vZVZ

Project Start Architectuur

Mitz

Datum:	4 mei 2021
Status:	Ter goedkeuring
Versie:	3.8.0.TG
Classificatie:	Vertrouwelijk
Eigenaar:	VZVZ
Revisie:	

Documenthistorie

Documentnaam	Locatie
Documentnaam VZVZ_Mitz_PSA v3.8.0.docx	Confluence

Documentversies

Datum	Status	Versie	Omschrijving	Auteur
12-04-2019	Concept	1.1	Initiële versie: 'as-is'-situatie uit GTS PSA 1.0 overgenomen in VZVZ PSA template / structuur. Verduidelijking en doorontwikkeling op basis voortschrijdend inzicht.	P.E. van Gemeren
25-04-2019	Ter goedkeuring	1.2	Opmaak conform huisstijl. Hoofstukken Wijzigingsbeheer en Definities verwijderd. Paragraaf 5.8 Risico's en omgang / acceptatie verwijderd en ondergebracht in separaat risicolijst document	P.E. van Gemeren
02-07-2019	Concept	2.01	Aanpassingen naar aanleiding van commentaar op versie 2.0	F. Schipper
30-09-2019	Ter verbetering	2.90	Versie voor interne review	F. Schipper
30-09-2019	Ter goedkeuring	2.91	Aanpassingen naar aanleiding van interne review	F. Schipper
15-10-2019	Concept	3.0.0.01	Doorontwikkeling versie 3.0.0.0	F. Schipper
26-11-2019	Concept	3.1.0.0	Tussenversie	F. Schipper
27-11-2019	Concept	3.1.0.01	Migratie	F. Schipper
2-12-2019	Ter verbetering	3.5.0.0	Review versie 3.5.0.0 release	F. Schipper
13-12-2019	Ter goedkeuring	3.5.0.0	After review versie 3.5.0.0 release	F. Schipper
06-03-2020	Ter goedkeuring	3.5.0.1	Consistentie PvE's	F. Schipper
03-04-2020	Ter goedkeuring	3.6.0.0	Ter Goedkeuring versie 3.6.0.0 release	F. Schipper
06-07-2020	Definitief	3.6.1	Versie voor release 3.6.1	F. Schipper
16-07-2020	Ter verbetering	3.6.2.TV	Interne review versie 3.6.2 release	F. Schipper
03-08-2020	Ter goedkeuring	3.6.2.TG	Externe review versie 3.6.2 release	F. Schipper
16-09-2020	Ter verbetering	3.7.0.TV	Interne review versie 3.7.0 release	F. Schipper
30-09-2020	Ter goedkeuring	3.7.0.TG	Externe review versie 3.7.0 release	F. Schipper
16-03-2021	Concept	3.8.0.C	Aanpassing Mitz high level model	F. Schipper
04-05-2021	Ter goedkeuring	3.8.0.TG	Externe review versie 3.8.0 release	F. Schipper

Accordering

Datum	Status	Versie	Wie
28-06-2019	Definitief	2.00	A. Vlug
15-10-2019	Definitief	3.0.0.0	A. Vlug
13-12-2019	Definitief	3.5.0.0.	A. Vlug
06-03-2020	Definitief	3.5.0.1	A. Vlug
17-04-2020	Definitief	3.6.0.0	A. Vlug
06-07-2020	Definitief	3.6.1	A. Vlug
01-09-2020	Definitief	3.6.2	A. Vlug
30-11-2020	Definitief	3.7.0	A. Vlug

Voorwoord

Dit document beschrijft de project start architectuur (PSA) van de online toestemmingsvoorziening Mitz.

Dit document dient als achtergrondkader voor de interpretatie van de eisen die aan Mitz en aan het gebruik van Mitz gesteld worden.

Doel van deze PSA is om ervoor te zorgen dat we in gezamenlijkheid de beste oplossing kunnen vaststellen voor een transparante en zorgbreed werkende (infrastructuur-onafhankelijke) toestemmingsvoorziening.

