IST EN SOLL ONDERZOEK VOOR DE GENERIEKE FUNCTIE AUTORISEREN

Ministerie van Volksgezondheid,
Welzijn en Sport

Datum	29 augustus 2023
Versie	1.0

D&A medical group BV
Postbus 71
4180 BB Waardenburg
www.dnagroup.nl

INHOUDSOPGAVE

1 OPDRACHTOMSCHRIJVING EN ONDERZOEKSAANPAK

1.1 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 de 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 duidelijke 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 een mogelijke oplossingsrichting. Autorisatie in de zorg is complex en elk detail van een oplossing heeft mogelijk veel impact. Dit rapport maakt het mogelijk om op inhoudelijke gronden (o.a. technisch en operationeel) een keuze te maken voor een ontwikkelperspectief voor de langere termijn.

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

- Een overzicht van de beschikbare oplossingen voor Autoriseren;
- Een voorgestelde SOLL-oplossingsrichting met praktijkvoorbeeld;
- Een inschatting van de haalbaarheid van een sectoroverstijgende implementatie per 2025;
- Analyse van de voorgestelde oplossingsrichting.

1.2 Onderzoeksaanpak

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

<u>Stap 1. Probleemdefinitie en een analyse van de functionele behoeften.</u>
Ten behoeve van het doorgronden van het probleem en de (functionele) behoeften voor een functie Autoriseren 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 autorisatiefunctie. De uitkomsten van deze workshops zijn samengevat in hoofdstuk 2.

Stap 2. Consultatie van partijen die oplossingen voor autoriseren ontwikkelen en implementeren.
Parallel aan de workshops met het expertteam, hebben semigestructureerde interviews plaats gevonden met partijen die (deel)oplossingen ontwikkelen en bieden voor autorisatie. Zie bijlage 7.6 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 7.3).

Stap 3. Een analyse van de haalbaarheid van de oplossing.
Voor de analyse van de functionele, organisatorische en politieke haalbaarheid van de zorgbrede oplossingsrichting 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 7.2.

De analyse en beoordeling van de oplossingsrichting is samengevat in hoofdstuk 5. In de beoordeling kijken wij ook naar aansluiting op project Janus[1] (VZVZ, 2023) en de aandachtspunten voor implementatie.

Bovenstaande analyses leiden tot een advies voor de functie Autoriseren, zie hoofdstuk 6.

[1] Het Informatieberaad van 30 november 2020 (besluit B27-04) heeft aan VZVZ de opdracht verstrekt om landelijke autorisatieafspraken op te stellen, op basis waarvan zorgaanbieders en zorgverleners met vertrouwen veilig informatie kunnen beschikbaar stellen en uitwisselen. VZVZ heeft hiervoor het programma Janus ingericht. Meer informatie over het programma via: https://www.vzvz.nl/initiatieven/programma-janus

2 PROBLEEMDEFINITIE EN FUNCTIONELE BEHOEFTEN

2.1 Introductie

Om tot een goed begrip te komen van het vraagstuk autoriseren en de functionele behoeften voor een generieke functie Autoriseren 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 patiënte onder behandeling is. Dit betreft informatie beschikbaarheid 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 zorgverleners in de huidige situatie ervaren en welke essentiële behoeften zij hebben die verband houden met autorisatie.

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).

2.2 Definitie

In dit onderzoek wordt de onderstaande definitie voor Autoriseren gehanteerd:
"Het verlenen van toegang aan een partij[2] tot bepaalde informatie of om een bepaalde actie uit te voeren".

In het uitwisselingskompas (VZVZ, 2022) wordt autorisatie als volgt omschreven:

1. Via autorisatie wordt bepaald of en welke gegevens de dossier houdende zorgaanbieder beschikbaar mag stellen aan de (interne en externe) zorgverleners. Een zorgaanbieder richt daarvoor een autorisatiematrix in.
2. Ook voor uitwisselingen tussen zorgaanbieders moeten autorisatieafspraken worden gemaakt. Dit heeft tot doel te regelen dat alleen de noodzakelijke medische gegevens worden uitgewisseld, passend bij het zorgproces.
3. Gegevensuitwisselingen moeten proportioneel zijn en gebaseerd op een bepaald doel.

In dit rapport wordt expliciet gekeken naar gegevensuitwisseling tussen zorgaanbieders en dus met externe zorgverleners. Door autorisatie te benaderen volgens de in dit rapport gehanteerde definitie worden de geldende wetten en regelgeving opgevolgd en sluiten wij aan bij de omschrijving van het uitwisselkompas.

Daarnaast zien wij ook de relatie met de generieke functies Toestemmingen, Lokalisatie en Authenticatie. De beginselen voor informationele privacy van de patiënt worden gewaarborgd, waarbij de patiënt zeggenschap behoud over zijn eigen gegevens. In de praktijk betekent dit dat de patiënt (expliciete) toestemming moet geven voor het lokaliseren en delen van zijn gegevens met derden. Een zorgverlener is alleen bevoegd om medische gegevens van een patiënt in te zien als er een behandelrelatie bestaat. Het controleren of degene die toegang zoekt ook daadwerkelijk degene is die hij pretendeert te zijn valt onder de generieke functie Authenticatie en valt buiten de scope van deze opdracht.

2.3 Functionele behoeften autoriseren

De functionele behoeften van zorgverleners met betrekking tot autoriseren zijn samen te vatten in één behoefte:

- Zorgverleners kunnen vanuit en voor hun rol of functie, mits zij bevoegd zijn, op het juiste moment over de juiste informatie over de patiënt beschikken.

Daarnaast willen patiënten (en hun mantelzorger, wanneer de patiënt daar toestemming voor gegeven heeft) hun eigen medische gegevens kunnen raadplegen.

De bevoegdheden van zorgverleners om informatie te raadplegen worden vastgesteld aan de hand van wet- en regelgeving (inclusief grondslagen), zie paragraaf 3.1.. Zorgverleners mogen alleen patiëntgegevens raadplegen indien een grondslag voor gegevensuitwisseling aanwezig is. Een grondslag is bijvoorbeeld een actieve behandelrelatie tussen de zorgverlener en de patiënt.

[2] Dit kan een zorgverlener, zorgaanbieder of patiënt zijn. Waar er in dit rapport verwezen wordt naar de patiënt wordt ook de cliënt en de burger bedoeld.

Met betrekking tot de functionele behoefte van patiënten: patiënten zouden altijd geautoriseerd moeten zijn om hun eigen medische gegevens te raadplegen. Dit is niet afhankelijk van een use case. De complexiteit zit in het waarborgen dat de patiënt is wie hij zegt dat hij is. Dit is onderdeel van de generieke functie authenticatie.

Voor secundair gebruik zijn de functionele behoeften mogelijk anders en kunnen deze tot een andere oplossing voor autorisatie leiden. Dit valt buiten scope van dit onderzoek.

3 IST - BESCHIKBARE OPLOSSINGEN

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

- Autorisatie in het LSP
- Autorisatie in Nuts
- XDS
- Whitebox.

In dit document worden de IST- en SOLL-oplossingsrichtingen beschreven volgens het Nictiz lagenmodel. De aspecten 'beveiliging' en 'wet- en regelgeving' zijn hierop van toepassing. Voor elk van de oplossingen, beschreven onder IST en SOLL, geldt dat ze moeten passen binnen de huidige wet- en regelgeving. Randvoorwaarde voor raadpleging is dat de patiënt zijn/haar expliciete (opt-in) toestemming heeft gegeven aan de dossierhouder.

3.1 Beveiliging en wet- en regelgeving

Vanwege de bijzondere gevoeligheid van medische gegevens is het bij gegevensuitwisseling noodzakelijk om zorgvuldig met privacy van patiënten om te gaan. Om deze reden is wet- en regelgeving rondom autoriseren een complex vraagstuk. In dit hoofdstuk worden de belangrijkste aspecten hoog-over beschreven.

Om ervoor te zorgen dat de juiste zorgaanbieder of zorgverlener geautoriseerd wordt en toegang krijgt tot de medische gegevens van een patiënt dient in beginsel rekening gehouden te worden met het recht op privacy van de patiënt. In de Nederlandse Grondwet is het recht op privacy te vinden in art. 10 (Rijksoverheid, 2023).

- Art. 10 lid 1: recht op eerbiediging van persoonlijke levenssfeer behoudens bij of krachtens de wet te stellen beperkingen.
- Art 10 lid 2 en 3: regels inzake de bescherming van de persoonlijke levenssfeer bij het vastleggen en verstrekken van persoonsgegevens (informationele privacy); daarbij geeft zij ook regels over het recht op inzage en op verbetering van gegevens.

Specifiek voor autorisatie schrijft de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) het volgende voor: Binnen een elektronisch uitwisselingssysteem worden aan zorgaanbieders bevoegdheden toegekend met betrekking tot - onder meer - het aanmelden en opvragen van gegevens. Om te verzekeren dat deze bevoegdheden niet verder reiken dan voor de behandeling van de betrokkene noodzakelijk is, dienen de zorgaanbieders gezamenlijk een autorisatiebeleid te formuleren. Dit autorisatiebeleid koppelt bevoegdheden van zorgaanbieders aan hun zorginhoudelijke rol (Rijksoverheid, 2020).

