Het uitwisselingskompas

Generieke functies en gemeenschappelijke voorzieningen

Datum:	9 juni 2022
Status:	Definitief
Versie:	1.0
Classificatie:	Openbaar
Eigenaar:	Kirsten de Wilde

Inhoudsopgave

1 Inleiding

HET LAATSTE JAAR WORDT DE ROEP OM BEPAALDE FUNCTIES GENERIEK IN TE RICHTEN EN GEMEENSCHAPPELIJKE VOORZIENINGEN TE BIEDEN TER ONDERSTEUNING VAN DE GEGEVENSUITWISSELINGEN IN DE ZORG STEEDS LUIDER. DIT HANGT SAMEN MET DE TOENEMENDE COMPLEXITEIT EN HOEVEELHEID VAN UITWISSELINGEN EN UITWISSELINGSSYSTEMEN. UITWISSELINGSSYSTEMEN ZIJN VEELAL VRAAGGERICHT ONTWIKKELD EN GEVEN INVULLING, OOK NU NOG, AAN EEN SPECIFIEKE INFORMATIEBEHOEFTE.

1.1 Verschuiving naar uitwisseling *tussen* domeinen

Er is in Nederland geen (grote) overlap qua uitgewisselde informatie binnen een domein; de gegevens die via uitwisselingssysteem A worden uitgewisseld, worden vaak niet via uitwisselingssysteem B uitgewisseld. Daarom is de noodzaak om uitwisselsystemen te koppelen binnen een domein er nooit geweest. Echter, door de verschuiving richting netwerkzorg en uitbestede zorg wordt de vraag om uitwisselingen tussen domeinen groter.

1.2 Van generieke functies naar gemeenschappelijke voorzieningen

Daarnaast zijn er generieke functies aan te wijzen die nodig zijn vanuit wet- en regelgeving. Deze zijn voor elk uitwisselingssysteem apart ontwikkeld en vaak verschillend ingericht. Hierdoor wordt uitwisselen tussen verschillende uitwisselsystemen bemoeilijkt. Tevens zorgen de nodige generieke functies tot onnodige druk op het portfolio van leveranciers, aangezien zij, naast hun concurrerende functies, ook noodzakelijke functies moeten bouwen waarvan het niet wenselijk is dat zij hier op concurreren. Het landelijk inrichten van generieke functies in gemeenschappelijke voorzieningen kan efficiënter en effectiever zijn.

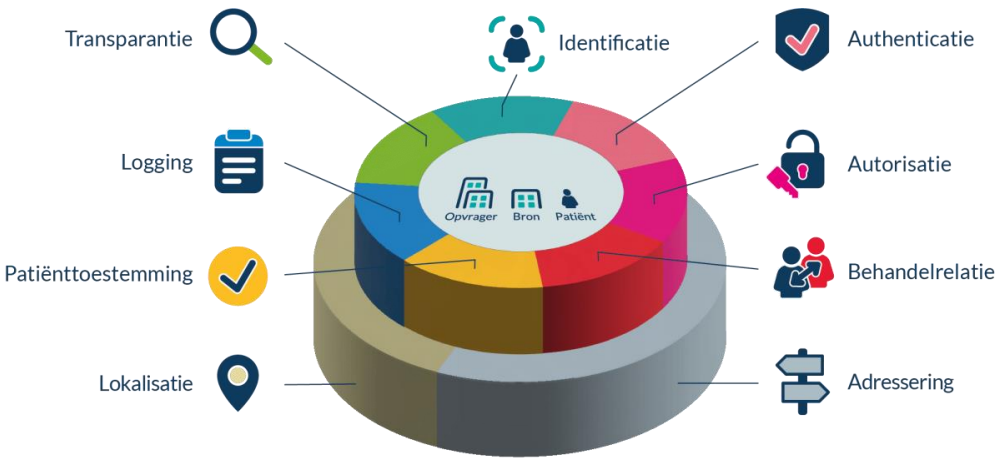
Uiteindelijk is de functionele wens van de eindgebruiker dat het niet uit moet maken welk uitwisselingssysteem er gebruikt wordt door de eigen zorgaanbieder en de uitwisselingspartner.

1.3 Het uitwisselingskompas

Voor goede uitwisseling moeten een aantal waarborgen zijn geregeld die kunnen worden ingevuld met gemeenschappelijke voorzieningen. De verschillende componenten uit het uitwisselingskompas bieden hier handvatten bij. In de volgende hoofdstukken worden de verschillende componenten beschreven in relatie tot gemeenschappelijke voorzieningen.

2 Het uitwisselingskompas in relatie tot gemeenschappelijke voorzieningen

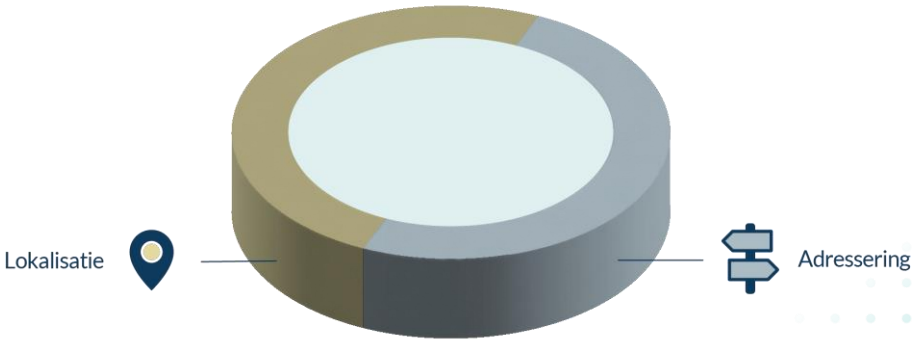
HET UITWISSELINGSKOMPAS BESTAAT UIT TWEE LAGEN. DE BOVENSTE LAAG IS HET VERTROUWENSMODEL. AAN DEZE LAAG WORDT INVULLING GEGEVEN ALS UITWISSELING VAN MEDISCHE GEGEVENS *BINNEN* DE MUREN VAN DE ZORGORGANISATIE PLAATSVINDT; TUSSEN ZORGVERLENERS EN MET PATIËNTEN. BIJ UITWISSELING *TUSSEN* ZORGAANBIEDERS WORDT ER DOOR DE PARTIJEN DIE UITWISSELEN INVULLING GEGEVEN AAN DE BEIDE LAGEN, WELKE SAMEN HET UITWISSELINGSKOMPAS VORMEN.