Inhoudsopgave

Lijst met figuren

1 Inleiding

Voor een goede zorgverlening is het van belang de juiste gegevens op het juiste moment en op de juiste plek beschikbaar te hebben. De uitwisseling van gegevens vergt soms een veronderstelde toestemming, soms een uitdrukkelijke toestemming van de betrokken patiënt. Door het vastleggen van een toestemmingskeuze (wel of geen toestemming) in een landelijke toestemmingsvoorziening, krijgt de patiënt meer regie, meer overzicht en meer transparantie. Door deze toestemmingsvoorziening te voorzien van open standaarden, kunnen alle uitwisselingssystemen (ongeacht de gekozen infrastructuur) aansluiten. Uitwisselingssystemen kunnen voor een specifieke uitwisseling via deze open koppelvlakken de betreffende toestemmingskeuze vast te stellen. Een toestemmingskeuze 'ja' levert een rechtsgeldige uitdrukkelijke toestemming op (voor uitwisselingen die een uitdrukkelijke toestemming als grondslag hebben; de 'opt-in'). Een toestemmingskeuze 'nee' is een bezwaar tegen een bepaalde uitwisseling (voor uitwisselingen die werken op basis van een veronderstelde toestemming, de 'opt-out').

1.1 Aanleiding

Het programma OTV (online toestemmingsvoorziening) beoogt de realisatie van een OTV-dienst voor burgers, patiënten en cliënten (hierna: patiënten) waarop elektronische uitwisselingssystemen voor zorgaanbieders kunnen aansluiten. Deze voorziening heet Mitz.

1.2 Stakeholders

Stakeholders binnen dit project zijn:

- Patiënten
- Zorgaanbieders
- Convenantpartijen
- Leveranciers
- Het programmateam GTS
- Management / bestuur VZVZ
- Interne medewerkers VZVZ

1.3 Doelstelling

Begin 2021 bestaat er een operationele online toestemmingsvoorziening, genaamd Mitz, waarop uitwisselingssystemen kunnen aansluiten. Mitz moet dan door minstens 80% van de patiënten te gebruiken zijn. Eind 2021 is op Mitz ten minste één uitwisselingssysteem aangesloten. Ten behoeve van tenminste één zorgaanbieder zijn de eventueel bestaande toestemmingen gemigreerd.

1.3.1 Beoogd resultaat

Mitz zal gefaseerd ingevoerd worden. In de eerste release van Mitz wordt een Minimal Viable Product (MVP) opgeleverd, waarna in de volgende fases steeds meer functionaliteit wordt toegevoegd.

1.4 Scope

1.4.1 In scope

Mitz heeft betrekking op de uitwisseling van gegevens tussen zorgaanbieders[1], waarbij toestemming als grondslag vereist is, of bezwaar gecontroleerd moet kunnen worden.

[1] US'en hoeven voor uitwisselingen tussen een zorgaanbieder en een niet-zorgaanbieder OTV niet te raadplegen (bijvoorbeeld voor uitwisselingen met RIVM, waarbij RIVM niet als zorgaanbieder optreedt).

1.4.2 Buiten scope

- De MedMij toestemmingen: Mitz gaat niet over toestemmingen om gegevens uit te wisselen met een persoonlijke gezondheidsomgeving (PGO). Afspraken daarover zitten in de scope van het programma MedMij.
- Artikel 66a geneesmiddelenwet waarin is vastgelegd dat apothekers met toestemming van de patiënt labbepalingen kunnen opvragen rechtstreeks bij de bron. Dit is de enige toestemming voor raadpleging. (artikel 15b uit de Wabvpz is komen te vervallen).
- Zorginkoop (bijvoorbeeld door zorgverzekeraars) is een ander domein; daar heeft Mitz geen betrekking op.
- Mitz integreert geen gegevensuitwisseling van verschillende uitwisselingssystemen.