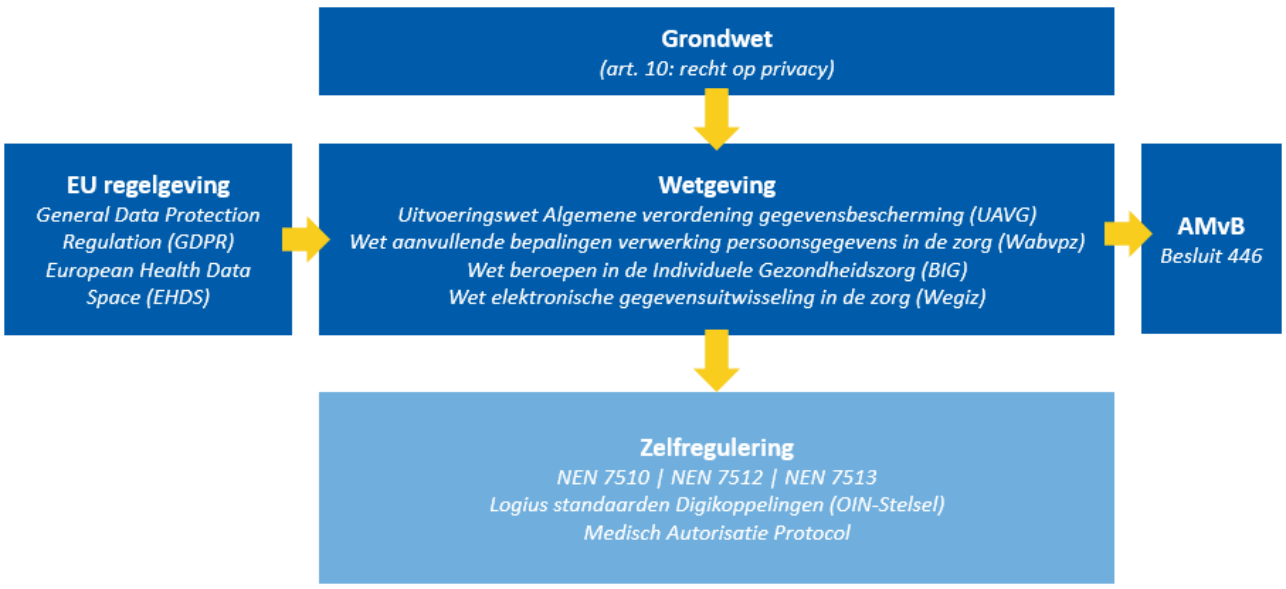
In de NEN 7512 (NEN, 2022) worden richtlijnen gegeven over autorisatie. De norm schrijft voor dat de dossierhouder (zorgaanbieder) verantwoordelijk is voor de toegangsverlening (WGBO, AVG, Wabvpz) tot het patiëntdossier. Hieronder te verstaan dat:

- Uitwisseling pas kan nadat er autorisatieafspraken zijn gemaakt tussen dossierhouders en raadplegers;
- De dossierhouder bepaalt welke rollen (intern/extern) toegang krijgen tot (delen van) het patiëntendossier.

Op Europees gebied gaat de European Health Data Space (EHDS) een steeds grotere rol spelen. De EHDS bouwt voort op de mogelijkheden die de General Data Protection Regulation (GDPR) biedt voor Europese wetgeving omtrent het gebruik van medische gegevens. Specifiek voor autoriseren schrijft de EHDS het volgende voor: “Maak afspraken over autorisatieniveaus voor bepaalde rollen van zorgverleners”. In de EHDS worden deze rollen tevens gekoppeld aan de authenticatie niveaus. Dat wilt zeggen dat alleen specifieke zorgverleners toegang krijgen tot (bepaalde delen van) het patiëntendossier.

Het Organisatie-identificatienummer (OIN), is een uniek nummer waarmee organisaties zich kunnen identificeren, autoriseren en of authentiseren en wordt gebruikt in de elektronische gegevensuitwisseling. Het OIN-nummer wordt als identificerend nummer gebruikt in PKI overheid certificaten (authenticatie), in de adressering en routering van berichten, en in autorisatietabellen. Organisaties mogen het OIN gebruiken voor identificatie van organisaties en organisatieonderdelen in het digitaal verkeer. Het UZI-nummer maakt onderdeel uit van het OIN stelsel (Logius, 2020).

De opbouw van wet- en regelgeving is weergegeven in figuur 2. Europese regelgeving overtroeft de Nederlandse wetgeving, omdat alleen op die manier eenheid in wetgeving binnen de EU kan worden gerealiseerd. Wetten bevatten ‘dwingendrechtelijke normen’, wat betekent dat elke afspraak die ervan afwijkt nietig is. In een AMvB of Koninklijk Besluit (KB) kunnen bijvoorbeeld specifieke functionele, technische en organisatorische eisen worden geformuleerd. Met zo’n AMvB kan steeds worden ingespeeld op de actuele stand van zaken. Deze worden in een gedragscode, protocol of richtlijn vastgelegd. Zelfregulering heeft niet dezelfde rechtskracht als een wet. Zij is ‘niet-bindend’. Tegelijkertijd zal men wel goed moeten kunnen motiveren waarom men van een richtlijn, protocol of gedragscode afwijkt, als dat het geval is.



Figuur 2 Verhouding relevante wet- en regelgeving t.a.v. autoriseren.

3.2 LSP

Autorisatie op het LSP gebeurt door middel van autorisatierichtlijnen. Per dataset die wordt uitgewisseld zijn autorisatieregels opgesteld.

Tabel 1 Samenvatting Autorisatie LSP

Organisatie	De autorisatierichtlijn beschrijft wie welke gegevens uit het patiëntendossier mag raadplegen en wie niet.
Proces	Autorisatie is gekoppeld aan de autorisatiematrix die hoort bij de use case.
Informatie	Er wordt uitgewisseld op basis van informatiestandaarden voor de betreffende use cases. Op basis van een rolcode uit het aanvragende systeem wordt bepaald of de betreffende gegevensset uit het bronsysteem mag worden opgevraagd.
Applicatie	De autorisatiefunctie, waarin de controle op autorisatie plaatsvindt, is onderdeel van het LSP.
Infrastructuur	Om gebruik te maken van het LSP moet het systeem aangesloten zijn en voldoen aan de eisen voor een Goed Beheerd Zorgsysteem.

Organisatie

Wanneer er gegevens worden uitgewisseld over het LSP, wordt er alleen toegang verleend tot gegevens, als aan de volgende voorwaarden voldaan wordt:

- De patiënt heeft uitdrukkelijk toestemming (opt-in) gegeven aan de dossierhouder;
- Er is een behandelrelatie tussen de zorgverlener die de gegevens opvraagt en de patiënt;
- Een zorgverlener (die bij het behandelproces betrokken is) onder mandaat van een BIG-geregistreerde zorgverlener informatie opvraagt;
- De zorgverlener BIG-geregistreerd is, werkzaam is bij een zorgaanbieder die mag aansluiten op het LSP en gebruik maakt van een Goed Beheerd Zorgsysteem (GBZ).

Het LSP heeft een Medisch Autorisatieprotocol waarin afspraken zijn opgenomen aan welke (zorgverleners)rol en onder welke voorwaarden, welke informatie beschikbaar mag worden gesteld bij specifieke use cases. Deze afspraken zijn gemaakt met de betrokken beroepsgroepen op basis van professionele (kwaliteits)standaarden en -richtlijnen en zijn vastgelegd in een autorisatierichtlijn voor de betreffende use cases. Hierbij wordt gebruik gemaakt van de rolcodes die door het UZI-register beschikbaar zijn gesteld.

Proces

De autorisatiematrix wordt toegepast voor die situatie waarin dossiergegevens uit bronsystemen worden geraadpleegd:

- Medicatieverstrekkingen uit het systeem van de apotheek en apotheekhoudende huisarts;
- Intoleranties/allergieën en contra-indicaties uit het systeem van de voorschrijvers en apotheken;
- Ketenzorginformatie uit de systemen van de betrokken zorgverleners.

Informatie

Er wordt uitgewisseld op basis van informatiestandaarden voor de betreffende use cases.

Applicatie

De autorisatiefunctie is nu (nog) onderdeel van het LSP. Het LSP neemt hiermee de controlerende taak van het systeem van de dossierhouder over. Op basis van een rolcode van de zorgverlener uit het aanvragende systeem bepaalt het LSP of de betreffende gegevensset uit het bronsysteem mag worden opgevraagd. Als gegevens zich eenmaal in het opvragende systeem bevinden, geldt de autorisatie die binnen dat systeem is ingericht. Alleen voor de zorgtoepassing Ketenzorg is afgesproken dat de landelijke autorisatierichtlijn ook intern in de (raadplegende) applicatie toegepast moet worden.

Infrastructuur

Systemen die gebruik maken van de autorisatiefunctie van het LSP moeten zijn aangesloten op het LSP en daarmee voldoen aan de eisen voor een Goed Beheerd Zorgsysteem (GBZ). Daarnaast moet dit Goed Beheerd Zorgsysteem via een Goed Beheerd Zorgnetwerk (GZN) zijn aangesloten op het LSP.

3.3 Nuts

Nuts regelt autorisatie decentraal. In Nuts worden systemen geautoriseerd om op het netwerk aan te sluiten. Systemen die aangesloten zijn op het Nuts-netwerk en een use case ondersteunen kunnen gegevens uitwisselen over het Nuts-netwerk. Nuts zorgt ervoor dat systemen elkaar vertrouwen en dat bij een aanvraag voor gegevens een geverifieerde set aan gegevens wordt meegegeven die het systeem van de dossierhouder kan gebruiken om te bepalen of toegang wordt gegeven.