Figuur 1: Het uitwisselingskompas

Allereerst is het van belang om te benoemen dat het vertrouwensmodel (bovenste laag) niet alleen van toepassing is bij uitwisselingen. Elke zorgaanbieder vertaalt ook binnen de eigen instelling, als er geen gegevens uitgewisseld worden met andere zorgaanbieders, de waarborgen van de bovenste laag van het vertrouwensmodel naar intern beleid.

Wanneer er sprake is van uitwisseling van (medische) persoonsgegevens, komen daar twee functies bij, die geen onderdeel uitmaken van het vertrouwensmodel, maar ingericht moeten worden om de uitwisseling te kunnen faciliteren binnen de wettelijke kaders, namelijk Lokalisatie en Adressering.



Figuur 2: De twee extra functies voor uitwisseling

2.1 Lokalisatie

Waarborgen ten aanzien van lokalisatie zijn nodig in het geval van het opvragen van gegevens wanneer deze ongericht beschikbaar gesteld zijn. In het geval van het ongericht beschikbaar stellen van gegevens worden na toestemming van de patiënt gegevens beschikbaar gesteld aan andere zorgaanbieders, zonder dat vooraf bekend is welke zorgaanbieder de gegevens op welk moment zal opvragen. Een raadplegende zorgaanbieder mag niet zo maar aan alle zorgaanbieders laten weten dat hij een patiënt in behandeling heeft, door aan alle andere zorgaanbieders te vragen om informatie over de patiënt omdat hij niet weet bij welke zorgaanbieders informatie beschikbaar is. Dit wordt overbevraging genoemd en druist in tegen het proportionaliteits- en subsidiariteitsbeginsel uit de AVG. Om dit te voorkomen is een functie nodig om overbevraging te voorkomen en toch antwoord te kunnen geven op de vraag waar informatie over de patiënt beschikbaar is. Gegevens kunnen alleen beschikbaar worden gesteld met de uitdrukkelijke toestemming van de patiënt. Het kan voorkomen dat de zorgaanbieder wel over gegevens van de patiënt beschikt, maar dat de patiënt geen toestemming heeft gegeven om deze gegevens te delen. In dat geval mag deze zorgaanbieder niet geduid worden als zorgaanbieder waar gegevens beschikbaar zijn.

2.2 Adressering

Adressering is zowel noodzakelijk bij het ongericht beschikbaar stellen als bij het gericht versturen van informatie. Bij het gericht versturen van gegevens worden gegevens vanuit het systeem van de brondossierhouder direct naar een bekende ontvanger gestuurd. Hier geeft adressering antwoordt op de vraag, wat het “digitale adres” van de ontvanger is. Bij het ongericht beschikbaar stellen van gegevens geeft adressering de opvragende zorgaanbieder antwoord op de vraag wat het “digitale adres” van de bron is.

3 Generieke functies, gemeenschappelijke en publieke voorzieningen

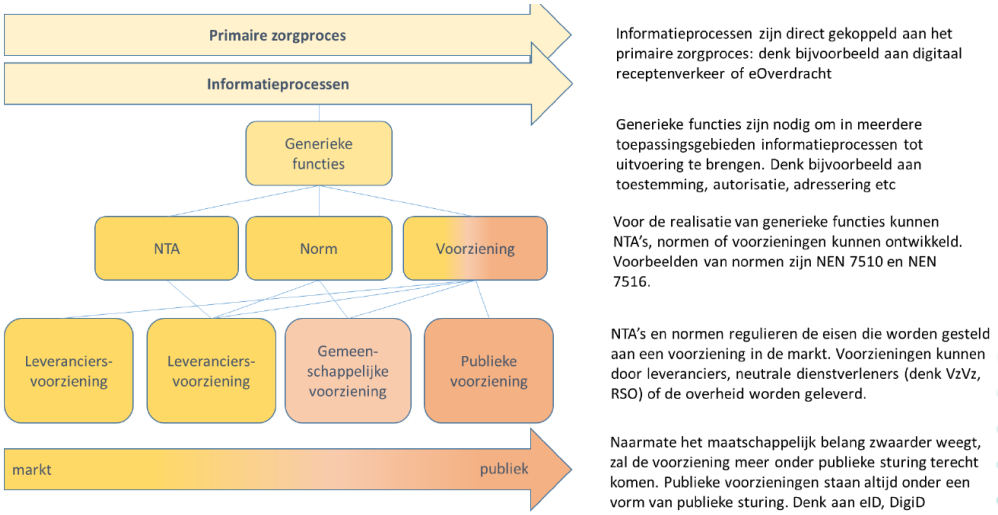
IN "INRICHTEN VAN EEN PROCES VOOR GEMEENSCHAPPELIJKE VOORZIENING; VOORSTEL VAN DE WERKGROEP GOVERNANCE GEMEENSCHAPPELIJKE VOORZIENING[1]" MAAKT HET BUREAU INFORMATIEBERAAD ZORG (BIZ) ONDERSCHEID TUSSEN GENERIEKE FUNCTIES, GEMEENSCHAPPELIJKE VOORZIENINGEN EN PUBLIEKE VOORZIENINGEN.

Generieke functie
Een functie die zorgbreed voor meerdere toepassingsgebieden nodig is om vindbaarheid, toegankelijkheid, interoperabiliteit of hergebruik van gegevens te kunnen realiseren. Een generieke functie is door de zorgICT-markt in te vullen op basis van een set van zorgbrede afspraken, protocollen en open (waar mogelijk internationale) standaarden. Deze afspraken worden in een norm/technische afspraak vastgelegd. Een generieke functie kan onder voorwaarden ook met een gemeenschappelijke of publieke voorziening worden ingevuld. Als voorbeeld van een zorgbrede generieke functie noemt BIZ de toegankelijkheid tot data met een protocol voor autorisatie en authenticatie.

Gemeenschappelijke voorziening
Een product of dienst gericht op het ondersteunen van een generieke functie, waarbij de ontwikkeling wordt overgelaten aan private partijen (marktwerking is mogelijk), maar er één gezamenlijke initiator is die de randvoorwaarden bepaalt (in de meeste gevallen de overheid). Als voorbeeld van een gemeenschappelijke voorziening noemt BIZ toestemming die door zowel VZVZ (Mitz) als door Stichting Nuts wordt aangeboden.

Publieke voorziening
Een product/ dienst gericht op het ondersteunen van een generieke functie, waarbij het noodzakelijk is dat de ontwikkeling plaatsvindt onder publieke sturing, er is samenwerking tussen publieke en private partijen nodig om de voorziening tot stand te laten komen (en er is geen marktwerking mogelijk). Als voorbeeld hiervan, die breder gaat dan de zorg, noemt BIZ DigiD.