1.5 Samenhang / afhankelijkheden met andere trajecten

Mitz maakt gebruik van het Zorgaanbiederadresboek, van DigiD, van Zorg-ID en van het UZI-register. Op termijn zal er ook gebruik gemaakt worden van de diensten van BZK (Logius), zoals de routeringsdienst en de machtigingsvoorziening (inclusief ouderlijk gezag). Er is een samenhang, maar geen afhankelijkheid met het TWIIN-afsprakenstelsel: landelijke afspraken over technische adressering van systemen kunnen desgewenst worden meegegeven op de koppelvlakken tussen US en Mitz.

1.6 Definities

Voor het raadplegen van definities en de betekenis van afkortingen, is een apart document opgesteld om zoveel mogelijk dezelfde begrippen te hanteren in de architecturen van diverse diensten die bij VZVZ in beheer zijn: '*VZVZ_Mitz_Afkortingen en Begrippenlijst*'.

1.7 Leeswijzer

Deze Project Start Architectuur (PSA) beschrijft op hoofdlijnen het ontwerp van Mitz. Op basis van de Programma's van eisen (PvE) worden detail ontwerpen gemaakt. In hoofdstuk 2 wordt de achtergrond van het programma OTV beschreven. Vervolgens wordt in hoofdstuk 3 ingegaan op de huidige situatie omtrent toestemmingen. Hoe de toekomstige situatie met Mitz er uit komt te zien wordt in hoofdstuk 4 beschreven. Gezien de korte tijd voor de ontwikkeling van Mitz, is gekozen om eerst een Minimal Viable Product (MVP) van Mitz te ontwikkelen. In latere fases zal de functionaliteit worden uitgebreid. Dit wordt in hoofdstuk 5 beschreven.
In hoofdstuk 6 en 7 wordt respectievelijk de gekozen oplossingsrichting en de overdracht naar project management beschreven.

2 Achtergrond

Mitz is een online toestemmingsvoorziening waarmee patiënten op een overzichtelijk wijze hun toestemmingskeuzes kunnen beheren en kunnen volgen of de betrokken zorgaanbieders zich aan de afspraken houden. De toestemmingskeuzes in Mitz kunnen geraadpleegd worden t.b.v. elektronische uitwisselingen die een toestemming vereisen: voorafgaand aan de uitwisseling kan via Mitz worden vastgesteld of er toestemming of bezwaar is vastgelegd voor die specifieke uitwisseling. Toestemmingen in Mitz voldoen aan het wettelijk kader hiervoor: WGBO, AVG, Wabvpz. Verder is Mitz is zodanig flexibel ontworpen dat nieuwe ontwikkelingen, na het informeren van alle betrokken partijen, hierin opgenomen kunnen worden.

Aanleiding: de juiste gegevens beschikbaar voor het zorgproces, op de juiste plek en het juiste moment.

Voor de verwerking van bijzondere persoonsgegevens vereist de AVG een wettelijke grondslag. Het uitwisselen van gegevens is een vorm van gegevensverwerking. Zowel het versturen als het opvragen van gegevens zijn vormen van gegevensuitwisseling. Medische gegevens worden, conform WGBO, actueel gehouden bij de behandelaar die het 'dossier voert'. In de zorg is er steeds meer sprake van het opvragen van gegevens die geregistreerd zijn bij de bron. Zo is het motto van het programma 'Registratie aan de Bron': "eenmalig registreren, meervoudig gebruik". Bij het opvragen van gegevens is een nieuw vraagstuk ontstaan: hoe weet je bij welke bron de relevante en noodzakelijke gegevens opgevraagd kunnen worden; en hoe maak je aan de bron duidelijk dat het beroepsgeheim doorbroken mag worden?