Tabel 2 Samenvatting autorisatie Nuts

Organisatie	Nuts is een volledig gedistribueerd netwerk. Er is geen centrale partij, ook niet voor de invulling van de generieke functies. Deelnemende leveranciers tekenen een deelnemersovereenkomst met Stichting Nuts voor ze aansluiten op het Nuts-netwerk.
Proces	Nuts autoriseert systemen. Dit concept kan op allerlei processen worden toegepast. Op dit moment is alleen eOverdracht in gebruik.
Informatie	Bij een aanvraag van gegevens worden er gegevens van de aanvrager (in Nuts termen credentials) meegestuurd. Dit betreft onder andere organisatiekenmerken en persoonsinformatie over de aanvragende gebruiker. Aan de hand van deze gegevens kan de dossierhouder controleren aan wie gegevens beschikbaar gesteld worden.
Applicatie	Autorisaties voor specifieke gebruikers zit in de systemen, dit valt buiten de scope van Nuts. Nuts levert credentials waarop een de dossierhouder kan checken of er voldoende vertrouwen is om toegang te geven tot gegevens.
Infrastructuur	Beveiligde verbindingen over het internet (op cryptografische basis).

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 Stichting Nuts, voor ze aansluiten op het Nuts-netwerk. Verder zijn er geen testen verplicht en moet de leveranciers zelf een risico-inschatting maken welke tests er nodig zijn. Het risico op een beveiligingsincident ligt namelijk bij de bron houdende leverancier.[3]

[3] https://nuts.nl/q-and-a/

Proces
De Nuts infrastructuur is in principe use case agnostisch, en wordt momenteel ten behoeve van eOverdracht gebruikt.

Het proces van autoriseren verloopt als volgt:

- Om te controleren of gegevens opgehaald en ingezien mogen worden moet het bronsysteem de volgende zaken kunnen controleren:
    - Welk opvragend systeem maakt verbinding?
    - Treedt het opvragende systeem op als verwerker optreedt voor de opvragende zorgaanbieder?
    - Welke zorgverlener vraagt de gegevens op?
    - Is deze zorgverlener werkzaam voor de opvragende zorgaanbieder?

  Om de beveiliging goed te kunnen waarborgen dient ieder van deze aspecten met een cryptografisch handtekening gecontroleerd te kunnen worden. Indien gewenst kan deze set met extra attributen worden uitgebreid.
  Deze attributen met bijbehorende cryptografische handtekening worden in zogenaamde credentials vastgelegd en meegegeven aan het bronsysteem zodat het bronsysteem kan controleren of de opvraging is toegestaan.

Informatie
Als een zorgverlener gegevens wil opvragen gaat er een bericht naar het systeem van de dossierhouder. In dit bericht wordt er informatie van de aanvrager meegestuurd (hiervoor bestaat geen standaard). Zorginstellingen zijn ervoor verantwoordelijk dat ze bijhouden wie hun medewerkers zijn en dat het dus hun eigen medewerkers zijn die gegevens opvragen. Er worden organisatiekenmerken en een grondslag meegestuurd. De credentials volgen Internationale standaarden, namelijk de W3C Verifiable Credentials.
Daarnaast maakt Nuts gebruik van OAuth 2.0.

Applicatie
Nuts gaat ervan uit dat de autorisaties van de individuele zorgverleners in de XIS-en correct geregeld is. Dit vormt namelijk de basis voor het uitgeven van een authorization token.

Als het systeem geautoriseerd is voor de betreffende use case komen de opgevraagde gegevens vervolgens beschikbaar in het XIS van de aanvrager. Of een specifieke medewerker toegang heeft tot de gegevens wordt in het XIS zelf geregeld.

Infrastructuur
Beveiligde verbindingen over het internet (op cryptografische basis).

3.4 XDS

XDS is een IHE-profiel dat gebruikt kan worden om gegevens tussen zorginstellingen uit te wisselen. Naast XDS zijn er meer profielen die hiervoor gebruikt kunnen worden zoals bijvoorbeeld XDR, XDM en XCA. Voor al deze IHE-profielen geldt dat deze gebruik maken van andere IHE-profielen voor onder andere authenticatie en autorisatie.

De verschillende IHE-profielen voor authenticatie en autorisatie zijn ontworpen met de gedachte dat deze in principe voor alle mogelijke authenticatie en autorisatie scenario's op landelijk, regionaal en organisatieniveau toepasbaar zouden moeten zijn. Het is daarom ook niet mogelijk om dit generiek te beschrijven aan de hand van het Nictiz lagenmodel. De specifieke invulling van de verschillende lagen zijn volledig afhankelijk van keuzes die binnen een land, regio of organisatie worden gemaakt bij de daadwerkelijke implementatie. We beschrijven geen specifieke XDS implementaties, omdat dit waarschijnlijk een onvolledig en onjuist beeld geeft van de mogelijkheden die de verschillende IHE-profielen bieden voor autorisatie.

Een aantal relevante aspecten van de verschillende IHE-profielen die gebruikt kunnen worden voor autorisatie worden toegelicht.

Zoals hiervoor aangegeven zijn de verschillende IHE-profielen ontworpen zodat ze ook complexe omgevingen kunnen ondersteunen. Daarbij worden scenario's ondersteund met centrale- en gedistribueerde authenticatiemechanismen, maar ook niet zorgspecifieke authenticatiemechanismen om bijvoorbeeld ook patiënten toegang te geven. Meer specifiek voor autorisatie worden ook meerdere autorisatiemodellen ondersteund, waaronder RBAC (Role-Based Access Control) voor rolgebaseerde autorisatie, maar ook modellen die rekening houden met de expliciete toestemming van de patiënt of een bepaalde grondslag voor gebruik of autorisatie op systeemniveau.

Belangrijke profielen en standaarden die hierin een rol spelen zijn de volgende:

- ATNA (Audit Trail and Node Authentication)
  ATNA zorg onder andere voor een volledige audit log van alle raadplegingen.
- XUA (Cross Enterprise User Assertion)
  XUA biedt de benodigde functionaliteiten om de identiteit van een geauthentiseerde gebruiker, applicatie of systeem te gebruiken bij het opvragen van gegevens bij een andere zorgaanbieder.
- IUA (Internet User Authorization)Onder andere ondersteuning voor OAuth 2.1 en JWT (JSON Web Token) tokens. Dit is een aanvulling op het XUA profiel en is vooral bedoeld voor gebruik in HTTP RESTful transacties.

3.5 Whitebox

Met Whitebox worden gegevens direct, één-op-één uitgewisseld met een andere bekende zorgaanbieder. Whitebox werkt op basis van beveiligde web technologie. In de Whitebox software wordt alle functionaliteit geïmplementeerd die de huisarts nodig heeft om met de belangrijkste partijen te communiceren.

Tabel 3 Samenvatting autorisatie Whitebox

Organisatie	Whitebox systems combineert lokalisatie, adressering en autorisatie in een push autorisatie model.
Proces	De ontvanger (en alleen de ontvanger) ontvangt een beveiligde link, waarmee die toegang krijgt tot gegevens.
Informatie	Op dit moment wordt alleen de professionele samenvatting of een subset ervan (b.v. medicatie overzicht) voor niet huisartsen ondersteund.
Applicatie	Implementatie van push-autorisatie in de Whitebox applicatie; deze applicatie is gekoppeld met het HIS.
Infrastructuur	Het systeem is decentraal, zonder externe opslag van gegevens.

Organisatie
Whitebox systems combineert lokalisatie, adressering en autorisatie in een push autorisatie model[4]. Conform WGBO mag de huisarts zonder expliciete toestemming gegevens delen met zijn vervanger. De vervanger mag (als waarnemer van de eigen huisarts) in spoedsituaties gegevens delen met een andere huisartsenpost, of met de Spoedeisende Hulp (SEH). In dit geval kan de SEH bellen naar de vervanger of huisarts om de sleutel (URL/autorisatiecode) op te vragen. De Whitebox controleert alle verzoeken om informatie en legt dit vast in een logbestand.

Proces
Het proces ziet er als volgt uit:

- Een HIS meldt de patiënt aan bij Whitebox (die acteert als een autorisatie-server).
- Na aanmelding wordt een unieke, patiëntspecifieke URL gemaakt naar de ontvanger met informatie over adressering (incl. type document), lokalisatie (waar de informatie te vinden is) en autorisatie (van de ontvanger om de gegevens te raadplegen).

[4] Push autorisatie is een standaard (set van protocollen) die door stichting Decozo wordt beheerd.

- De ontvanger kan met de URL en UZI-pas of een ander middel voor identificatie en authenticatie middels 2FA de gegevens ophalen.
- Deze autorisatie kan ook gebruikt worden om een nieuwe autorisatie aan te vragen en deze door te sturen naar de volgende zorgverlener in de keten (‘door-autoriseren’).

Informatie
Whitebox kan de professionele samenvatting, gebaseerd op de NHG-richtlijnen, uitwisselen, of een subset daarvan (medicatieoverzicht) afhankelijk van rolcode. De huisarts heeft de mogelijkheid om een langere of kortere periode (mini-PS) van het dossier te delen.

Applicatie
De Whitebox wordt gehost op een klein wit fysiek kastje op de huisartsenpraktijk. . Er wordt ook aan een (open source) versie van de Whitebox gewerkt die door de HIS leverancier gehost kan worden.

Infrastructuur
Voor adresseren maakt Whitebox gebruik van public key infrastructuren (PKI’s) zoals UZI, PKIoverheid, web/https-CA’s. Het systeem werkt decentraal en slaat geen gegevens op in externe bronnen.