Onderstaande afbeelding toont de onderlinge samenhang.

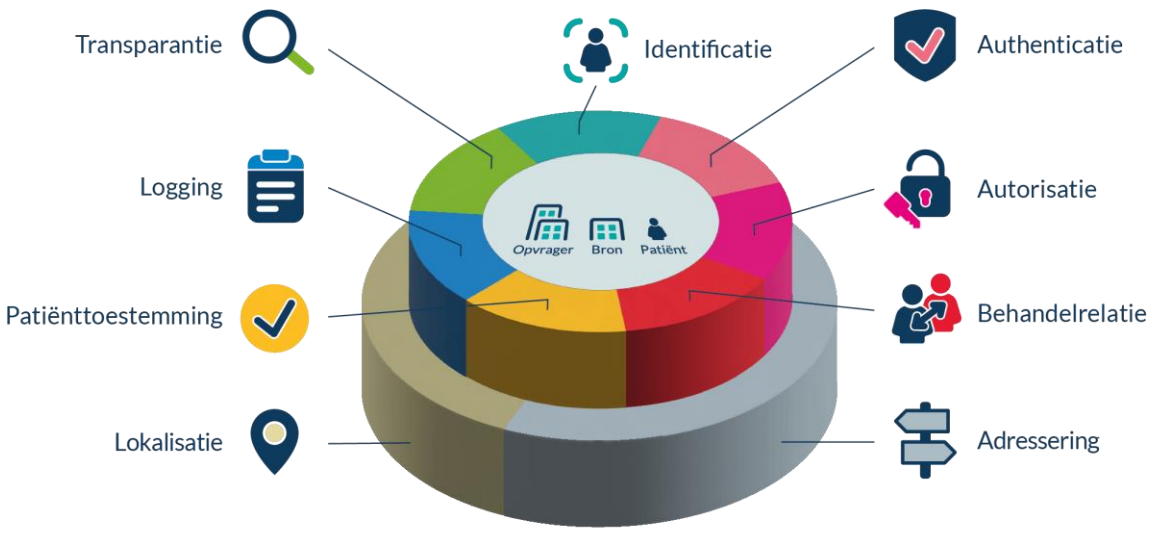


Figuur 3: Samenhang tussen processen, generieke functies en voorzieningen (bron: BIZ)

[1] Tekst overgenomen uit: Bureau Informatieberaad Zorg (4 februari 2021). *Inrichten van een proces voor gemeenschappelijke voorziening; Voorstel van de werkgroep Governance Gemeenschappelijke Voorziening.*

4 Het uitwisselingskompas, uitwisseling en generieke functies, gemeenschappelijke voorzieningen en publieke voorzieningen

ZOALS EERDER IS BESCHREVEN, IS ER BIJ UITWISSELING EEN AANVULLENDE LAAG AAN AFSPRAKEN NODIG ONDER HET VERTROUWENSMODEL. SAMENGEVOEGD LEVEREN HET VERTROUWENSMODEL EN DE UITWISSELFUNCTIES EEN MODEL OP VAN FUNCTIES VOOR UITWISSELING, BESTAANDE UIT NEGEN PUNTEN: HET UITWISSELINGSKOMPAS.



Figuur 4: Het uitwisselingskompas

Per punt van het model wordt beschreven welke generieke functies, gemeenschappelijke voorzieningen en/of publieke voorzieningen er zijn, om zo een beeld te geven van de keuzes die nog gemaakt moeten worden voordat interoperabiliteit voor de uitwisseling van medische gegevens op landelijke schaal gerealiseerd kan worden.

4.1 Identificatie

Identificatie beschrijft op basis van welke attributen patiënten, organisaties en zorgverleners geïdentificeerd worden.

Identificatie van de patiënt

Binnen Nederland is het verplicht om bij de uitwisseling van medische gegevens het BSN van de patiënt mee te sturen als identificatie van de patiënt.

Identificatie van de zorgaanbieder

Zorgaanbieders kunnen op veel verschillende manieren geïdentificeerd worden. Voorbeelden van codestelsels aan de hand waarvan zorgaanbieders geïdentificeerd kunnen worden zijn de AGB-code of het URA.

De AGB-code komt uit het codestelsel van het AGB-register. In dit register staat alle noodzakelijke (zorg) informatie vermeld om het declareren, de zorginkoop, het contracteren en het 'gidsen' van de zorg mogelijk

te maken[2]. Vektis beheert het AGB-register. Zorgaanbieders hebben een AGB-code nodig om geleverde zorg te kunnen declareren.

URA staat voor UZI Register Abonneenummer. Een instelling kan als abonnee in het UZI-register worden geregistreerd wanneer er sprake is van een zorgaanbieder in de zin van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)[3].

Het uitgifteproces van de identificaties bepaalt mede de betrouwbaarheid. URA's worden bijvoorbeeld op een hoog niveau uitgegeven.

Identificatie van de zorgverlener
Zorgorganisatie geven medewerkers vaak een personeelsnummer. Uiteraard heeft een zorgverlener ook een BSN. Echter, het BSN mag in de zorg alleen gebruikt worden om een patiënt te identificeren. Wanneer het BSN van de zorgverlener door een vertrouwde instantie wordt gekoppeld aan een unieke code, kan de zorgverlener wel uniek geïdentificeerd worden. Bij de aanvraag van een UZI-pas stelt het CIBG de identiteit van de zorgverlener of medewerker vast. Deze ontvangt als bewijs daarvan een certificaat op zijn UZI-pas [4].

4.2 Authenticatie

Authenticatie beschrijft de manier waarop een identiteit bewezen kan worden.

Authenticatie van de patiënt
Instellingen zijn verplicht het BSN van de patiënt te verifiëren. Hiertoe wordt gecontroleerd of het BSN voorkomt in de landelijke basisadministratie. Tevens moet de zorgaanbieder de identiteit van de patiënt controleren aan de hand van een identiteitsbewijs. Wanneer een patiënt gebruik maakt van digitale diensten waarin (medische) persoonsgegevens betrokken zijn, moet de patiënt inloggen met een authenticatiemiddel eIDAS hoog[5]. Authenticatiemiddelen met eIDAS hoog zijn echter nog niet breed beschikbaar. De autoriteit persoonsgegevens gedoogt daarom tijdelijk een lager niveau[6]. Hiervoor wordt nu DigiD gecombineerd met SMS gebruikt.

