaar te concurreren. Een gelijk speelveld waarin ook voor nieuwe toetreders kansen bestaan om te concurreren.’

De definitie van- en nadere toelichting op het principe ‘Gelijk speelveld’ wordt onverkort overgenomen uit DIZRA.

## PRIVACY EN SECURITY

**16. De functie voldoet aan privacy by design (AVG)**

Privacy by design betekent dat privacy een fundamenteel doel van ontwerp van de functie moet zijn. Dit gaat verder dan alleen het gebruik van Privacy Enhancing Technologies (PET), maar betekent dat de functie wordt ontworpen volgens ‘de stand van de techniek’ en dus volgens erkende privacy design strategies en privacy design patterns.

Een onomstreden uitwerking van het principe van privacy by design in abstracte design strategies en design patterns ontbreekt voor de Nederlandse zorg-ICT. Uitwerking van concrete Privacy Enhancing Technologies is wel beschikbaar, in de vorm van normen als de NEN7510 en de NEN7512. Daarnaast zijn de NEN-normen niet zozeer gericht op ICT-systemen en -architecturen, maar stellen zij eisen aan de kwaliteitssystemen van organisaties.

Voor de beoordeling van de functie wordt in dit onderzoek gebruik gemaakt van de 8 privacy design strategies van Jaap-Henk Hoepman (TNO, 2012):

---

<sup>11</sup> Zie: <https://dizra.gitbook.io/dizra/perspectieven/motivation/gelijk-speelveld>



1. Minimise  
De hoeveelheid verwerkte persoonsgegevens dient minimaal te zijn (niet meer dan voldoende voor het beoogde doel).
2. Hide  
De verwerking van persoonsgegevens dient vertrouwelijk te gebeuren, niet zichtbaar voor onbevoegden.
3. Separate  
De verwerking van persoonsgegevens dient zo veel als mogelijk gedistribueerd plaats te vinden.
4. Aggregate  
De verwerking van persoonsgegevens dient plaats te vinden op het hoogst mogelijke aggregatieniveau (met dus minimaal detail).
5. Inform  
Betrokkenen dienen adequaat te worden geïnformeerd over (de werking van) de verwerking.
6. Control  
De betrokkenen hebben autonomie over de verwerking van hun persoonsgegevens.
7. Enforce  
Een privacy beleid/ vertrouwensmodel dat in overeenstemming is met wet- en regelgeving dient aan de basis van het ontwerp te liggen en te (kunnen) worden afgedwongen.
8. Demonstrate  
Het kunnen aantonen van compliance aan privacy beleid/ vertrouwensmodel en wet- en regelgeving dient aan de basis van het ontwerp te liggen.

#### **17. De functie betracht standaard maximale privacy (privacy by default) (AVG)**

Privacy by default of 'gegevensbescherming door standaardinstellingen' betekent dat een functie standaard de maximale privacy betracht. Daar waar de betrokkene van rechtswege invloed heeft op (de mate van) verwerking van persoonsgegevens, dient dus altijd uitgegaan te worden van maximale privacy. Dit betekent bijvoorbeeld keuze voor een expliciete opt-in in plaats van opt-out.

Op dit moment staat dit principe op gespannen voet met de mogelijkheden om het delen van de juiste informatie te faciliteren. Vanuit het veld komt steeds meer de vraag om opt-out op de gegevens die nodig zijn voor acute zorgverlening. In het toetsingskader gaan we uit van het huidig wettelijk kader, om deze reden is dit principe opgenomen in het toetsingskader.

#### **18. De functie voldoet aan secure by design (AVG)**

Op grond van artikel 32 van de AVG dient een verwerkingsverantwoordelijke passende organisatorische en technische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te borgen. Secure by design is nauw verbonden aan privacy by design, maar richt zich op het inperken van kwetsbaarheden in systemen om bedoelde of onbedoelde inbreuken op de privacy te voorkomen. Secure by design wil zeggen dat kwetsbaarheden al op het niveau van een hoog over abstract ontwerp, zoals de scenario's, worden voorkomen.

Net zoals in het geval van privacy by design, ontbreekt een onomstreden uitwerking van het principe van secure by design in abstracte design strategies en design patterns. Normen zoals NEN7510, NEN7512 en NEN7513 bevatten wel concrete beveiligingsmaatregelen.