De afgelopen jaren zijn hiervoor uitwisselingssystemen ontstaan: met een index kan de betreffende bron worden gevonden en daarmee wordt het onnodig benaderen van *alle* zorgaanbieders ('broadcasten') voorkomen. Een broadcast verhoudt zich immers niet met de eis van dataminimalisatie (AVG), maar een broadcast is ook niet efficiënt bij 50.000 zorgaanbieders. Een uitwisselingssysteem met een index kan het versturen efficiënt organiseren, het gericht bevragen faciliteren, en ook een open bevraging ondersteunen. Bij een open bevraging weet de raadpleger niet welke bron(nen) bevraagd moeten worden. Omdat dit via de index van een uitwisselingssysteem achterhaald kan worden, is de bevraging van de bron daarna een gerichte actie: het uitwisselingssysteem weet wie de raadplegende zorgaanbieder is en bij welke dossierhoudende zorgaanbieder er gegevens opgevraagd moeten worden.

Het vraagstuk dat overblijft is: hoe maak je aan de bron duidelijk dat het beroepsgeheim doorbroken mag worden? Een patiënt of een zorgverlener kan daarvoor contact opnemen met de dossierhouder. Het probleem daarbij is dat op de momenten dat gegevens nodig zijn, de dossierhouder niet altijd beschikbaar of bereikbaar is, laat staan met de patiënt kan overleggen (en een mogelijkheid tot bezwaar kan geven). Om de juiste gegevens toch beschikbaar te maken op de plek waar ze nodig zijn, is het van tevoren regelen van een uitdrukkelijke en specifieke toestemming in het licht van de AVG een adequate grondslag voor deze gegevensverwerking.

Aandacht voor uitdrukkelijke toestemming naar aanleiding van de Wabvpz

Om alle onduidelijkheid te voorkomen, is dit vereiste uit de AVG (toen nog WBP) expliciet in een aparte wet geformuleerd. Op 4 oktober 2016 heeft de Eerste Kamer na zorgvuldige beraadslaging de Wabvpz aangenomen. Artikel 15a lid1 gaat over deze manier van toestemming verlenen. Het amendement van het Tweede Kamerlid Bruins Slot heeft geleid tot artikel 15a, lid 2 in de wet, waarin het recht van de patiënt om *gespecificeerde* toestemming te geven voor gegevensuitwisseling met bepaalde (categorieën van) zorgverleners is vastgelegd. De uitdrukkelijke toestemming (lid 1) voor het beschikbaar stellen van gegevens via een elektronisch uitwisselingssysteem, moet conform lid 2 dus 'gespecificeerd' zijn.

Het nieuwe van de 'gespecificeerde toestemming' conform de Wabvpz (artikel 15a, tweede lid) is dat het 'specifieke' van de AVG is uitgewerkt naar categorieën en dat er een toestemmingskeuze mogelijk moet zijn per categorie (als de patiënt dat wil). Vanwege onduidelijkheden over de uitvoering van artikel 15a lid 2 heeft het ministerie van VWS in 2015 een Bestuurlijk Overleg georganiseerd met de KNMG, de KNMP, de LHV, de Patiëntenfederatie en Nictiz, met het doel te komen tot een eensluidende interpretatie van het artikel en een aanpak die werkbaar is voor zowel de patiënt als de zorgaanbieder. Om partijen daarvoor voldoende tijd te gunnen, heeft de minister de inwerkingtreding van artikel 15a, tweede lid, destijds uitgesteld.

Het Bestuurlijk Overleg heeft geleid tot een gedeelde visie op de uitvoerbaarheid van het wetsvoorstel, waarbij de patiënt uiteindelijk zelf zijn toestemmingsprofiel moet kunnen vastleggen, inzien en aanpassen. In maart 2016 is door alle partijen, inclusief VWS, een programmaplan geaccordeerd.

De zorgpartijen, verenigd in de stuurgroep Gespecificeerde Toestemming (GTS), hebben het daaruit voortkomende programma de opdracht gegeven om met experts en partijen in de zorg te onderzoeken of, en zo ja hoe, het wetsartikel over gespecificeerde toestemming werkbaar en uitvoerbaar gemaakt kan worden voor de patiënt en zorgaanbieder.