IRMA, is een ander authenticatiemiddel waarmee patiënten kunnen inloggen op een patiëntenportaal[7]. IRMA stelt de patiënt in staat om online, via zijn mobiele telefoon, bepaalde attributen van zichzelf wel te laten zien ("ouder dan 18"), maar ook om andere gegevens juist niet te laten zien (bijvoorbeeld naam of telefoonnummer). IRMA wordt gemaakt door de stichting Privacy by Design. IRMA is een app die de burger op zijn telefoon kan zetten en die hij beveiligt met een pincode[8]. De burger kan attributen, zoals zijn naam, adres, leeftijd en BSN, in de app ontvangen, door eerst bij de uitgever van de attributen (bijvoorbeeld de gemeente voor gegevens uit de basisadministratie) te authentiseren[9] met een ander middel, bijvoorbeeld DigiD. Vervolgens kan de uitgever de bij de burger horende attributen aan de IRMA-app van de burger geven, voorzien van een digitale handtekening. Op dit moment heeft alleen DigiD een wettelijke basis om het BSN te verwerken[10]. Andere (private) inlogmiddelen kunnen deze wettelijk basis ook krijgen als de Wet digitale overheid van kracht wordt en zij als middel worden toegelaten.

[2] Bron: https://www.agbcode.nl/Home
[3] Bron: https://www.uziregister.nl/uzi-pas/word-abonnee
[4] Bron: https://www.uziregister.nl/privacy
[5] Zie voor meer informatie eIDAS: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/identiteit/eidas/
[6] Zie https://www.bdo.nl/nl-nl/perspectieven/eidas-beveiligingsniveau-veranderde-regelgeving-rondom-authenticatie-eisen
[7] Bron: https://irma.app/
[8] Bron: https://privacybydesign.foundation/irma-uitleg/#hoe
[9] Dit bepaalt ook het betrouwbaarheidsniveau van het attribuut
[10] Bron: Beantwoording kamervragen over het bericht dat de IRMA-app wordt gebruikt in een huisartsenpost. 7 januari 2020. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Beschikbare publieke voorziening voor authenticatie van burgers: DigiD[11]

Voor de authenticatie van burgers is DigiD de landelijke standaard. DigiD wordt versterkt, waardoor het een hoger betrouwbaarheidsniveau krijgt . Hierdoor wordt het mogelijk voor overheidsorganisaties en zorginstellingen om meer diensten online aan te bieden. Daarnaast is het de intentie dat de overheid private inlogmethoden toelaat als alternatief voor DigiD. De overheid werkt hiervoor aan een nieuwe wet, de Wet digitale overheid[12]. De Wet digitale overheid (Wdo) heeft als doel het regelen van het veilig en betrouwbaar kunnen inloggen voor Nederlandse burgers bij de (semi-)overheid. Met veilig en betrouwbaar inloggen wordt bedoeld dat burgers elektronische identificatiemiddelen (eID) krijgen met een hogere mate van betrouwbaarheid dan het huidige DigiD. Deze identificatiemiddelen geven publieke dienstverleners meer zekerheid over iemands identiteit. Het Programma eID van het ministerie van Binnenlandse Zaken is bezig met de voorbereiding en invoering daarvan.

Authenticatie van de zorgaanbieder

Wanneer er over authenticatie van zorgaanbieders gesproken wordt, is het van belang onderscheid te maken tussen de authenticatie van de organisatie en van systemen of servers binnen die organisatie.

Beschikbare publieke voorziening voor authenticatie van organisaties: eHerkenning[13]

eHerkenning is een manier om veilig en betrouwbaar in te loggen voor ondernemers, bedrijven, organisaties en intermediairs. eHerkenning wordt gebruikt om online zaken te doen met (overheids)organisaties en daarnaast steeds vaker tussen bedrijven onderling. Met één inlogmiddel kunnen zij nu terecht bij meer dan 500 overheidsorganisaties voor meer dan 1.200 diensten. eHerkenning is persoonsgebonden. Iemands identiteit wordt grondig gecheckt bij de aanvraag. Medewerkers worden gemachtigd om namens hun organisatie specifieke online diensten te regelen. Dit zorgt ervoor dat een organisatie meer zekerheid krijgt over de online identiteit van de persoon waarmee zij zaken doen.
eHerkenning is een initiatief van de Rijksoverheid en is ontwikkeld in samenwerking met het bedrijfsleven. Alleen door de overheid goedgekeurde leveranciers mogen eHerkenning leveren. Deze zogenaamde ‘erkende leveranciers’ voldoen allen aan de strenge eisen en afspraken zoals vastgelegd in het Afsprakenstelsel Elektronische Toegangsdiensten. Namens de Rijksoverheid zorgt Logius (onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties) voor het beheer van het Afsprakenstelsel Elektronische Toegangsdiensten.

Beschikbare publieke voorziening voor authenticatie (burgers en zorgaanbieders): ToegangVerleningService

In opdracht van het ministerie van BZK werkt DICTU aan de ToegangVerleningService (TVS) . De ToegangVerleningService maakt het voor overheidsorganisaties en zorgorganisaties eenvoudig om via inlogmiddelen zoals eHerkenning en DigiD hun digitale dienstverlening te ontsluiten voor ondernemers en burgers. Deze inlogmiddelen worden beschikbaar gesteld door publieke dan wel private partijen. TVS fungeert als toegangspoort voor dienstverleners. Daardoor is het niet langer nodig dat overheidsorganisaties zelf aansluitingen ontwikkelen en beheren voor deze inlogmiddelen. TVS neemt daarmee overheidsorganisaties een zorg uit handen. Ook als er nieuwe inlogmiddelen komen[14]. TVS wordt bovendien voorbereid op het verlenen van toegang met nieuwe toegangsmiddelen in Europees verband (eIDAS). Met TVS kunnen organisaties op hun portalen Nederlandse én Europese ondernemers en burgers nu en in de toekomst identificeren en authentiseren.

Beschikbare gemeenschappelijke voorziening voor authenticatie van apparaten, servers en groepen bij zorgaanbieders: UZI-servercertificaat

Het UZI-servercertificaat is voor systemen[15]. Het servercertificaat waarborgt betrouwbare uitwisseling van zorginformatie. De website, applicatie of server van een zorgaanbieder kan met een certificaat aantonen dat deze bij de zorgaanbieder als UZI-abonnee hoort. Met een servercertificaat kunnen beveiligde verbindingen worden gemaakt. Een servercertificaat mag niet op ieder systeem worden geïnstalleerd. Naast het systeem moet vanwege de veiligheid ook de omgeving waar het systeem staat aan een aantal voorwaarden voldoen.