Voor de beoordeling van de functie wordt in dit onderzoek gebruik gemaakt van de STRIDE-categorisatie (Praet Garg en Loren Kohnfelder, Microsoft 2009). STRIDE wordt gebruikt door onder andere het Open Web Application Security Project (OWASP). Scenario's kunnen worden beoordeeld op de generieke 'STRIDE' kwetsbaarheden:

1. Spoofing

Spoofing wil zeggen dat een component (fysiek of software) of een menselijke actor zich voordoeft als een ander (bijvoorbeeld door het plegen van identiteitsfraude). Spoofing kan worden voorkomen door gebruik van sterke authenticatie van zowel mens als machine, inclusief de veilige distributie van beveiligingscertificaten. Maar ook de veilige distributie van adresgegevens is van groot belang om spoofing te voorkomen.

2. Tampering

Dit betreft het moedwillig wijzigen van data at-rest of in-motion. Hoe meer bronsystemen in een scenario onderling gegevens uitwisselen, hoe groter de kans dat gegevens in die bronsystemen (at rest) of tussen de bronsystemen (in motion) worden gewijzigd. Het minimaliseren van communicerende bronnen en de methodes van communicatie is dan ook van belang. Het digitaal ondertekenen van berichten en informatie helpt om tampering te detecteren, niet om het te voorkomen.

3. Repudiation

Dit betreft het uitvoeren van niet-traceerbare acties. De functie moet logging van alle acties mogelijk maken, op zo'n wijze dat de log zelf niet kan worden aangepast (immutable), dat detectie op ongeoorloofde acties mogelijk is en dat eenvoudige inzage van de log door de betrokkene mogelijk is.

4. Information Disclosure

Dit betreft het ongeautoriseerd inzien van informatie at rest of in motion. Het digitaal versleutelen van informatie, zowel at rest als (end-to-end) in motion is een maatregel om Information Disclosure te voorkomen. De betrouwbare distributie van sleutels is dan echter een belangrijke voorwaarde.

5. Denial of Service

Naarmate de afhankelijkheid van digitale infrastructuur toeneemt, is de beschikbaarheid van die infrastructuur van steeds groter belang. Voorkomen dient te worden dat delen van de infrastructuur kwetsbaar zijn voor het verwerken van (te) grote hoeveelheden informatie(verzoeken). Maatregelen zijn onder andere het voorkomen van te grote hoeveelheden legitieme verzoeken, maatregelen om verwerking te garanderen zelfs onder grote stress en maatregelen om DOS aanvallen te detecteren en af te slaan.

Centrale scenario's, waarbij de werking van de gehele infrastructuur afhankelijk is van één of enkele centrale componenten, zijn fundamenteel meer kwetsbaar voor Denial Of Service dan gedistribueerde scenario's.

6. Elevation of privilege

Dit betreft het inzien van informatie waarvoor geen autorisatie bestaat door legitieme gebruikers van het netwerk. Maatregelen richten zich vooral op sterke autorisatiecontrole zo dicht mogelijk bij de brondata. Centrale systemen voor autorisatiecontrole zijn geen vervanging voor controle bij de bronsystemen zelf

**19. Het scenario dient te voorzien in/ te kunnen samenwerken met een 'national contact point' in de MyHealth@EU infrastructuur, voor toegang tot- en uitwisseling van zorginformatie. (EHDS)**

Alle Nederlandse zorgaanbieders dienen te worden aangesloten op het national contact point voor zowel ontvangst als verzenden van zorginformatie.



### 3. Haalbaarheid

Haalbaarheid is een breed en ook enigszins subjectief criterium. We beoordelen de haalbaarheid van de lokalisatie functies aan de hand van onderstaande subcriteria.