Tussen maart 2016 en december 2017 heeft het programma GTS een eerste onderzoek uitgevoerd naar de technische en praktische mogelijkheden voor het online beheren van gespecificeerde toestemmingen door de burger. De bestaande en operationele elektronische uitwisselingen waar uitdrukkelijke toestemming voor nodig is, zijn geïnventariseerd. Voor deze scope zijn de toestemmingsmogelijkheden beredeneerd. De uitwerking van de definitie van gespecificeerde toestemming in het betreffende wetsartikel is nader getoetst door juridische experts en gevalideerd door PBLQ. Er is gekeken naar een model voor aansluiting van informatie- en uitwisselingssystemen in de zorg op een dergelijke voorziening. De eerste onderzoeksfase heeft geleid tot een juridisch optimum met 160 toestemmingsmogelijkheden. De stuurgroep heeft aan de minister haar zorg geuit over de uitvoerbaarheid door dit hoge aantal.

De minister heeft de stuurgroep gevraagd om een alternatief scenario te bedenken waarin de bedoeling van de wet als uitgangspunt wordt genomen, en waarin het gebruik van informatiestandaarden in de zorg bepaalt hoe gespecificeerd het kan en de burger bepaalt hoe gespecificeerd het moet.

Ondertussen is duidelijk geworden dat de nieuwe vormen van ‘realtime’ gegevens opvragen bij de bron, op het moment dat ze elders in de behandeling nodig zijn, vaak een uitdrukkelijke en specifieke toestemming nodig hebben. Immers, als de WGBO geen grondslag levert, kan de uitdrukkelijke en specifieke toestemming uit de AVG een grondslag vormen voor dit type uitwisseling. Daarnaast geeft artikel 15a lid 1 van de Wabvpz expliciet aan dat uitdrukkelijke toestemming nodig is voor vormen van gegevensuitwisseling, waarbij de dossierhouder van tevoren de gegevens ‘beschikbaar stelt’ voor de bevraging door een of meer zorgaanbieders, die hij op dat moment niet weet en ook niet met de patiënt besproken heeft.

Zorgaanbieders moeten daarom voor het ‘ongericht’ delen van gegevens een uitdrukkelijke toestemming van de patiënt organiseren. Om wildgroei van toestemmingssystemen en toestemmingskeuzes te voorkomen en om de administratie in de zorg te ontlasten, is de noodzaak ontstaan om het organiseren van toestemmingen te uniformeren en te faciliteren. Eén plek waar de patiënt (cliënt / burger) een overzicht heeft van alle toestemmingsmogelijkheden, en waarmee de patiënt kan volgen wat er met de toestemmingskeuzes gebeurt in de gegevensuitwisseling, is dan een efficiënte manier om hieraan invulling te geven. Het ontwerp van een Online ToestemmingsVoorziening (OTV), waar iedereen zijn toestemming voor digitale gegevensuitwisseling tussen zorgaanbieder kan beheren, wordt in deze PSA beschreven.

3 Huidige situatie toestemmingen

3.1 Algemeen

De huidige situatie beschrijft hoe de patiënt momenteel toestemming aan de zorgaanbieder verleent. Ten opzichte van de gewenste situatie wordt dan de verandering duidelijk waarvoor deze PSA is opgesteld.

3.1.1 Toestemming

In de huidige situatie wordt er in één toestemmingsmogelijkheid:

1. beschreven welke gegevens worden uitgewisseld tussen welke zorgaanbieders, bijvoorbeeld huisartswaarneemgegevens, medicatie of ketenzorg (via het LSP) of medische beelden (via een regionaal XDS netwerk).
2. een toestemmingskeuze gevraagd, meestal per zorgaanbieder, voor het uitwisselen van de beschreven gegevens via het betreffende uitwisselingssysteem.

Per zorgaanbieder en/of uitwisselsysteem kunnen er variaties op bovenstaande zijn.