[11] Bron: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/identiteit/digid/
[12] Bron: https://www.digitaleoverheid.nl/dossiers/wet-digitale-overheid/
[13] https://www.eherkenning.nl/algemeen/over-eherkenning
[14] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/identiteit/toegangsverleningservice/
[15] https://www.uziregister.nl/servercertificaat

Authenticatie van de zorgverlener
Een zorgverlener wordt binnen de instelling digitaal vaak geïdentificeerd op basis van een medewerkerspas. Hiermee kan de medewerker inloggen in het XIS. Voor uitwisseling van medische persoonsgegevens voldoet deze wijze van authenticatie niet aan het vereiste eIDAS hoog niveau. Dit volgt uit het uitgifteproces en niet uit het middel.

Beschikbare gemeenschappelijke voorziening: UZI-register en UZI-pas[16]
De UZI-pas wordt uitgegeven door het CIBG. Met een UZI-pas kan een zorgverlener, afhankelijk van het soort pas dat hij heeft, verschillende zaken regelen: Authentiseren wie hij is, welke functie hij heeft en welke zorgaanbieder hij vertegenwoordigt, versleutelde informatie verzenden en opslaan en elektronische handtekening zetten. Net als een paspoort, is de pas een belangrijk persoonsgebonden waardedocument. De persoonlijke gegevens van de pashouder staan in het certificaat van de pas. In geval van een BIG-geregistreerde zorgverlener, staat ook de rol-code van de zorgverlener in het certificaat van de pas. De pas wordt uitgegeven via een uitgifteproces met betrouwbaarheidsniveau hoog.

Beschikbare gemeenschappelijke voorziening voor eenvoudiger gebruik UZI-pas: ZORG-ID-Smart[17]
Om de kosten van de pas terug te dringen wordt ZORG-ID-Smart ontwikkeld. Met ZORG-ID-Smart wordt de UZI-pas van de zorgverlener op de mobiele telefoon van de zorgverlener geplaatst. Hierdoor zijn er minder fysieke passen nodig. ZORG-ID-Smart werkt zowel met de software Zorg-ID[18] als SafeSign. Daarnaast wordt door de toepassing van extra tokens het mandateren vergemakkelijkt.

4.3 Autorisatie
Via autorisatie wordt bepaald of en welke gegevens de dossierhoudende zorgaanbieder beschikbaar mag stellen aan de raadplegende zorgverlener. Ziekenhuizen zijn verplicht om een autorisatiematrix op te stellen waarin bepaald is welke medewerkers toegang hebben tot (delen van) het dossier. Ook bij uitwisseling tussen zorgaanbieders is het van belang dat alleen de daarvoor geautoriseerde zorgverleners toegang krijgen tot (delen van) het dossier van een andere zorgaanbieder. Omdat de dossierhouders verantwoordelijk zijn voor de toegangsverlening zijn hierover afspraken tussen dossierhoudende zorgaanbieders en de raadplegende zorgverleners. Over het algemeen worden autorisaties gegeven op basis van een rol die een medewerker heeft en niet op persoonsniveau. Zo zal een autorisatie niet gegeven worden aan de heer Pieter Jansen, maar wordt hem de autorisatie toebedeeld op basis van zijn rol als cardioloog in het zorgproces. Afhankelijk van hoe processen zijn ingericht, kan een persoon meerdere rollen hebben binnen de zorgaanbieder.

Zorgaanbieders bepalen zelf op basis van welke rollen zij hun interne autorisatiematrix opstellen. Hierdoor zijn er verschillen in de autorisaties die zorgaanbieders toepassen. Vaak zijn deze verschillen logischerwijs terug te voeren op de wijze waarop processen zijn ingericht. Werken er binnen een ziekenhuis bijvoorbeeld slechts enkele artsen uitsluitend op de SEH, dan zullen alleen deze artsen de autorisaties hebben die bij een SEH-arts horen. Werken in een ziekenhuis alle artsen bij toerbeurt op de SEH, dan zullen zij naar verwachting allemaal ook de autorisaties hebben die bij een SEH-arts horen. Binnen een instelling (zorgaanbieder) is dit uitlegbaar. Lastiger wordt het, wanneer er sprake is van een uitwisseling. Wettelijk gezien mag een zorgaanbieder, ook na toestemming van de patiënt, bij een opvraag via een uitwisselingssysteem (pull) alleen die informatie delen die proportioneel is. Wanneer er geen afspraken over autorisaties bij (pull) uitwisseling worden gemaakt, is de vraag wie bepaalt wat proportioneel is. Hier wordt op verschillende manieren mee om gegaan.

Allereerst moeten zorgaanbieders afstemmen op welke wijze zij de rollen duiden aan welke gegevens beschikbaar mogen worden gesteld. Omdat de dossierhouders verantwoordelijk zijn voor de toegangsverlening moeten de afspraken over de toegang worden gemaakt tussen raadplegers en dossierhouders. In sommige gevallen doen zorgaanbieders dit onderling. Zij spreken dan af welke rollen er bij een uitwisseling gebruikt kunnen worden. De autorisatie die de betreffende rol kan hebben, staat hier vaak los van.

[16] https://www.uziregister.nl/uzi-pas/vraag-een-uzi-pas-aan/kies-de-juiste-uzi-pas
[17] Hier een verwijzing naar ZORG-ID smart zodra deze op de site staat
[18] Bron: https://www.vzvz.nl/diensten/zorg-id/over-zorg-id

In andere gevallen worden de rollen gedefinieerd op basis van de UZI-rolcodes. Zorgverleners met een bepaalde kwalificatie kunnen worden opgenomen in het BIG-register. Zij moeten aan eisen voldoen om hierin opgenomen te worden en hun BIG-registratie te behouden. Zij worden door het BIG-register geregistreerd in een bepaalde rol, bijvoorbeeld cardioloog. Deze BIG-geregistreerde rollen hebben van het UZI-register een UZI-rolcode gekregen. Omdat de UZI-rolcode gekoppeld is aan de inschrijving in het BIG-register, kunnen in beginsel zorgverleners geen UZI-rolcode krijgen wanneer zij niet aan de eisen voldoen die het BIG-register aan de zorgverlener met die rol stelt. De UZI-rolcode beschrijft niet welke autorisaties aan een rol gekoppeld zijn en dus, welke informatie deze rol bij een andere zorgaanbieder kan opvragen in een bepaalde context. Niet BIG-geregistreerde medewerkers worden in dit stelsel niet gedefinieerd als zorgverlener en worden daarom niet gedefinieerd in een rol. Er is een uitzondering gemaakt voor een beperkt aantal niet-BIG geregistreerde beroepen[19]. Medewerkers in deze beroepen kunnen wel een UZI-pas op naam met rolcode krijgen[20].