3.6 Conclusie huidige oplossingen

De oplossingen in de huidige situatie voldoen niet volledig aan de functionele behoeften, zoals beschreven in paragraaf 2.2. De belangrijkste oorzaken hiervan zijn:

- De dossierhouder van de informatie is verantwoordelijk voor wat er verstrekt wordt. Dit terwijl de raadpleger weet wat hij nodig heeft. De wettelijke regels, WGBO, zijn van toepassing op de dossierhouder. Met de manier waarop nu invulling gegeven wordt aan de wetgeving kan er niet volledig voldaan worden aan de functionele behoeften.
- De huidige oplossingen bieden niet voldoende flexibiliteit. Tijdens de interviews zijn verschillende voorbeelden naar voren gekomen waaruit het gebrek aan flexibiliteit en de noodzaak daarvan blijkt. Hieronder twee voorbeelden uit de interviews:
    - Ketenzorg: de autorisatie is heel fijnmazig en specifiek gemaakt voor de opvrager (bijvoorbeeld omdat een diëtist alleen een beperkte set gegevens mag opvragen). Gevolg: er zijn 14 verschillende datasets gedefinieerd. Het opvragende systeem dwingt af dat de landelijke autorisatierichtlijn intern wordt toegepast. De systemen worden hierop gekwalificeerd. Het probleem bij ketenzorg is dat de autorisatie voor bijvoorbeeld een diëtist in de context van diabetes anders is dan voor ouderenzorg. Daarnaast kunnen autorisatierichtlijnen wijzigen. Deze wijzigingen in alle XIS'en doorvoeren kost veel tijd.
    - In een crisissituatie is het noodzaak dat autorisaties snel aangepast kunnen worden. Een voorbeeld hiervan is COVID-19: verpleegkundigen in het ziekenhuis hebben in principe geen toegang tot vaccinatiegegevens, maar tijdens de COVID-19 periode moesten zij hier wel over kunnen beschikken, omdat zij zelf moesten vaccineren. Dit soort wijzigingen moeten snel doorgevoerd kunnen worden.

- Autoriseren op basis van rolcodes biedt niet de gewenste zekerheid, hiermee kan niet alles gecontroleerd worden. Denk bijvoorbeeld aan de controle of er een behandelrelatie is met een patiënt. Dat is een controle die alleen door het opvragende systeem gedaan kan worden en dus niet bij de dossierhouder. Daarnaast vinden sommige uitwisselingen op systeemniveau plaats, zoals eOverdracht. Een deel van de gegevens is van belang voor de administratieve medewerkers (ZIB Patiënt, etc.) terwijl de overige gegevens alleen door verpleegkundigen of specialisten ingezien mogen worden. Ook dat kun je alleen in het systeem van de ontvanger regelen.
- Het ontbreekt aan een gemeenschappelijk vertrouwensmodel. Een vertrouwensmodel bevat alle overstijgende afspraken om het vertrouwen in uitwisseling van medische gegevens en de vertrouwelijkheid van het medisch dossier te borgen. Het gaat om technische, organisatorische en juridische afspraken waarmee de vertrouwensbasis tussen zorgaanbieders gelegd wordt. Het gebrek aan een gemeenschappelijk model leidt ertoe dat bij elke gegevensuitwisseling steeds opnieuw afspraken gemaakt moeten worden over dezelfde onderwerpen, met vertraging in de realisatie van een oplossing tot gevolg. Daarnaast zijn er voor verschillende uitwisselsystemen verschillende vertrouwensmodellen: zo hebben leveranciers vertrouwensmodellen, maar ook partijen als Nuts en VZVZ. Wanneer zorgaanbieders van systemen met een eigen vertrouwensmodel willen koppelen met zorgaanbieders met een systeem met een ander vertrouwensmodel, kan dit niet zomaar gerealiseerd worden. Er kunnen bijvoorbeeld verschillen zitten in beveiligingseisen die gesteld worden. Dit leidt ertoe dat partijen niet met elkaar communiceren uit angst dat een beveiligingsincident of datalek bij één van de communicerende partijen verregaande consequenties heeft voor de overige communicerende partijen.

In hoofdstuk 5 wordt de oplossingsrichting voor de SOLL-situatie beschreven.

4 TOETSINGSKADER

De sector overstijgende SOLL-situatie die in hoofdstuk 5 beschreven wordt, wordt naast een toetsingskader gelegd. 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 een landelijk dekkend netwerk van infrastructuren voor gegevensuitwisseling in de zorg (D&A Medical Group, 2022). De functionele behoeften uit het toetsingskader zijn voor deze beoordeling vervangen door de functionele behoeften die voort zijn gekomen uit de werksessies zoals beschreven in hoofdstuk 2.

In dit hoofdstuk lichten we toe hoe het toetsingskader is toegepast in het beschrijven van de SOLL-situatie voor autoriseren. Zoals in hoofdstuk 3 beschreven, is de oplossing voor autoriseren geen systeem dat getoetst kan worden aan het toetsingskader. De SOLL-situatie zal ingevuld worden door afspraken op organisatie en procesniveau. Hoe dit eruit ziet wordt onder paragraaf 5.1 beschreven. In paragraaf 5.2 wordt beschreven wat aandachtspunten zijn in de uitwerking van de SOLL-situatie. Deze aandachtspunten komen voort uit de leidende principes uit het toetsingskader.

Voor de leidende principes is vastgesteld welke relevant zijn in relatie tot autoriseren. De reden om een principe niet mee te nemen kan bijvoorbeeld zijn dat het buiten scope van de definitie van autoriseren valt of niet van toepassing is op de functie autoriseren. In bijlage 7.2 is bij het principe aangegeven als dit het geval is. Voor de principes die toegepast kunnen worden op de SOLL-situatie voor autoriseren wordt beschreven in hoeverre deze ingevuld kan worden in de SOLL-situatie. Daarnaast worden ook de onderdelen met betrekking tot haalbaarheid en draagvlak beschreven.

De onderdelen uit het toetsingskader zijn als op de SOLL-situatie toegepast:

- *Voor de functionele behoeften*
  De vraag die bij de functionele behoeften gesteld is: Is het mogelijk om de functionele behoefte met betrekking tot autoriseren te realiseren? Zo ja, op welke manier?

- *Voor de leidende principes*
  Is het mogelijk om invulling te geven aan het principe?
  - Ja: op welke manier?
  - Nee: dit is niet mogelijk.

- *Voor haalbaarheid*
  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 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 OPLOSSINGSRICHTING

Tijdens de werksessies met de experts was er consensus dat voor reguliere zorg er geen behoefte is aan een aparte, extra autorisatiefunctie, in de vorm van een systeemoplossing. Dit kwam ook in de interviews naar voren. De belangrijkste reden hiervoor is dat de gewenste flexibiliteit met een centrale autorisatiefunctie moeilijker te realiseren is, dan wanneer de verantwoordelijkheid bij de bron wordt gelegd. De bevoegdheden van zorgverleners zijn namelijk reeds vastgelegd in hun primaire zorgsysteem (HIS, ECD, EPD). Daar zou men op moeten kunnen vertrouwen. Daarnaast kunnen zorgverleners in verschillende organisaties een andere rol/functie hebben of zelfs binnen een organisatie op verschillende momenten. Hun bevoegdheden zijn gekoppeld aan die rol/functie. Dit leidt wel tot een aantal randvoorwaarden waar de SOLL-situatie aan moet voldoen:

1. Het vertrouwen moet geborgd worden in aansluitvoorwaarden voor zorgorganisaties en systemen. Zo moet elke zorgorganisatie over een autorisatiematrix beschikken, die correct geïmplementeerd is.
2. De autorisatiefunctie moet voldoende flexibiliteit bieden, zodat er om gegaan kan worden met de verschillende rollen en functies die zorgverleners kunnen hebben en de verschillende bevoegdheden die daaraan gekoppeld zijn. De ontwikkeling van netwerkzorg zal steeds meer flexibiliteit vragen.

In paragraaf 5.1 wordt de richting voor de SOLL-situatie op hoofdlijnen beschreven. De verdere gedetailleerde uitwerking kent veel consequenties. Om deze goed te overzien en een keuze voor de specifieke invulling te maken is het van belang om dit in detail uit te werken. Dit gebeurt binnen het programma Janus. In paragraaf 5.2 worden, op basis van het toetsingskader en de expertsessies, aandachtspunten voor de nadere uitwerking beschreven.

5.1 Beschrijving SOLL-situatie

5.1.1 Kaders

Tijdens de expertsessies en interviews zijn een aantal kaders naar voren gekomen. De beschrijving van de SOLL-situatie is tot stand gekomen op basis van deze kaders. Het gaat enerzijds om het definiëren van stappen in de autorisatie bij gegevensuitwisseling en anderzijds om kenmerken voor een oplossingsrichting.

In de SOLL-situatie wordt er onderscheid gemaakt tussen twee stappen in autorisatie, die beide nodig zijn wanneer er gegevens tussen zorginstellingen uitgewisseld worden. Deze twee stappen van autorisatie zijn:

1. De autorisatie om gegevens op te mogen vragen/te mogen raadplegen tussen zorginstellingen.
2. De autorisatie van zorgverleners binnen een zorginstelling, op het moment dat gegevens beschikbaar zijn.

Naast dat er invulling moet worden gegeven aan beide niveaus van autorisatie zijn er een aantal kenmerken waaraan een autorisatie-oplossing moet voldoen. Onderstaande kenmerken zijn in de expertsessies naar voren gekomen:

1. De oplossing is gebaseerd op vertrouwen[5] tussen de raadpleger en de dossierhouder. De raadpleger weet immers beter wat hij nodig heeft dan de dossierhouder.
2. Het delen van informatie tussen zorgverleners is gebaseerd op een grondslag[6] voor gegevensuitwisseling.
3. De oplossing biedt voldoende flexibiliteit, in verband met verschillende rollen, wijzigingen daarin, veranderende richtlijnen, etc. De huidige oplossingen zijn te rigide en bieden niet de benodigde flexibiliteit.
4. De oplossing gaat uit van afspraken en normen, niet van een systeemoplossing.
5. De oplossing autoriseert tussen zorginstellingen op zorgaanbiedertype.