3.1.2 Toestemming vragen

Toestemming voor uitwisseling van medische gegevens kan op dit moment op de volgende manieren worden gegeven:

1. Een patiënt geeft mondeling aan dat hij / zij het goed vindt dat de gegevens door de betreffende zorgaanbieder gedeeld worden, conform de informatie die de zorgaanbieder verstrekt heeft;
2. De patiënt vult een toestemmingsformulier in en levert dat in bij de zorgaanbieder;
3. De patiënt regelt toestemming via een portaal, zoals volgjezorg.nl waarna de toestemming wordt verzonden aan de betreffende zorgaanbieder.

Bij alle drie de varianten is het belangrijk dat de patiënt de voorlichtingsfolder heeft doorgenomen (zie bron). De zorgaanbieder is hier altijd de dossierhouder.

Soms is het mogelijk om voor iemand anders toestemming te regelen en om online toestemmingen in te trekken (bijvoorbeeld via volgjezorg.nl).

Zodra de toestemming(swijziging) in de systemen verwerkt is, is die effectief in de gegevensuitwisseling.

3.1.3 Acceptatie door patiënt en zorgaanbieder

In de huidige situatie is er sprake van:

1. Een door patiënten geaccepteerde situatie:
   1.1. Alle patiënten kunnen werken met het geven van mondelinge toestemming of het invullen van een analoog formulier.
   1.2. Hiernaast kunnen de patiënten die dit willen ook op digitale wijze hun toestemming verlenen.
2. Een door zorgaanbieders geaccepteerde situatie:
   2.1. Indien de zorgaanbieder schriftelijk toestemming ontvangt voor het delen van patiëntdata, dan kan de zorgaanbieder deze verkregen toestemming bewaren.
   2.2. Soms kan deze toestemming worden geregistreerd, bijvoorbeeld indien het zorginformatiesysteem (XIS) hiervoor een mogelijkheid biedt. Bij sommige uitwisselingssystemen wordt op basis van deze toestemming een index bijgewerkt (vergelijk de verwijsindex (VWI) van het LSP).

3.2 Probleemomschrijving huidige situatie

Het is voor een patiënt in de huidige situatie onduidelijk aan wie er ooit toestemming is gegeven voor uitwisseling en voor welke medische gegevens die toestemming dan geldt. Er is niet één plek om alle toestemmingen in te zien, laat staan te beheren en daarmee is er geen eenduidige regie over de uitwisseling van gegevens.

3.2.1 Knelpunten en Oorzaken

Het is voor een patiënt in de huidige situatie moeilijk in te zien waarom je bij elke zorgaanbieder waar je voor het eerst komt, opnieuw toestemming moet geven.

Het is voor een zorgaanbieder tijdrovend om toestemmingen te verzamelen van alle patiënten, ten behoeve van continuïteit van zorg. Als een toestemmingsformulier wel wordt ingevuld maar door de zorgaanbieder nog niet verwerkt is, levert dat een risico op voor de kwaliteit van de zorgverlening. Daarnaast is het vaak lastig om als zorgaanbieder te bepalen of eenmaal vastgelegde toestemmingen nog wel actueel zijn en passend op het geldende wettelijk kader.

Ook is het vaak niet mogelijk om bij een zorgaanbieder die gegevens nodig heeft, toestemming te geven aan zorgaanbieders die de gegevens in het dossier hebben staan. Wettelijk gezien moet immers de dossierhouder het beroepsgeheim doorbreken op basis van de toestemming van de patiënt. Waar een patiënt veronderstelt dat er alleen maar een toestemming gegevens hoeft te worden voor het raadplegen van zijn gegevens, is het wettelijk zo dat er juist eerst toestemming nodig is om gegevens vanuit de bron te delen. Om zo dicht mogelijk aan te sluiten bij de praktijk moet er dus een mogelijkheid komen dat de patiënt bij een raadpleger toestemming kan geven aan een bron die het dossier voert. Die dossierhoudende zorgaanbieder moet er dan wel op kunnen vertrouwen dat de toestemming rechtsgeldig is en eenduidig. En dat moet in de systemen geborgd worden, zodat de gegevens ook gedeeld kunnen worden als de dossierhouder niet zelf aanwezig is.