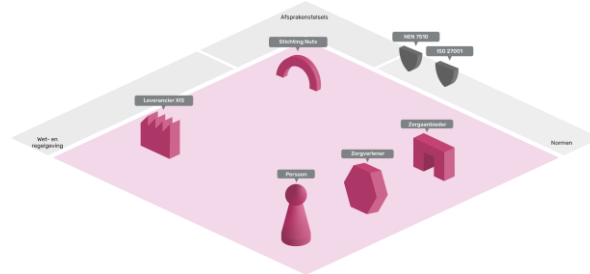
Haalbaarheidscriteria	
H1	De oplossing is <b>technisch haalbaar</b> . We beoordelen een oplossing als technisch haalbaar als de functie met reeds bestaande technologieën kan worden gerealiseerd en reeds is aangetoond dat deze technologie werkt (mogelijk in andere landen of een andere sector dan de zorg).
H2	De functie maakt gebruik van al bestaande oplossingen ( <b>hergebruik van wat er al is</b> ) De haalbaarheid van een oplossing neemt af naarmate de oplossing nieuwe onderdelen introduceert of grote aanpassingen aan bestaande onderdelen (bronsystemen, authenticatiemiddelen, etc.) introduceert.
H3	De <b>impact</b> van de oplossing. De oplossing is meer of minder haalbaar naarmate de impact klein of groot is. We beoordelen daarom de impact van laag tot zeer hoog. We stellen de hoogte van de impact vast op basis van hoe makkelijk of moeilijk het te realiseren is en in hoeverre de werkprocessen veranderen.
H4	De functie kan rekenen op <b>draagvlak bij de leveranciers</b> .
H5	Er is <b>maatschappelijk en politiek draagvlak</b> voor deze oplossing.