5.1.2 Beschrijving oplossingsrichting

De oplossingsrichting gaat uit van de stappen en kenmerken die onder 5.1.1 beschreven zijn. Hieronder wordt op hoofdlijnen de invulling op de Nictiz lagen beschreven. In de SOLL-situatie beperkt zich dit tot de bovenste drie lagen, omdat er gekozen is om niet voor een systeemoplossing te kiezen.

Tabel 4 Samenvatting oplossingsrichting voor autorisatie

Organisatie	Landelijke afspraken voor vertrouwen uitgaande van autorisatie in twee stappen: 1. Autoriseren van de zorgaanbieder 2. Autoriseren van zorgverleners bij de zorgaanbieder.
Proces	Het proces voor autoriseren is use case onafhankelijk. Het vindt altijd plaats in dezelfde twee stappen.
Informatie	Het zorgaanbiedertype wordt gekoppeld aan een gegevensuitwisseling. Er wordt gebruikt gemaakt van internationale standaarden zoals OAuth 2 en XUA.
Applicatie	*Niet van toepassing*

[5] Complexiteit in de huidige wet- en regelgeving zorgt voor onduidelijkheid bij zorgverleners en patiënten over wanneer wat en met wie gegevens uitgewisseld mag worden (VWS, 2023).
[6] Een beperking hierbij is dat de grondslagen niet voldoen aan de wensen en behoeften van zorgverleners ten aanzien van beschikbaarheid van actuele informatie (VWS, 2023).

Infrastructuur	*Niet van toepassing*

Organisatie

Er is meer vrijheid bij de raadpleger nodig dan nu het geval is, omdat de raadpleger weet welke informatie hij op welk moment nodig heeft. Aangezien de dossierhouder ervoor verantwoordelijk is dat gegevens alleen gedeeld worden met een zorgverlener die bevoegd is om de gegevens in te zien, moet de oplossing voldoende bescherming aan de dossierhouder bieden. Hiervoor is vertrouwen nodig. Om dit vertrouwen te borgen moeten er landelijk afspraken gemaakt worden waar elke zorgaanbieder aan moet voldoen om gegevens uit te kunnen wisselen. Alle overstijgende afspraken om het vertrouwen in uitwisseling van medische gegevens te borgen worden vastgelegd in een vertrouwensmodel. Het gaat om technische, organisatorische en juridische afspraken om de vertrouwensbasis tussen zorgaanbieders te leggen. Het vertrouwensmodel is erop gericht om de vertrouwelijkheid van het medisch dossier te borgen (Twiin, 2021).
Aansluitend hierop worden aansluitvoorwaarden voor zorgorganisaties en systemen opgesteld. Zo kan afgesproken worden dat elke zorgorganisatie over een correct geïmplementeerde autorisatiematrix beschikt. Het voldoen aan de aansluitvoorwaarden en overige afspraken kan worden vastgelegd in een convenant.
Wanneer er gesproken wordt over de dossierhouder, dan hoeft dit niet enkel een zorgaanbieder te zijn. Een dataplatform kan bijvoorbeeld in deze context ook de rol van dossierhouder vervullen.

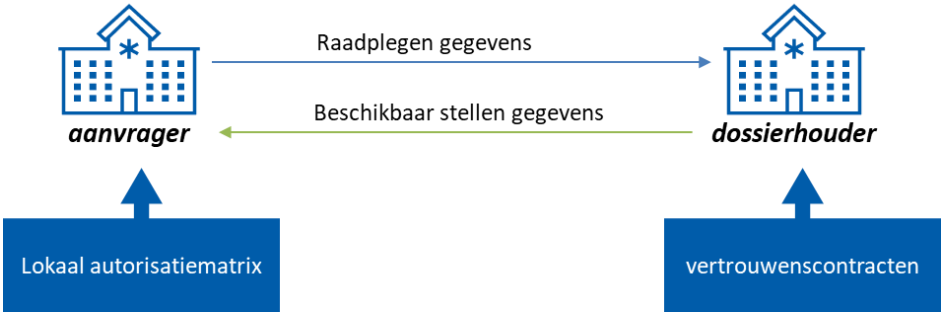
Zoals eerder gedefinieerd vindt autorisatie in twee stappen plaats. Voor invulling van beide stappen zijn afspraken nodig:

1. **Autoriseren van een zorgaanbieder om gegevens op te vragen bij een dossierhouder.**
   Een zorgaanbieder kan bijvoorbeeld een ziekenhuis of GGZ-instelling zijn, maar het kunnen ook individuele zorgverleners zijn, zoals een huisarts of diëtist met een eigen praktijk. Hiervoor moet worden vastgesteld welk zorgaanbiedertype welke gegevens mag opvragen. Dit kan gerelateerd worden aan een gegevensset, bijvoorbeeld door het te koppelen aan een informatiestandaard. Er moet ook vastgesteld worden welk type zorgaanbieder het is. Dit zou bijvoorbeeld kunnen op basis van de WTZa-toelating.

2. **Het autoriseren van zorgverleners binnen de zorgorganisatie**.
   De invulling van deze stap kan door afspraken vast te stellen waaraan een zorgorganisatie moet voldoen. Deze afspraken kunnen gaan over een autorisatiematrix en de naleving ervan. Maar ook over het inrichten van een ‘break the glass’ procedure. Als zorgverleners gegevens willen inzien, waarvoor zij niet bevoegd zijn, moeten zij een reden opgeven en wordt dit gelogd. Een ander onderdeel kan het inrichten van een audittrail zijn. Dit zijn afspraken die allemaal opgenomen zouden kunnen worden in een norm voor de zorgaanbieder. Een voorbeeld van een best practice is het OLVG, zij hebben een autorisatiematrix en procedures voor naleving ingericht. Deze best practice is opgenomen in bijlage 7.4.

Proces

Het uitgangspunt bij de SOLL is dat autorisatie het proces van de zorgverlener volgt, dus dat hij op het juiste moment over de juiste informatie kan beschikken. Hoe autoriseren plaatsvindt is in principe use case onafhankelijk. Het vindt altijd plaats in dezelfde twee stappen. Figuur 2 geeft een versimpelde weergave van de stappen die in de SOLL-situatie doorlopen worden om te autoriseren:



Figuur 3 versimpelde weergave van het proces van autorisatie

Het start bij een zorgverlener, werkzaam bij een zorgaanbieder, die gegevens wil raadplegen. De vraag om gegevens komt vervolgens bij de dossierhouder. Daar is bekend of de zorgaanbieder voldoet aan de landelijk gemaakte afspraken (op basis van het afgesloten convenant). Vervolgens wordt door de dossierhouder gecontroleerd of de zorgaanbieder, waar de zorgverlener werkt conform de landelijk gemaakte afspraken bevoegd is om de gevraagde gegevens te raadplegen. Ook controleert de dossierhouder of de aanvragende zorgverlener voldoet aan één of meerdere grondslagen voor gegevensuitwisseling. Als dit het geval is, dan worden de gegevens beschikbaar gesteld aan de zorgorganisatie van de aanvrager (pull). De zorgaanbieder heeft intern geregeld dat alleen de zorgverleners, die geautoriseerd zijn op basis van hun functie en behandelrelatie, bij de gegevens kunnen. Dit is vastgelegd in de lokale autorisatiematrix.

Deze oplossing kan ook werken in de situatie dat er informatie gepusht wordt naar een andere zorgaanbieder. In dat geval is er een vertrouwensbasis tussen de dossierhouder en de ontvangende zorgaanbieder. De dossierhouder kan ervan uitgaan dat de ontvangende zorgaanbieder voldoet aan de afspraken en beschikt over een juist geïmplementeerde autorisatiematrix. Hiermee kunnen alleen bevoegde zorgverleners bij de verzonden informatie.

De controle op autorisaties vindt in deze situatie decentraal plaats. Er is geen centrale voorziening.

De SOLL-situatie is een use case onafhankelijke inrichting van autorisatie. Het proces van autoriseren kan er in verschillende use cases wel anders uitzien. Bij het opvragen van gegevens gaat het in de twee stappen zoals hiervoor beschreven. Wanneer gegevens naar een zorgaanbieder verstuurd worden, is alleen de tweede stap van autoriseren van toepassing. De zorgaanbieder is namelijk al geautoriseerd om de gegevens te ontvangen.

Informatie

In deze SOLL-situatie wordt het autoriseren van een zorgaanbieder gekoppeld aan een gegevensuitwisseling. Dit kan op verschillende niveaus: van zib tot een dataset of bijvoorbeeld gekoppeld aan een informatiestandaard. Daarnaast is elke gegevensuitwisseling gebaseerd op één

of meerdere grondslagen. De grondslagen van de gegevensuitwisseling moeten bekend zijn bij de dossierhouder. Hoe dit kan werken vraagt nadere uitwerking. Deze specificaties kunnen op verschillende manieren vastgelegd worden. Voorbeelden waarin dit nader kan worden uitgewerkt zijn een richtlijn voor een specifieke informatie-uitwisseling of een informatiestandaard waarin staat beschreven welke gegevens door welk type zorgaanbieder opgevraagd mogen worden.
In de SOLL-situatie wordt gebruik gemaakt van internationale standaarden voor autorisatie zoals OAuth 2 en/of XUA.

5.2 Aandachtspunten voor de verdere uitwerking

De SOLL-situatie zoals beschreven onder 5.1 geeft een richting voor een oplossing. De verdere uitwerking van de oplossing vraagt een nadere analyse en valt buiten de scope van dit onderzoek. Elke keuze die in de uitwerking gemaakt wordt, kan grote consequenties hebben voor de implementatie. In de uitwerking zijn er een aantal aspecten die extra aandacht verdienen. Het toetsingskader kan hierbij als leidraad gebruikt worden. Deze aandachtspunten worden in deze paragraaf beschreven.