Ook de manier waarop afspraken worden gemaakt over de autorisaties van rollen, verschilt. Eén manier is om tussen zorgaanbieders af te stemmen dat degene die de opvraag doet, het best kan bepalen welke informatie in de gegeven situatie proportioneel is. In dat geval moet de brondossierhouder erop vertrouwen dat de opvragende partij alleen datgene opvraagt wat er noodzakelijk is en dat alleen daartoe geautoriseerde medewerkers van de opvragende partij kunnen opvragen. De bron heeft in dit geval geen inzicht in welke autorisaties de rollen van de opvragende partij hebben. De brondossierhouder blijft echter verantwoordelijk voor het bepalen wat proportioneel is voor de raadpleger. Dat vergt afstemming en het maken van afspraken.

Een andere manier is om op basis van use cases (context) met de betrokken beroepsgroepen op basis van professionele (kwaliteit)standaarden en -richtlijnen vast te leggen in een autorisatierichtlijn aan welke rol onder welke voorwaarde, welke informatie beschikbaar mag worden gesteld. De autorisatierichtlijn bevat daarom naast een autorisatiematrix (ook wel medisch autorisatieprotocol[21] of MAP genoemd) ook andere afspraken[22] op basis waarvan de afgesproken autorisatiematrix geldt. Deze afspraken stellen de brondossierhouder in staat om bij elke opvraag te controleren of de rol die de opvraag doet, deze opvraag mag doen en om alleen die informatie vrij te geven waarvoor de betreffende rol geautoriseerd is. Voordeel hiervan is dat voor zowel de bron als de opvrager helder is wat er beschikbaar gesteld en dus opgevraagd kan worden. Nadeel hiervan is dat deze afspraken voor elke use case beschreven zullen moeten worden en er geen ruimte voor uitzonderingen is. Een ander nadeel is, dat -bij gebruik van UZI rolcodes- niet BIG-geregistreerde medewerkers in het algemeen geen UZI-rol hebben en daarom niet zelfstandig kunnen opvragen. Dit kan opgelost worden door te werken met mandaten. Hierbij mandateert een zorgverlener met UZI-rolcode een andere medewerker om namens hem gegevens te mogen opvragen. De mandaterende is in dat geval verantwoordelijk voor de opvraag die de gemandateerde namens hem uitvoert. Wanneer er een directe relatie is tussen mandaterende en gemandateerde en wanneer de “span of control” niet te groot is kan dit goed werken. Wanneer de afstand tussen mandaterende en gemandateerde groot is, of wanneer de span of control van de mandaterende erg groot is, rijst de vraag of mandatering nog past binnen het vertrouwensmodel. Een andere oplossing is om als zorgsector, naast de CIBG rolcodes ook andere functiecodes af te spreken. Van belang is hierbij het betrouwbaarheidsniveau in het uitgifteproces van de codes.

Tot slot moeten de zorgaanbieders afspraken maken over waar er controle op de autorisatie plaatsvindt. Dit kan lokaal, bij de opvragende zorgaanbieder of bij de brondossierhoudende zorgaanbieder. Dit kan ook regionaal of centraal plaatvinden. Op het Landelijk Schakelpunt (LSP) vindt de controle op de autorisatie centraal plaats, namens de dossierhouder; de autorisatieafspraken, zoals vastgelegd in de autorisatierichtlijn, wordt voor de betreffende zorgtoepassing geprogrammeerd op het LSP. Bij een opvraag door een zorgverlener controleert het LSP op basis van de UZI-rolcode of en welke informatie er opgevraagd moet worden bij brondossierhoudende zorgaanbieders.

[19] https://zorgcsp.nl/certification-practice-statement-cps
[20] Een beroepsbeoefenaar die zorg verleent in de zin van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, maar geen beroepsbeoefenaar is zoals bedoeld in artikel 3, 34 of 36a van de Wet BIG moeten bij hun aanvraag tot registratie als abonnee stukken overleggen waaruit blijkt dat er zorg wordt verleent, zoals genoemd in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.
[21] Verwijzing naar websites met beschikbare landelijke autorisatierichtlijnen.
[22] Het betreft hier met name afspraken over andere onderdelen van het vertrouwensmodel, zoals bijvoorbeeld de controle op de logging, de transparantie naar de patiënt en afspraken over scholing van medewerkers over de vertrouwelijkheid van medische gegevens.

Beschikbare gemeenschappelijke voorziening: BIG-register en UZI-register
Zoals hierboven beschreven is er vastgestelde welke beroepen zich mogen registreren in het BIG-register. Het CIBG beheert het BIG-register. Het CIBG is onderdeel van het ministerie van VWS[23] en beheert ook het Unieke Zorgverlener Identificatie Register (UZI-register)[24]. Het UZI-register vervult de rol van Trust Service Provider (TSP) [25].

Beschikbare gemeenschappelijke voorziening: vastgestelde landelijke autorisatierichtlijnen
Voor uitwisselingen via het Landelijk Schakelpunt (LSP) worden samen met de koepels van beroepsgroepen en zorgaanbieders en patiënten landelijke autorisatierichtlijnen afgesproken. De beschikbare autorisatierichtlijnen worden gepubliceerd op de website van VZVZ[26].

4.4 Behandelrelatie

Een zorgverlener mag alleen toegang hebben tot (medische) gegevens, wanneer deze een behandelrelatie met de patiënt heeft. In het geval van het opvragen van medische gegevens bij andere zorgaanbieders, geldt in de meeste gevallen de afspraak dat de opvragende zorginstelling er zorg voor draagt dat alleen zorgverleners met een behandelrelatie gegevens opvragen bij een andere zorgaanbieder. Dit kan het zorginformatiesysteem (XIS) van de opvragende zorgaanbieder afdwingen door de behandelrelatie van een zorgverlener in het XIS vast te leggen. Dit is echter niet eenvoudig. Wanneer hier te rigide mee wordt omgegaan, heeft dit als gevolg dat een zorgverlener die onvoorzien toch een behandelrelatie krijgt met de patiënt, niet bij de gegevens in het medisch dossier kan en ook geen gegevens kan opvragen bij andere zorgaanbieders. Wanneer daarentegen de behandelrelatie te ruim wordt vastgelegd in het XIS, verliest het zijn functie.