### 7.1.4 IST Nuts

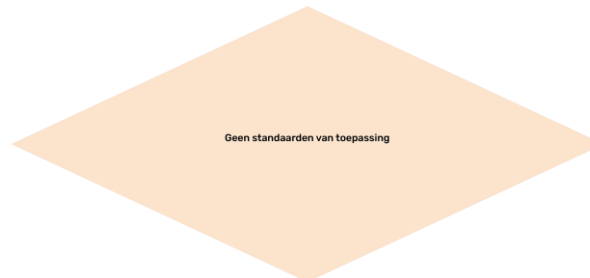
Organisatie



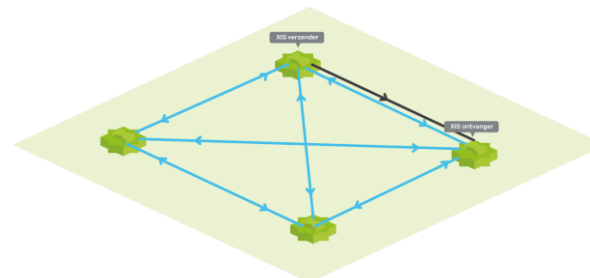
Zorgproces



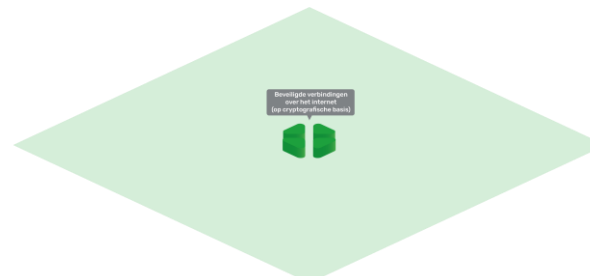
Informatie



Applicatie



Infrastructuur

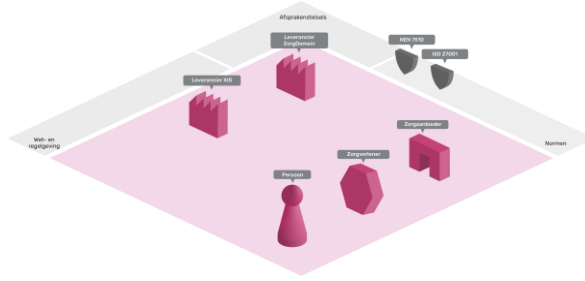




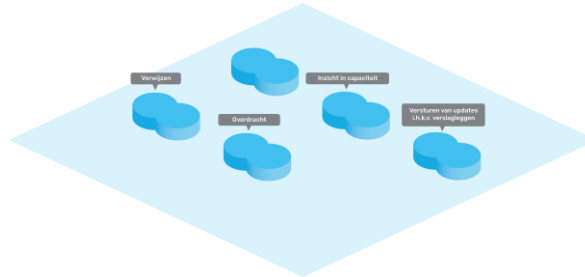


### 7.1.5 IST ZorgDomein

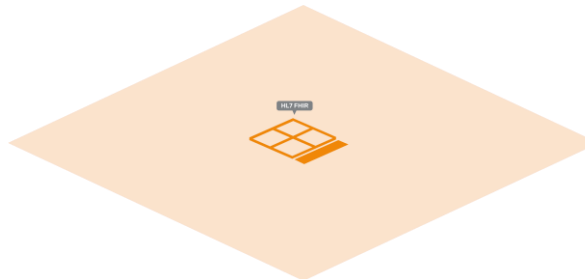
Organisatie



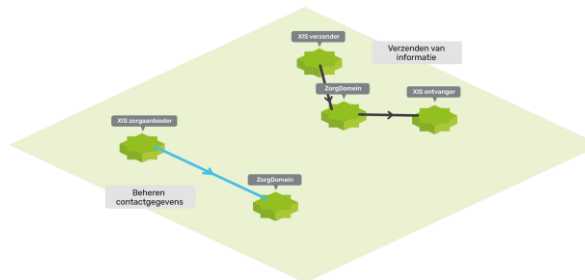
Zorgproces



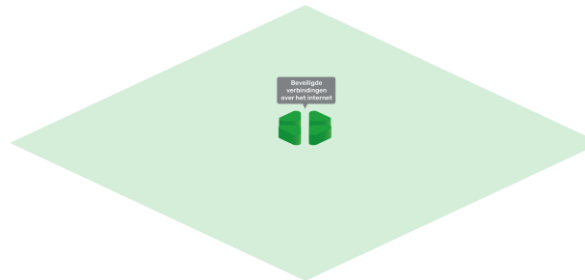
Informatie



Applicatie



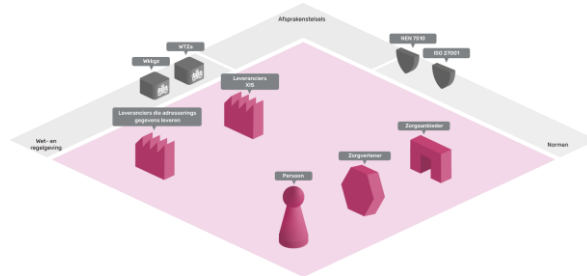
Infrastructuur





**7.1.6 SOLL 1**

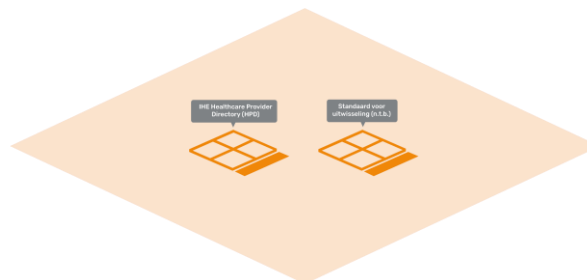
**Organisatie**



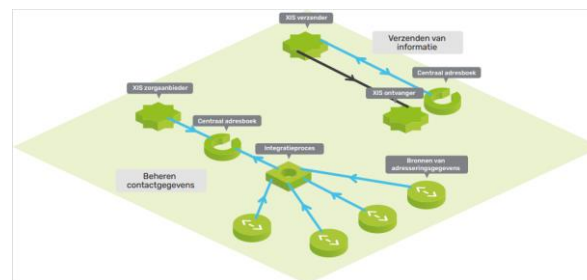
**Zorgproces**



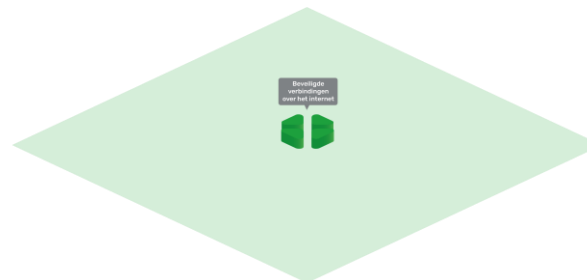
**Informatie**



**Applicatie**



**Infrastructuur**

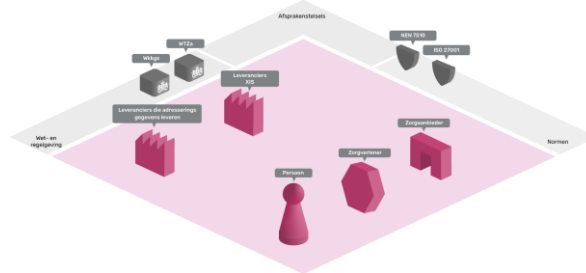






### 7.1.8 SOLL 3

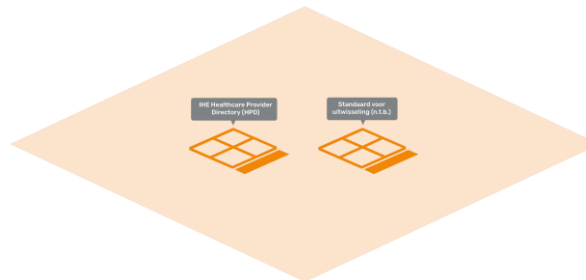
**Organisatie**



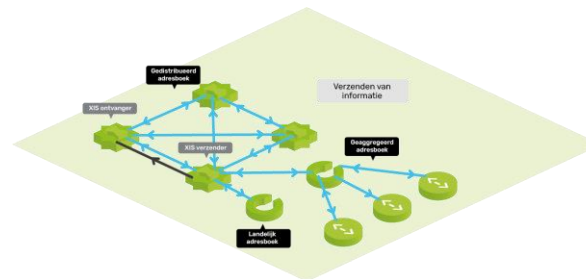
**Zorgproces**



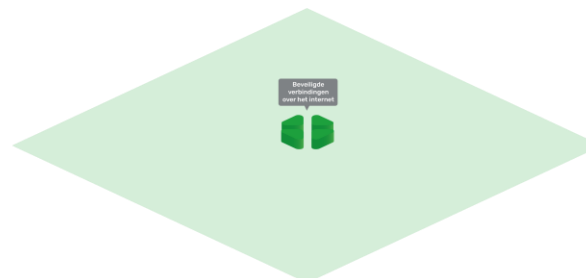
**Informatie**



**Applicatie**



**Infrastructuur**





## Detail analyse SOLL

In deze bijlage is de volledige analyse van de mogelijke oplossingen ten opzichte van het toetsingskader (de functionele behoeften, leidende principes en haalbaarheidscriteria) opgenomen.

Functionele behoeften	SOLL 1	SOLL 2	SOLL 3
	Centraal adresboek	Gedistribueerde oplossing	Combinatie van adresseringsfuncties
<b>Adresseren</b>			
F1 Onderscheid tussen wat adresseren: zorgaanbieder, specifieke afdeling, specifieke zorgverlener	Ja, dit is mogelijk. Het past binnen het IHE-profiel. Alle gegevens kunnen centraal worden opgeslagen.	Ja, dit is mogelijk, maar in twee stappen: adresseren van de zorgaanbieder, vervolgens specifieke adresseringsgegevens opvragen. Er moet een API zijn om de tweede laag in te vullen.	Ja, dit is mogelijk als alle adresseringsfuncties de gegevens aanbieden (in één of twee stappen).