5.2.1 Toepassing van het toetsingskader

In bijlage 7.2 is beschreven welke principes uit het toetsingskader kunnen worden toegepast in de uitwerking van de SOLL-situatie. Deze worden hieronder uitgewerkt.

De oplossing is duurzaam (P2)

Een oplossing voor autoriseren kan op een duurzame manier ingericht worden. Dit betekent dat de oplossing voldoende flexibiliteit biedt en toekomstbestendig is. Flexibiliteit houdt in dat er niet per use case nieuwe afspraken nodig zijn. Daarnaast is een oplossing duurzaam als een wijziging, bijvoorbeeld in een richtlijn, tot zo min mogelijk aanpassingen leidt. Dit kan gerealiseerd worden door wat centraal geregeld wordt te beperken en meer aan zorgaanbieders zelf over te laten. In de rollen en functies van medewerkers kunnen wijzigingen plaatsvinden. Bijvoorbeeld tijdens COVID-19: verpleegkundigen in het ziekenhuis hebben in principe geen toegang tot vaccinatiegegevens, maar tijdens de COVID-19 periode moesten zij hier wel over beschikken, omdat zij zelf moesten vaccineren. Dit soort wijzigingen moeten snel doorgevoerd kunnen worden.

De oplossing is federatief (P3)

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). Door de afhankelijkheid van centrale partijen te beperken kan de oplossing eenvoudiger federatief tot stand komen. Elke zorgaanbieder is verantwoordelijk dat er voldaan wordt aan de (nog te maken) landelijke afspraken.

Afspraken (P6 t/m P8)

Afspraken zijn in de SOLL-situatie heel belangrijk. Deze afspraken gaan over hoe elke zorgaanbieder, met zijn XIS-leverancier, autorisatie regelt.

Er is een gelijk speelveld voor alle leveranciers (P15)

Dit betekent dat er afspraken worden gemaakt over het gebruik van standaarden en niet over het gebruik van een product of dienst. Door normen te stellen die voor elke zorgaanbieder gelden is het speelveld gelijk; iedereen moet eraan voldoen. Er is geen centraal systeem waarbij het verplicht is om aan te sluiten.
Om hier eenduidigheid in te bereiken kan worden aangesloten op internationale standaarden voor autorisatie. Mogelijkheden hiervoor zijn:

- OAuth 2.0: OAuth 2.0 is een API Autorisatiestandaard. Met deze standaard kunnen gebruikers toegang krijgen tot specifieke gegevens in een ander systeem, zonder dat ze hiervoor hun authenticatiegegevens hoeven te overhandigen aan een ander systeem[7]. Onder andere MedMij en Nuts maken gebruik van de OAuth 2.0 standaard.
- XUA: XUA biedt de benodigde functionaliteiten om de identiteit van een geauthentiseerde gebruiker, applicatie of systeem te gebruiken bij het opvragen van gegevens bij een andere zorgaanbieder

Privacy en security (P16 t/m 18)

Privacy by design is een belangrijk uitgangspunt bij het realiseren van autorisatie. Als autorisatie goed geregeld wordt, wordt er voor een groot deel voldaan aan de acht 'privacy by design strategies', die beschreven staan onder P16 in het toetsingskader. Met goede afspraken en normen voor autorisatie en de naleving ervan is 'privacy by design' ook geborgd.
Wat betreft 'security by design' worden drie van de zes STRIDE-categorieën in de SOLL-situatie geborgd. Namelijk, repudiation, denial of service en elevation of privilege. Repudiation gaat over het loggen van alle acties die plaatsvinden. De afspraken rondom logging kunnen onderdeel zijn van de normering. Denial of service is hier niet van toepassing, dat gaat over beschikbaarheid van systemen. Deze oplossingsrichting bestaat uit landelijke afspraken die decentraal worden geïmplementeerd. De functie op zichzelf kan, als gevolg hiervan, niet uitvallen. Elevation of privilege betreft het inzien van informatie waarvoor geen autorisatie bestaat. Dit wordt opgelost door het maken van afspraken. De overige drie STRIDE-categorieën zijn niet van toepassing. De STRIDE-categorieën worden beschreven onder P18 in het toetsingskader.

Haalbaarheid

Wij verwachten dat dit een haalbare oplossingsrichting is. De impact op de realisatietermijn komt voort uit de benodigde discussies over de te maken afspraken en uit te werken details van de SOLL-situatie. Het voordeel van de voorgestelde oplossingsrichting is dat het technisch realiseerbaar is en optimaal gebruik maakt van de bestaande systemen. Deze systemen zullen wel moeten gaan voldoen aan de nog te maken normen. De impact daarvan is nu nog niet in te schatten.

Tabel 5 Haalbaarheid voorgestelde oplossingsrichting

H1	**Technisch realiseerbaar** Ja, dit scenario kan met bestaande technologieën worden gerealiseerd.
H2	**Gebruik bestaande oplossingen** Ja, er wordt volledig gebruik gemaakt van bestaande oplossingen, deze zullen wel moeten gaan voldoen aan de normen.
H3	**Impact** Gemiddeld, er wordt gebruik gemaakt van bestaande oplossingen, maar het tot stand komen van afspraken is complex en zal bepalend zijn voor de realisatietermijn.
H4	**Draagvlak bij de leverancier** Hoog, alle leveranciers kunnen met hun eigen oplossing continueren.

[7] https://www.forumstandaardisatie.nl/open-standaarden/oauth

H5	**Maatschappelijk en politiek draagvlak** Hoog, er zijn geen maatschappelijke of politieke bezwaren.

5.2.2 Overige aandachtspunten

Bij het verder invullen van de oplossingsrichting is het van belang om goed te monitoren dat de oplossing past binnen wet- en regelgeving, zowel op Europees als nationaal niveau. In de EHDS zijn ook kaders voor autorisatie opgenomen, maar hoe deze geïmplementeerd worden is nog onduidelijk (zie hoofdstuk 3). Bij de concretisering van de SOLL-oplossing is het dus relevant om deze ontwikkeling te blijven volgen.

Bij de uitwerking van de oplossingsrichting adviseren wij om te focussen op een oplossing waarmee het grootste deel van autorisatie ingevuld kan worden. Er zijn altijd situaties denkbaar waarin de oplossing niet passend is. Dit is echter een klein deel. Voor het deel van de populatie of use cases waar deze oplossingsrichting geen oplossing biedt kan aanvullend naar een oplossing gezocht worden. Een voorbeeld van een aanvulling op de voorgestelde SOLL-oplossingsrichting is het push autorisatie model. Push autorisatie betreft een specifieke toepassing van de decentrale implementatie van de generieke functies lokalisatie, adressering en autorisatie. Onder de WGBO biedt push zorgverleners de mogelijkheid om relevante gegevens van de patiënt te delen onder het principe “doorautoriseren“.

5.2.3 Kosten en baten

De baten die met de beschreven oplossing gerealiseerd kunnen worden zijn afhankelijk van de verdere uitwerking hiervan. De belangrijkste baat rondom autoriseren is het realiseren van meer flexibiliteit, passend binnen wet- en regelgeving.
De kosten die gemaakt moeten worden zijn eveneens afhankelijk van de verdere uitwerking. Kosten hangen bijvoorbeeld samen met de aanpassingen die nodig zullen zijn aan de systemen, hoe afspraken tot stand gaan komen en hoe deze vervolgens gehandhaafd gaan worden. Hiermee is het niet mogelijk om nu een inschatting van de verwachtte kosten te geven.

6 ADVIES

Zoals eerder beschreven zitten er nog haken en ogen aan de SOLL-situatie en is er een diepgaande analyse nodig hoe de geschetste SOLL-situatie verder ingevuld kan worden en wat de mogelijke impact van te maken keuzes is. In algemene zin moet de afweging gemaakt worden wat er passend is binnen wet- en regelgeving. Het is zoeken naar de juiste balans tussen voldoende vrijheid bij de raadpleger en voldoende bescherming bij de dossierhouder.

Hieronder staan een aantal onderwerpen waarover afspraken moeten worden gemaakt. Dit is een niet uitputtende lijst.

1. Geef invulling aan het autoriseren op zorgaanbiedertype:
   Om te kunnen autoriseren op zorgaanbiedertype zijn er landelijke afspraken nodig. Dit zijn afspraken die minimaal gaan over:
   a. Hoe vastgesteld wordt welk zorgaanbiedertype welke gegevens op mag vragen; dit kan gerelateerd worden aan een gegevensset, bijvoorbeeld door het te op te nemen in een richtlijn of informatiestandaard.
   b. Hoe vastgesteld wordt om welk type zorgaanbieder het gaat. Dit zou bijvoorbeeld kunnen op basis van de WTZa-toelating. De volledigheid hiervan moet nader onderzocht worden.
2. Geef invulling aan het normeren van autoriseren van zorgverleners bij een zorgaanbieder. Hierover moeten verschillende keuzes gemaakt worden die mogelijk impact hebben op individuele zorgaanbieders. De normering zou tot doel moeten hebben om te borgen dat zorgaanbieders intern hun autorisatie goed op orde hebben. Welke normering er specifiek nodig is en op welk niveau (bijvoorbeeld zorgaanbieder of leverancier) vraagt om verdere uitwerking.
3. Als is vastgesteld welke normering er nodig is, moet er ook invulling worden gegeven aan de handhaving. Handhaving op normen is nodig omdat de dossierhouder er op moet kunnen vertrouwen dat de raadpleger op de juiste manier met de verstrekte gegevens om gaat.
4. Stel vast hoe vertrouwen geborgd gaat worden en sluit hierbij aan op de ontwikkeling van het landelijk vertrouwensmodel (voorheen TwiinXNuts). Dit zou bijvoorbeeld kunnen in een (landelijk) convenant. Hierin worden afspraken opgenomen waar instellingen aan voldoen, voordat ze gegevens kunnen uitwisselen. Zorgaanbieders ondertekenen het convenant. Er moet een kader gesteld worden wanneer een zorgaanbieder te vertrouwen is. Dit kunnen bijvoorbeeld zorgaanbieders zijn die voldoen aan de normering en aansluitvoorwaarden en het convenant ondertekenen.
5. Kies voor het gebruik van internationale standaarden zoals OAuth 2 en XUA zodat er brede ondersteuning is door leveranciers.