4.5 Patiënttoestemming

Voor het (ongericht) beschikbaar stellen (medische) gegevens door de dossierhouder is toestemming van de patiënt nodig. Er wordt hierbij onderscheid gemaakt tussen twee vormen van patiënttoestemming; veronderstelde toestemming en uitdrukkelijke toestemming. Voor beide vormen van toestemming geldt dat de patiënt goed geïnformeerd moet zijn over de toestemming die verondersteld kan worden of uitdrukkelijk gevraagd wordt en hoe hij hier bezwaar tegen kan maken. De toestemming mag in bepaalde situaties verondersteld worden, bijvoorbeeld wanneer de patiënt instemt met een verwijzing. Wanneer de zorgaanbieder de patiëntgegevens ongericht beschikbaar wil stellen maken voor toekomstige zorgaanbieders van de patiënt, dan is uitdrukkelijke toestemming noodzakelijk.

Op dit moment wordt de patiënt meestal over de toestemming en de bezwaarprocedure geïnformeerd via de website van de zorgaanbieder en bij het LSP aangevuld met informatie zoals een voorlichtingsfolder en de website van Volgjezorg.

De uitdrukkelijke toestemming van patiënten wordt op dit moment veelal vastgelegd in het bronsysteem. De toestemming vanuit het brondossier kan eventueel doorgezet worden naar het uitwisselingssysteem, bijvoorbeeld in de vorm van een BPPC[27]. De patiënt moet bij elke brondossierhouder uitdrukkelijke toestemming geven voor het beschikbaar stellen van zijn gegevens, of er bezwaar tegen maken. Ook wanneer de patiënt zijn toestemming wil intrekken, moet de patiënt dit bij elke brondossierhoudende zorgaanbieder aangeven. Via de website volgjezorg.nl[28] kan de patiënt zijn toestemming voor het uitwisselen van gegevens via het LSP vastleggen en intrekken.

[23] Bron: https://www.bigregister.nl/registratie
[24] Zie voor verschillende soorten passen: https://www.uziregister.nl/uzi-pas/vraag-een-uzi-pas-aan/kies-de-juiste-uzi-pas
[25] Bron: https://www.uziregister.nl/over-het-register
[26] Verwijzing naar website met autorisatierichtlijnen.
[27] De BPPC wordt gebruikt bij uitwisselingen via bijvoorbeeld XCA. IHE heeft een profiel gedefinieerd om de toestemming van de patiënt te uniformeren. Dit profiel heet BPPC-profiel. BPPC staat voor Basic Patient Privacy Consent. Binnen het BPPC-profiel kunnen verschillende 'policies' gedefinieerd worden. Een policy zou kunnen zijn: 'mijn medische gegevens mogen alleen gedeeld worden met ziekenhuizen in provincie Noord Holland'. De patiënt kan kiezen uit voorgedefinieerde 'policies'. Bron: *Toepassing BPPC-profiel; Richtlijn voor implementatie van toestemmingsprofielen binnen XDS-netwerken.* Nictiz (Juli 2012)
[28] Zie voor meer informatie https://www.vzvz.nl/diensten/volgjezorg

Beschikbare gemeenschappelijke voorziening: Toestemmingsvoorziening Mitz[29]

In een landelijke toestemmingsvoorziening worden de toestemmingen van patiënten centraal vastgelegd. Mitz is ontworpen als landelijke toestemmingsvoorziening. Via MijnMitz kan de patiënt zelf zijn toestemmingen registreren. Via Mitz kan de patiënt aangeven welke zorgaanbieder, welke soort gegevens mag delen met welke soort zorgaanbieders. De zorgaanbieders worden in Mitz geduid in categorieën van zorgaanbieders[30]. De gegevens worden ingedeeld in soorten gegevens. Uitgangspunt is dat er alleen gegevens gedeeld worden die nodig en relevant zijn voor de opvragende zorgverlener binnen de context van de behandelrelatie met de patiënt en binnen de autorisatieafspraken. Mitz zegt niets over de medische autorisatie van zorgverleners. Een zorgmedewerker kan namens een patiënt toestemming vastleggen in Mitz. Een medewerker van een zorginstelling die op verzoek van een patiënt een toestemmingskeuze registreert, moet zelf zorgverlener zijn (BIG-geregistreerd) of onder verantwoordelijkheid van een zorgverlener werken[31]. Door het centraal registreren van de patiënttoestemming in Mitz, hoeft de patiënttoestemming niet meer in elk bronsysteem vastgelegd te worden.

4.6 Logging

Logging heeft twee functies. Allereerst kan door middel van logging het beheer van uitwisselingen goed ingericht worden. Wanneer er technische problemen zijn bij het tot stand brengen van de uitwisseling kan via de logging nagegaan worden waar in de keten het probleem ligt.
De andere functie van logging is dat op basis van inzage in de logging van transacties nagegaan kan worden of de uitwisselingen via de afspraken plaatsvinden. Dit betreft altijd controle achteraf.
Voor beide functies van logging geldt dat de, bij de uitwisseling betrokken zorgaanbieders, afspraken moeten maken over wat er gelogd wordt, hoe er gerapporteerd wordt over de logging, wie inzage heeft in de logging en of en hoe vaak de logging gecontroleerd wordt op naleving van de afspraken.

In de NEN 7513 staan de eisen die aan logging worden gesteld, beschreven. Landelijke afspraken over generieke monitoring van de logging om mis-use cases (bijvoorbeeld: zorgaanbieder X vraagt normaal 3x per dag op en nu 3x per uur, dat is verdacht) tegen te gaan bestaan tot op heden niet. Evenmin bestaan landelijke afspraken over specifieke monitoring. Dit laatste kan alleen de patiënt zelf doen, aangezien deze als enige weet hoe het eigen zorgproces eruit heeft gezien. Hiervoor is het noodzakelijk dat er landelijke afspraken worden gemaakt over transparantie voor de patiënt door de logging van de uitwisseling te koppelen aan de logging voor inzage. Zo weet een patiënt niet alleen wie er heeft uitgewisseld, maar ook wie er heeft ingezien.
Op dit moment wordt logging op uitwisseling nauwelijks gecontroleerd. In de instellingen vindt wel periodiek controle plaats op de logging van inzage van eigen medewerkers in het eigen EPD. Wanneer sprake is van een centraal punt waarover de uitwisseling plaatsvindt, zoals bij een regionaal centraal netwerk, het LSP of het Twiin Portaal, is er wel toezicht op de logging van de uitwisseling. In het geval van LSP kan ook de patiënt via volgjezorg.nl controleren wie zijn gegevens heeft opgevraagd via het LSP.

Transparantie

Het is dus van belang dat er controle kan plaatsvinden op de logging. Dit is een vorm van transparantie. Een andere eerder genoemde vorm van transparantie is informatievoorziening aan de patiënt over de uitwisseling van gegevens, het geven van toestemming voor het uitwisselen van gegevens en de manier waarop de patiënt bezwaar kan maken.