F2 Naast digitale adres ook logische naam en contactgegevens	Ja, dit is mogelijk. Het past binnen het IHE-profiel. Alle gegevens kunnen centraal worden opgeslagen.	Ja, dit is mogelijk, maar in twee stappen: adresseren van de zorgaanbieder, vervolgens specifieke contactgegevens opvragen. Er moet een API zijn om de tweede laag in te vullen.	Ja, dit is mogelijk als alle adresseringsfuncties de gegevens aanbieden (in één of twee stappen).
F3 Patiënten digitaal kunnen adresseren (e-mail, PGO)	Het is mogelijk, maar er is een aanvullende functie nodig. Adressen van patiënten zitten niet in het centrale adresboek.	Ja, Dit is mogelijk, een PGO kan een node in het netwerk zijn, maar er zijn wel aanvullende maatregelen nodig om dit te realiseren.	Ja dit is mogelijk, bijvoorbeeld met een specifieke adresseringsfunctie voor gegevens van patiënten (kan in een systeem staan, maar ook gedistribueerd).



Leidende principes		SOLL 1 Centraal adresboek	SOLL 2 Gedistribueerde oplossing	SOLL 3 Combinatie van adresseringsfuncties
<b>Algemene principes</b>				
P1	Functionele behoeften			
P2	Duurzaam	Ja, als er scheiding van data en functionaliteit is, dit kan door gebruik te maken van open standaarden.	Ja, er is scheiding van data en functionaliteit.	Scheiding van data en functionaliteit. Daarnaast is dit een toekomstvaste oplossing.
P3	Federatief	Nee, er wordt een centrale oplossing gebruikt. Deze zou wel federatief tot stand kunnen komen.	Ja, geen impact op interne werking van systemen en geen afhankelijkheid van een centrale partij.	Geen impact op interne werking van systemen en er is keuze.
P4	Data bij de bron			
P5	Generieke functies			
<b>Afspraken</b>				
P6	Open internationale standaarden	Ja, mits er open internationale standaarden gebruikt worden, zoals het HPD-profiel (IHE).	Ja, mits er open internationale standaarden gebruikt worden, zoals het HPD-profiel (IHE).	Ja, mits er open internationale standaarden gebruikt worden, zoals het HPD-profiel (IHE).
P7	Machineleesbaar			
P8	Gemeenschappelijke taal			
<b>Databeschikbaarheid</b>				
P9	Regie op eigen gegevens			
P10	Relevante data			
P11	Secundaire doelen			
P12	Systemen zijn open			
P13	Fair data			
P14	Combinatie uit verschillende bronnen			