In de huidige situatie kan er voor elke zorgaanbieder, voor elke uitwisseling (of voor elk uitwisselingssysteem) een toestemmingsvoorziening gebouwd worden. Daarmee ontstaat echter een knelpunt voor de patiënt omdat die met al die verschillende voorzieningen om moet leren gaan. Het aantal toestemmingsmodelijkheden is dan ook niet meer vanuit het oogpunt van de patiënt te organiseren. Ook is het met meerdere bronnen van toestemmingen lastig om te achterhalen bij wie de toestemming geraadpleegd moet worden. Daarnaast moeten alle voorzieningen borgen dat de toestemmingen rechtmatig en betrouwbaar zijn. Immers, een zorgaanbieder heeft niet alleen te maken met de toestemmingen die voor hem (als bron) gelden, maar moet (namens de patiënt) ook toestemmingen voor andere zorgaanbieders kunnen vastleggen. Ook dat moet op een eenduidige wijze worden gerealiseerd.

Bij het digitaliseren van diensten in de zorg, zijn er ook knelpunten die breder zijn dan de zorg. Zo is voor het inloggen door de patiënt, op diensten waar medische gegevens worden uitgewisseld, een authenticatiemiddel vereist op een betrouwbaarheidsniveau dat hoger ligt dan gebruikersnaam en wachtwoord. Echter, de introductie en adoptie van zo'n authenticatiemiddel is alleen voor zorgdoeleinden lastig gebleken. Daarom wordt voor zorgdiensten steeds meer aangesloten bij diensten die (soms vanuit de overheid) voor alle burgers worden geregeld. Het gaat dan bijvoorbeeld om de inlogdienst DigiD (die meeloopt met de Europese regelgeving van laag naar midden naar hoog). Een ander voorbeeld is een machtigingsvoorziening (bv. om mantelzorgers te kunnen machtigen). Als er door de overheid een machtigingsvoorziening (voor het 'BSN-domein') wordt geregeld, is het voor de burger erg handig als de zorg daar ook gebruik van kan maken. Met de wet Digitale Overheid wordt de zorgsector expliciet meegenomen in deze ontwikkelingen. Toestemmingsvoorzieningen moeten daarom niet alleen continu aangepast worden op de wet- en regelgeving in de zorg, maar ook op die van de overheid. Het borgen van een (blijvende) rechtmatige toestemming is bij verschillende toestemmingsvoorzieningen een kostbare aangelegenheid.

Naast het blijven voldoen aan wet- en regelgeving, is er ook sprake van een minimale set aan (gebruiksvriendelijke) functionaliteiten, die landelijk afgestemd zou moeten worden. Zo is het voor de kinderen die in een intensief of langdurig behandeltraject zitten ook van groot belang om de gegevensuitwisseling te faciliteren. Het organiseren van toestemming bij deze groep (onder de 12; vanaf 12 tot 16; en vanaf 16 en ouder) is een knelpunt en wordt in een digitale voorziening daarom bijna niet ondersteund. Een ander voorbeeld is het organiseren van gegevensuitwisseling in spoed situaties. Voor het organiseren van toestemmingen gelden aparte regels en soms willen patiënten geen toestemming geven voor het delen van gegevens in normale situaties, maar dan een uitzondering maken voor spoed situaties. Omdat een toestemming voor normale situaties ook geldt voor spoedsituaties, moet een toestemmingsvoorziening beide kunnen ondersteunen.

Meerdere toestemmingsvoorzieningen is vanuit het perspectief van de patiënt een knelpunt en vanuit het perspectief van organisatie en financiering zeer inefficiënt.

4 Toekomstige situatie: Mitz

Het programma OTV realiseert een toestemmingsvoorziening binnen de hieronder genoemde kaders, uitgangspunten en principes.