Een andere vorm van transparantie is de inzage door de patiënt in diens gegevens en de uitwisseling van die gegevens. Veel zorgaanbieders bieden patiënten de mogelijkheid om hun gegevens in te zien door middel van een patiëntenportaal. De patiënt kan hierop inloggen en (delen van) zijn dossier bij de betreffende zorgaanbieder inzien.

De patiënt kan ook zijn gegevens van verschillende zorgaanbieders opvragen en bewaren in een Persoonlijke GezondheidsOmgeving (PGO). Om de uitwisseling tussen verschillende PGO-leveranciers en bronsystemen mogelijk te maken, is het afsprakenstelsel MedMij ontwikkeld[32]. Leveranciers en zorgaanbieders moeten aantonen dat zij aan de gestelde voorwaarden voldoen, om vervolgens aan te

[29] Bron: https://www.vzvz.nl/diensten/mitz
[30] Bron: Factsheet Toestemmingskeuzes Mitz. Versie 7 mei 2020
[31] Bron: Whitepaper “Mitz Juridisch”. Versie 20 januari 2022
[32] Voor meer informatie zie https://www.vzvz.nl/diensten/medmij

kunnen sluiten op MedMij en gegevens naar de patiënt de kunnen ontsluiten. Patiënten kunnen zelf kiezen welk PGO zij gebruiken. Patiënten kunnen via hun PGO hun gegevens opvragen bij verschillende zorgaanbieders. De ontsluiting van de gegevens vindt plaats via een DVZA[33]. Brondossierhoudende zorgaanbieders die aangesloten zijn op het LSP, kunnen gebruik maken van LSP+[34] (een DVZA), zodat zij te bevragen zijn voor PGO's.

Voor gegevens die uitgewisseld worden via het LSP biedt de website "Volgjezorg"[35] inzage aan de patiënt in de uitwisseling. Via de website kan de patiënt zien welke zorgaanbieder, wanneer, welke gegevens heeft opgevraagd. Daarnaast kan de patiënt op volgjezorg.nl zien welke zorgverleners hij toestemming heeft gegeven om gegevens beschikbaar te stellen via het LSP.

4.7 Lokalisatie

De lokalisatieservice is een voorziening, die nodig is om er achter te komen waar gegevens van de patiënt beschikbaar zijn. De lokalisatieservice houdt hiervoor een index bij waar zorgaanbieders aan kunnen geven dat ze gegevens van een patiënt hebben. Dat zijn gegevens waarvoor de patiënt toestemming heeft gegeven om te delen.
Het LSP bevat een lokalisatieservice. Bij een vraag aan het LSP, wordt eerst de lokalisatieservice geraadpleegd om te zien aan welke zorgaanbieders de vraag gesteld kan worden. Als patiënttoestemming geregistreerd is bij die zorgaanbieder, volgt antwoord van die zorgaanbieder.

Beschikbare gemeenschappelijke voorziening: Lokalisatieservice Mitz
Mitz kan gebruikt worden als een landelijke lokalisatieservice. Met de zogenaamde 'open autorisatievraag' kan een zorgaanbieder aan Mitz vragen welke bronnen geraadpleegd mogen worden van de patiënt. Mitz kan daar antwoord op geven, door eerst de toestemmingskeuzes van de patiënt te raadplegen; welke bronnen hebben toestemming gekregen van de patiënt om de gegevens beschikbaar te stellen? De toestemming kan categoraal of individueel zijn (aan de bronkant) en in beide gevallen zal Mitz nagaan welke individuele zorgaanbieders zich als bron (dossierhouder) hebben geabonneerd (voor die patiënt op Mitz). Dus alleen met de toestemming van de patiënt wordt het abonnementregister van de betreffende zorgaanbieder(s) geraadpleegd. Het antwoord op de open autorisatievraag bevat de bronnen die daadwerkelijk een dossier van die patiënt beheren en toestemming van de patiënt hebben gekregen om gegevens beschikbaar te stellen aan de categorie raadplegers waar de opvragende instelling toe behoort.

4.8 Adressering

Zorgaanbieders wisselen op verschillende manieren elektronisch gegevens met elkaar uit[36]. Dat kan via een goed beveiligde infrastructuur zoals het Landelijk Schakelpunt, maar ook via bijvoorbeeld beveiligde e-mailservices, XDS-, MedMij- en Mitz-diensten. Voor al deze vormen van gegevensuitwisseling is het noodzakelijk dat zorgaanbieders elkaar snel kunnen vinden, zodat gegevens naar een juist adres worden verstuurd. Verschillende landelijke zorginitiatieven, zoals de invoering van een landelijke voorziening voor toestemmingen (Mitz) en de ontwikkelingen binnen MedMij, vragen om één digitaal adresboek van beschikbare zorgaanbieders.

Beschikbare gemeenschappelijke voorziening: ZORG-AB[37]
ZORG-AB is een gemeenschappelijke adresinformatievoorziening die alle dienstverleners in de zorg kunnen gebruiken om (medische) gegevens met elkaar uit te wisselen. ZORG-AB voorziet in de sterke behoefte aan één betrouwbare en actuele bron met alle gedetailleerde (digitale) adresgegevens van zorgaanbieders en zorgverleners in Nederland. ZORG-AB bevat naast de noodzakelijke contactinformatie ook allerlei technische informatie om computers en applicaties met elkaar te kunnen verbinden. Compleet met alle gegevens, zoals statutaire- en gevelnamen, URA- en/of AGB-codes en elektronische adressen/services die nodig zijn voor de uitwisseling van medische gegevens en het optimaliseren van administratieve processen. Een deel van de informatie wordt ontsloten vanuit bronregisters en kan alleen daar gewijzigd worden.

[33] Voor meer informatie zie Factsheet MedMij "DVZA-kwalificatie". Versie november 2021.
[34] Voor meer informatie zie https://www.vzvz.nl/diensten/lsp
[35] Voor meer informatie zie https://www.vzvz.nl/diensten/volgjezorg
[36] Bron: https://www.vzvz.nl/diensten/zorg-ab
[37] Voor meer informatie zie https://www.vzvz.nl/diensten/zorg-ab

Wanneer zorgaanbieders, veelal via hun XIS-leverancier, aansluiten op ZORG-AB kunnen zij zelf aanvullende informatie ontsluiten naar ZORG-AB. Denk bijvoorbeeld aan locaties, de beschikbaarheid van zorgverleners, diverse e-mailadressen en (mobiele) telefoonnummers. De zorgaanbieder wordt dan ook zelf auteur van deze informatie en blijft daar ook zelf verantwoordelijk voor.