Leidende principes		SOLL 1 Centraal adresboek	SOLL 2 Gedistribueerde oplossing	SOLL 3 Combinatie van adresseringsfuncties
<b>Mededinging</b>				
P15	Gelijk speelveld	Het is een gemeenschappelijke voorziening die door iedereen gebruikt moet worden, daarentegen is het wel gelijk voor alle leveranciers dat ze hierop moeten aansluiten.	Elke leverancier bouwt de functie zelf in en sluit zelf aan.	Elke leverancier kan een eigen oplossing voor adresseren ontwikkelen, mits deze aan de afspraken voldoet.
<b>Privacy &amp; security by design</b>				
P16	Privacy by design	Het gaat in principe niet om persoonsgegevens, maar om publieke gegevens.	Het gaat in principe niet om persoonsgegevens, maar om publieke gegevens.	Het gaat in principe niet om persoonsgegevens, maar om publieke gegevens.
P16	Privacy by default	Het gaat in principe niet om persoonsgegevens, maar om publieke gegevens.	Het gaat in principe niet om persoonsgegevens, maar om publieke gegevens.	Het gaat in principe niet om persoonsgegevens, maar om publieke gegevens.
P18	Secure by design	Oplossing voldoet niet by design: er is een groot risico op spoofing en een single point of failure.	Oplossing voldoet by design.	Niet volledig: de risico's uit SOLL 1 zijn er ook in SOLL 3, maar op kleinere schaal.
P19	National contact point EHDS			



Haalbaarheid		SOLL 1 Centraal adresboek	SOLL 2 Gedistribueerde oplossing	SOLL 3 Combinatie van adresseringsfuncties
H1	Technisch realiseerbaar	Ja, dit scenario kan met bestaande technologieën worden gerealiseerd.	Ja, technisch is dit mogelijk, het wordt op kleine schaal al toegepast.	Moeilijk, omdat functies aan elkaar gekoppeld moeten worden breng dit complexiteit met zich mee.
H2	Gebruik maken van bestaande oplossingen	Gemiddeld, er kan gebruik gemaakt worden van ZORG-AB, maar dit moet dan nog verder doorontwikkeld worden.	Gemiddeld, elk systeem zou de vereisten met betrekking tot deze functie kunnen inbouwen, maar dit vraagt grote aanpassingen.	Gemiddeld, elk systemen kan de huidige oplossing in stand houden. Er zullen wel aanpassingen nodig zijn aan de bestaande oplossingen om ze te kunnen koppelen.
H3	Impact en daarmee samenhangende realisatietermijn	Gemiddeld, omdat er een kleine aanpassing nodig is en alle zorgaanbieders aan moeten sluiten.	Hoog, als gevolg van de benodigde aanpassingen is de impact hoog en de realisatietermijn lang.	Hoog, er moet een oplossing gevonden worden voor het kunnen combineren van verschillende functies.
H4	Draagvlak bij leverancier	Laag, er is weerstand tegen de manier waarop gemeenschappelijke voorzieningen tot stand komen.	Gemiddeld, het draagvlak is wisselend onder leveranciers.	Hoog, elke leverancier kan een eigen keuze maken.
H5	Maatschappelijk en politiek draagvlak	Hoog, er zijn geen maatschappelijke of politieke bezwaren.	Hoog, er zijn geen maatschappelijke of politieke bezwaren.	Hoog, er zijn geen maatschappelijke of politieke bezwaren.