7 BIJLAGEN

7.1 Afkortingen en begrippen

7.1.1 Afkortingenlijst

Afkorting	Definitie
AMvB	Algemene Maatregel van Bestuur
API	Application Programming Interface
ATNA	Audit Trail and Node Authentication
AVG	Algemene Verordening Gegevensbescherming
BSN	Burgerservicenummer
CDA	Clinical Document Architecture
DIZRA	Duurzaam Informatiestelsel in de Zorg Referentie Architectuur
ECD	Elektronisch Cliënten dossier
EHDS	European Health Data Space
EPD	Elektronisch Patiënten dossier
GBZ	Goed Beheerd Zorgsysteem
GDPR	General Data Protection Regulation
GGZ-instelling	Geestelijke Gezondheidszorg instelling
HAP	Huisartsenpost
IHE	Integrating the Healthcare Enterprise
ISO	International Organization for Standardization
IST	"Ist-Zustand" in het Duits, wat letterlijk betekent "huidige situatie"
IUA	Internet User Authorization
IZA	Integraal Zorgakkoord
KB	Koninklijk Besluit
LSP	Landelijk Schakelpunt
NEN	Stichting Koninklijk Nederlands Normalisatie Instituut
OID	Wereldwijde Unieke Object Identificatie
PGO	Persoonlijke gezondheidsomgeving
PKI	Public Key Infrastructure
RBAC	Role-based access control
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 Thuiszorginstelling
Wabvpz	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg

Wegiz	Wet elektronische gegevensuitwisseling in de zorg
WGBO	Wet geneeskundige behandelingsovereenkomst
XCA	Cross Community Access
XCPD	Cross-Community Patient Discovery
XDS	Cross-enterprise Document Sharing
XDR	Cross-Enterprise Document Reliable Interchange
XDM	Cross-Enterprise Document Media Interchange
XUA	Cross Enterprise User Assertion

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.
IHE – profiel	IHE-profielen zorgen voor integratiemogelijkheden die ontstaan door de gecoördineerde toepassing van communicatiestandaarden. Ze geven gedetailleerde richtlijnen over hoe deze standaarden kunnen worden geïmplementeerd om aan specifieke klinische vereisten te voldoen.
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 online toestemmingsvoorziening 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.

Begrip	Definitie
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 uitwissing van patiëntgegevens.
URA	Een uniek nummer dat een zorgaanbieder heeft voor elektronische communicatie van zorgdata.
XCA	Ondersteunt de middelen om patiëntrelevante medische gegevens van andere gemeenschappen op te vragen en op te halen.
XDS	Standaard voor het delen van medische documenten en beelden tussen samenwerkende zorginstellingen.
XIS	Ongedefinieerd elektronisch uitwisselsysteem.

7.2 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 Wabvpz 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 leverrealiseerbaarheid, realisatie- en implementatietermijn, organisatie en governance, politiek draagvlak.

Functionele behoeften

De functionele behoeften voor autoriseren zijn geformuleerd in hoofdstuk 2. Dit is als volgt beschreven:

Zorgverleners kunnen vanuit hun rol of functie, mits zij bevoegd zijn, op het juiste moment over de juiste informatie beschikken.

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 **functionele behoeften** van patiënten en zorgverleners. Niet getoetst: Zie 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)
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).
4.	De data **blijft bij de bron**, onder de verantwoordelijkheid van de dossierhouder, voor een veilig en vertrouwd informatiestelsel waarin het voor cliënten transparant is welke dossierhouders welke gezondheidsgegevens registreren en wie het raadpleegt. (DIZRA, 2020) Niet van toepassing op de SOLL-situatie: de SOLL-situatie staat los van de infrastructuur en in hoeverre die het mogelijk maakt om data zoveel mogelijk bij de bron te laten staan.
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). Niet van toepassing: de oplossing gaat specifiek over de generieke functie autoriseren.
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).
7.	Data is **machineleesbaar**, 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).
8.	In het informatiestelsel spreken we een **gemeenschappelijke taal** en hanteren

	gemeenschappelijke terminologie, waarbij we de contextuele verschillen omarmen (DIZRA, 2020).
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) Niet van toepassing: de zeggenschap die patiënten hebben over wie hun medische gegevens mogen inzien ligt in de generieke functie toestemmingen.
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). Data is beschikbaar voor alle betrokkenen in het zorgnetwerk van een persoon (Visie op het zorginformatiestelsel, 2022). Niet van toepassing: de beschikbaarheid van data volgt na autorisatie.
11.	Data worden digitaal, eenduidig en gestandaardiseerd geregistreerd in het zorgproces en beschikbaar gesteld voor diverse **secundaire doelen** (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 van toepassing: Voor autorisatie met betrekking tot secundaire doelen gelden zijn er andere functionele behoeften.
12.	Systemen zijn open (Integraal Zorgakkoord, 2022). Niet van toepassing: De zorgaanbieders moeten geautoriseerd worden om gegevens te raadplegen. Vervolgens zijn systemen open om ook daadwerkelijk gegevens te delen, maar dit is geen onderdeel van de functie autoriseren.
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). Niet van toepassing: Dit is een principe dat gesteld kan worden aan bronsystemen, het is niet onderscheidend voor de autorisatiefunctie.
14.	Data uit **verschillende bronnen kan gecombineerd** worden; zowel uit de bronsystemen van zorgverleners als data die een patiënt zelf verzamelt. Niet van toepassing: dit vraagt functionaliteit van de systemen.
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).
Wettelijke eisen	
16.	De functie voldoet aan **privacy by design** (AVG)
17.	De functie betracht **standaard maximale privacy** (privacy by default) (AVG).

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

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[8] 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 onderstaande toelichting uitgebreid.

   Een onomstreden uitwerking van het begrip duurzaamheid, in de vorm van ontwerpstrategieën of ontwerppatronen, 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)

[8] Zie https://dizra.gitbook.io/dizra/perspectieven/motivation/duurzaam

- 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 dossierhouder, voor een veilig en vertrouwd informatiestelsel waarin het voor cliënten transparant is welke dossierhouders welke gezondheidsgegevens registreren en wie het raadpleegt** (DIZRA, 2020)
   DIZRA definieert data bij de bron [9] als volgt: 'Data bij de bron betekent dat we gegevens 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.

[9] Zie: https://dizra.gitbook.io/dizra/perspectieven/motivation/data-bij-de-bron

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 [10]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.

7. **Data is machineleesbaar, 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 Machineleesbaar [11]is te vinden bij DIZRA.
   De definitie van- en nadere toelichting op het principe 'machineleesbaar' 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[12] 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.

[10] Zie https://dizra.gitbook.io/dizra/perspectieven/motivation/open-standaarden
[11] Zie: https://dizra.gitbook.io/dizra/perspectieven/motivation/machineleesbaar
[12] Zie: https://dizra.gitbook.io/dizra/perspectieven/motivation/gemeenschappelijke-taal

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-patiëntsamenvatting, labuitslagen, 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 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[13].

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.

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 [14] wordt door DIZRA als volgt gedefinieerd, waarbij zij de definitie van de Autoriteit Consument en Markt gebruiken: 'Een eerlijk speelveld 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

[13] Zie: https://www.meliushealthinformatics.nl/post/waarom-is-een-pgo-koppelen-moeilijker-dan-een-stopcontact-vervangen

[14] Zie: https://dizra.gitbook.io/dizra/perspectieven/motivation/gelijk-speelveld

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):

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. <u>Spoofing</u>
   Spoofing wil zeggen dat een component (fysiek of software) of een menselijke actor zich voordoet 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. <u>Tampering</u>
   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. <u>Repudiation</u>
   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. <u>Information Disclosure</u>
   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.

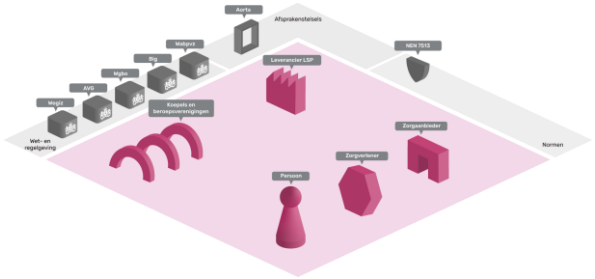
Haalbaarheidscriteria	
H1	De oplossing is **technisch haalbaar**. We beoordelen een oplossing als technisch haalbaar als de functie met reeds bestaande technologieën kan worden gerealiseerd en reeds is aangetoond dat deze technologie werkt (mogelijk in andere landen of een andere sector dan de zorg).
H2	De functie maakt gebruik van al bestaande oplossingen (**hergebruik van wat er al is**) 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 **impact** 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 **draagvlak bij de leveranciers**.
H5	Er is **maatschappelijk en politiek draagvlak** voor deze oplossing.

7.3 IST en SOLL visualisaties

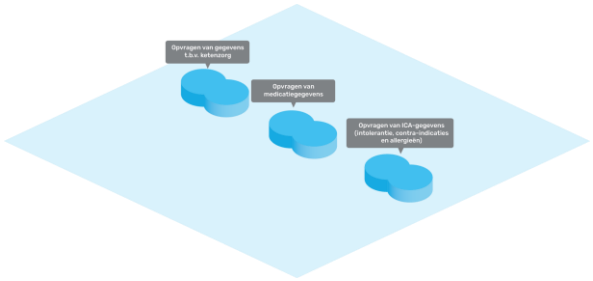
De visualisaties zijn opgesteld door BeBright en zijn voor de volledigheid hier opgenomen. Voor de details verwijzen we naar de visualisatie generieke functie adresseren van BeBright.