## Geraadpleegde bronnen

- CIBG. (2022). *Waarom verwerkt het CIBG uw persoonsgegevens*. Opgehaald van CIBG:  
<https://www.cibg.nl/lrza#Waarom%20verwerkt%20Het%20CIBG%20UW%20Persoonsgegevens?>
- D&A Medical Group. (2022). *Onderzoek landelijk netwerk van infrastructuren voor gegevensuitwisseling in de zorg*. Den Haag: Ministerie van VWS.
- D&A Medical Group. (2023). *IST EN SOLL ONDERZOEK VOOR DE GENERIEKE FUNCTIE AUTORISEREN*. Den Haag: Ministerie van VWS.
- D&A Medical Group. (2023). *IST EN SOLL ONDERZOEK VOOR DE GENERIEKE FUNCTIE LOKALISATIE*. Den Haag: Ministerie van VWS.
- DIZRA. (2020, April). *Manifest*. Opgehaald van DIZRA:  
<https://dizra.gitbook.io/dizra/manifest>
- Duurzaam, D. (2020). *Duurzaam*. Opgehaald van DIZRA:  
<https://dizra.gitbook.io/dizra/perspectieven/motivation/duurzaam>
- EHDS. (2022). *Proposal for a regulation - The European Health Data Space*. Directorate General for Health and Food Safety.
- Holland, I. (1987). *Law of Demeter*. Northeastern University.
- IHE. (2020, augustus 28). *Healthcare Provider Directory*. Opgehaald van IHE International:  
[https://www.ihe.net/uploadedFiles/Documents/ITI/IHE\\_ITI\\_Suppl\\_HPDPdf](https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPDPdf)
- Integraal Zorgakkoord. (2022, September). *Integraal Zorgakkoord: 'Samen werken aan goede zorg'*. Opgehaald van Rijksoverheid:  
<https://www.rijksoverheid.nl/documenten/rapporten/2022/09/16/integraal-zorgakkoord-samen-werken-aan-gezonde-zorg>
- ITUWRC. (2005, november 11). Opgehaald van International Telecommunication Union: <https://www.itu.int/en/ITU-T/ipr/Pages/open.aspx#:~:text=%20Open%20Standards%22%20are%20standards%20made,are%20intended%20for%20widespread%20adoption.>
- Kenniscentrum voor beleid en regelgeving. (2022, 11 3). *Beleidsinstrumenten op categorie*. Opgeroepen op 11 30, 2022, van Kenniscentrum voor beleid en regelgeving: <https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/integraal-afwegingskader-voor-beleid-en-regelgeving/6-wat-het-beste-instrument/61-beleidsinstrumenten/beleidsinstrumenten-op-categorie>



- Korsten, A. (2019). Omgaan met 'wicked problems'. *Beleidsonderzoek Online*.
- KPMG. (2021). *Digitale gegevensuitwisseling en ICT-infrastructuur in het zorgdomein*. Den Haag: Ministerie van Volksgezondheid, Welzijn en Sport.
- Logius. (2023, februari 13). *Digikoppelingen*. Opgehaald van Logius:  
<https://publicatie.centrumvoorstandaarden.nl/dk/bpadres/#nr-1-direct>
- Meyer, B. (1988). *Object-Oriented Software Construction*. Hemel Hempstead, United Kingdom.
- Nictiz. (2022). *Visie op het zorginformatiestelsel*.
- Nuts. (2023, maart 16). *Nuts wiki*. Opgehaald van Nuts wiki:  
<https://wiki.nuts.nl/books/autorisatie>
- Tesink, W., & Spee, J. (2022). *TxN 2026 - Gezamenlijk groeipad Twiin & Nuts*. Programma Twiin.
- VZVZ. (2022, juni 9). *Het uitwisselingskompas*. Opgehaald van VZVZ:  
<https://www.vzvz.nl/het-uitwisselingskompas>
- VZVZ. (2022). *Het uitwisselingskompas; generieke functies en gemeenschappelijke voorzieningen*.



## Geïnterviewde partijen

De onderstaande partijen zijn geïnterviewd omdat zij een lokalisatie oplossing gebruiken, aanbieden of ontwikkelen.

Naam	Rol
ChipSoft	Adresseringsoplossing in uitwisselingsstelsel
Epic	Adresseringsoplossing in uitwisselingsstelsel
PharmaPartners	Gebruiker van de adresseringsfunctie
Enovation	Adresseringsoplossing in uitwisselingsstelsel
Stichting MedMij	Gebruiker van de adresseringsfunctie
Stichting Nuts	Adresseringsoplossing in infrastructuur
Stichting VZVZ	Adresseringsoplossing in het LSP
Whitebox systems	Gecombineerde adresseringsoplossing in uitwisselingsstelsel
ZORG - AB	Generieke adresseringsoplossing
ZorgDomein	Adresseringsoplossing in uitwisselingsstelsel