7.3.1 IST LSP

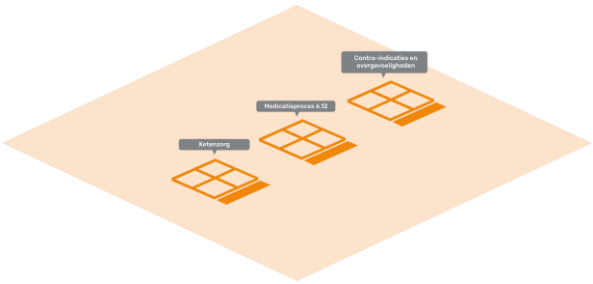
Organisatie



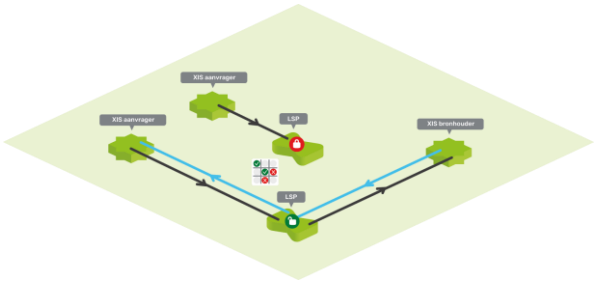
Zorgproces



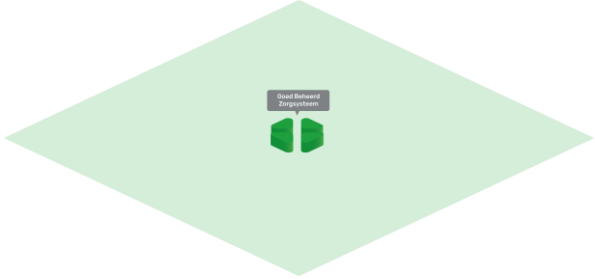
Informatie



Applicatie

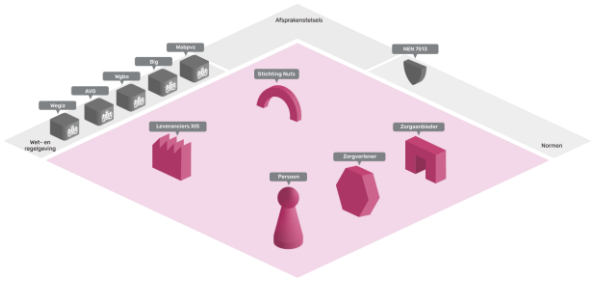


Infrastructuur

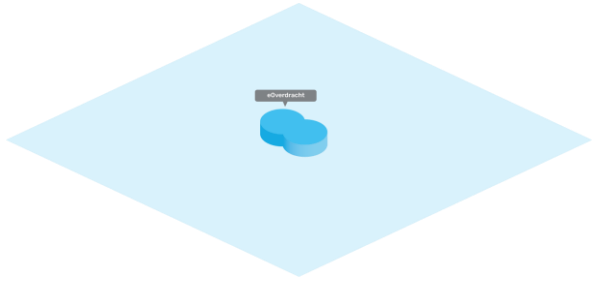


7.3.2 IST Nuts

Organisatie

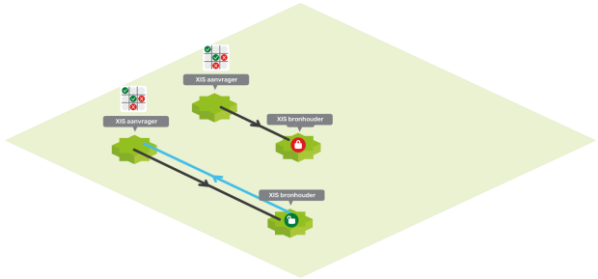


Zorgproces

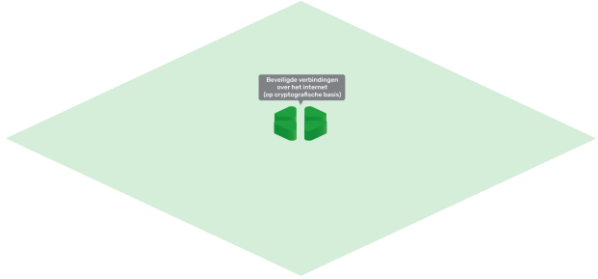


Informatie

Applicatie



Infrastructuur



7.4 Praktijk voorbeeld autorisatie OLVG

Het OLVG heeft in een autorisatiematrix vastgelegd: welke rechten er zijn (bijvoorbeeld dossier raadplegen, berichtensysteem, etc.), welke functies en waarom deze functies toegang moeten krijgen tot gegevens in het dossier.

Voor het grootste deel gaat de toepassing hiervan automatisch, bijvoorbeeld: Iemand komt in dienst als verpleegkundige, er worden dan automatisch de goede rechten toegekend. Dit werkt voor 70% van alle functionarissen. Voor de overige is er dus maatwerk nodig.
Als er subbevoegdheden nodig zijn, die niet standaard bij de functie horen, worden deze handmatig toegekend. Hier is een proces voor ingericht: als er extra autorisaties toegekend moeten worden of gewijzigd moeten worden komt dit in de autorisatiecommissie. Die bestaat uit juridische zaken, de EPD-dienst en vertegenwoordiging van de medische staf. Deze commissie bepaald of rechten worden toegekend.

Om de naleving van de gemaakte afspraken te controleren zijn er een aantal afspraken gemaakt:

- Een arts kan alles inzien van een patiënt, maar mag dat niet zomaar. Daarom is er een ‘Break the glass’-systematiek ingericht. Als een arts bijvoorbeeld geen behandelrelatie heeft, van een andere afdeling is, geen afspraak met de patiënt heeft, krijgt hij een melding en moet vervolgens een reden geven waarom hij het dossier toch wil inzien. Dit wordt gelogd.
- Er is structurele logging. Hierover wordt een rapport gemaakt, waar logica in zit. Bijvoorbeeld: een zorgverlener kijkt bij de patiënt met dezelfde achternaam, er worden gegevens geraadpleegd van een patiënt die ook collega is, er is geen afspraak of opname geweest met de patiënt, etc. In het rapport komen deze situaties naar voren en wordt nagegaan of de zorgverlener inderdaad ten onrechte in het dossier gekeken heeft.

De beleidsmatige vraagstukken rondom autorisaties worden in de privacy commissie: besproken. In deze commissie neemt de CISO, de voorzitter van de autorisatiecommissie, de functionaris gegevens bescherming en juridische zaken deel.

7.5 Geraadpleegde bronnen

D&A Medical Group. (2022). *Onderzoek landelijk netwerk van infrastructuren voor gegevensuitwisseling in de zorg.* 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.

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=%22Open%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. (2020, maart 31). *Organisatie-identificatienummer (OIN).* Opgehaald van Logius : https://gitdocumentatie.logius.nl/publicatie/dk/oin/2.0/OIN-Stelsel.pdf

Meyer, B. (1988). *Object-Oriented Software Construction.* Hemel Hempstead, United Kingdom.

MyHealth @ EU. (2023, Maart). *Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU.* Opgehaald van European Comission: https://health.ec.europa.eu/system/files/2023-04/ehn_guidelines_patientsummary_en.pdf

NEN. (2022, juli 1). NEN7512 Medische informatica - Informatiebeveiliging in de zorg - Vertrouwensbasis voor gegevensuitwisseling. Nederland.

Nictiz. (2022). *Visie op het zorginformatiestelsel.*

Nuts. (2023, maart 16). *Nuts wiki*. Opgehaald van Nuts wiki: https://wiki.nuts.nl/books/autorisatie

Rijksoverheid. (2020, juli 1). *Wettenbank.* Opgehaald van Overheid.nl : https://wetten.overheid.nl/BWBR0023864/2020-07-01

Rijksoverheid. (2023, februari 22). *Wetenbank.* Opgehaald van overheid.nl: https://wetten.overheid.nl/BWBR0001840/2023-02-22#Hoofdstuk1

Tesink, W., & Spee, J. (2022). *TxN 2026 - Gezamenlijk groeipad Twiin & Nuts.* Programma Twiin.

Twiin. (2021, december 16). *Twiin*. Opgehaald van Vertrouwensmodel: https://www.twiin.nl/vertrouwensmodel

VWS. (2023, april 13). *Heroriëntatie grondslagen.* Opgehaald van Tweede Kamer : https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2022Z08875&did=2022D17935

VZVZ. (2022, juni 9). *Het uitwisselingskompas.* Opgehaald van VZVZ: https://www.vzvz.nl/het-uitwisselingskompas

VZVZ. (2022). *Het uitwisselingskompas; generieke functies en gemeenschappelijke voorzieningen.*

VZVZ. (2023, augustus). *Programma Janus*. Opgehaald van https://www.vzvz.nl/initiatieven/programma-janus

7.6 Geïnterviewde partijen

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

Naam	**Rol**
ChipSoft	Autorisatie oplossing in uitwisselingssysteem
Epic	Autorisatie oplossing in uitwisselingssysteem
Enovation	Autorisatie oplossing in uitwisselingssysteem
Stichting MedMij	Gebruiker van de autorisatie functie
Stichting Nuts	Autorisatie oplossing in infrastructuur
Stichting VZVZ	Autorisatie oplossing in het LSP
Whitebox systems	Autorisatie oplossing in uitwisselingssysteem