4.1 Kaders

4.1.1 Juridische kaders

Een rechtmatige toestemming moet voldoen aan het huidige wettelijk kader (WGBO, AVG en Wabvpz, zie voor de onderlinge samenhang het 'Juridisch kennisdocument toestemmingen'). Om er voor te zorgen dat met deze ene toestemming, ook de uitwisseling van gegevens rechtmatig is, kan er juridisch gezien, sprake zijn van verschillende toestemmingen die in één toestemmingskeuze kunnen worden gecombineerd. Een online toestemmingsvoorziening dient hier rekening mee te houden. De volgende toestemmingen kunnen (vanuit juridisch perspectief) worden onderscheiden.

I. Het gaat in de eerste plaats om de toestemming om het beroepsgeheim te doorbreken. Het beroepsgeheim wordt niet doorbroken als gegevens gedeeld worden met:
   a. degenen die *rechtstreeks betrokken* zijn bij de uitvoering van de behandelingsovereenkomst en
   b. degene die optreedt als *vervanger van de hulpverlener*, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden (WGBO)

   De toestemming om het beroepsgeheim te doorbreken kan soms worden verondersteld:

   1. in concrete situaties (inclusief *spoedeisende zorg*);
   2. waarin het *kenbaar* is voor de patiënt dat:
      a. gegevens *voor zorgdoeleinden* worden verstrekt
      b. de patiënt daartegen *geen bezwaar* heeft gemaakt; en
      c. de gegevensverstrekking beperkt blijft tot hetgeen *noodzakelijk is voor de ontvanger.*

II. Het gaat in de tweede plaats om een toestemming als *grondslag voor de verwerking* van gegevens. In het algemeen eist de AVG van een rechtmatige verwerking van gegevens dat *één* van de volgende grondslagen aanwezig moet zijn:
   a. de betrokkene heeft *toestemming* gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden;
   b. de verwerking is noodzakelijk voor de uitvoering van een *overeenkomst* waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
   c. de verwerking is noodzakelijk om te voldoen aan een *wettelijke verplichting* die op de verwerkingsverantwoordelijke rust;
   d. de verwerking is noodzakelijk om de *vitale belangen* van de betrokkene of van een andere natuurlijke persoon te beschermen.

   Voor het verlenen van zorg door zorgaanbieders en de verwerking van bijzondere persoonsgegevens hiervoor, is een ontheffing beschreven in de Uitvoeringswet van de AVG (UAVG). Voor de uitwisseling van medische gegevens in de zorg gaat het over het algemeen om de AVG grondslag 'overeenkomst' of 'toestemming'.

III. In de derde plaats gaat het om toestemming voor *elektronische uitwisseling via het beschikbaar stellen* van gegevens. Dat wordt sinds 1 juli 2017 vereist door de Wabvpz artikel 15a lid 1.

IV. In de vierde plaats kan er toestemming nodig zijn om de gegevens te verwerken door een beheerder van een uitwisselingssysteem. Als de zorgaanbieders die op een uitwisselingssysteem zijn aangesloten zich verenigd hebben in een aparte rechtspersoon en deze is gegevensverwerkingsverantwoordelijk voor de verwerking van de gegevens in bijvoorbeeld de index van het uitwisselingssysteem, dan dient de patiënt hier ook toestemming voor te geven.

NB. Dit geldt niet altijd voor uitwisselingssystemen met een index, immers de verwerking van gegevens in een index kan ook onder gegevensverwerkingsverantwoordelijkheid blijven van de (dossierhoudende) zorgaanbieder. Op Mitz moeten beide type uitwisselingssystemen kunnen aansluiten:

a. Type 1 waarbij de index van een zorgaanbieder (met de BSN's van de patiënten van wie er door die zorgaanbieder een dossier wordt gevoerd) onder (gegevensverwerkings)verantwoordelijkheid van die zorgaanbieder bijgehouden wordt. In dat geval mag de index worden gevuld als onderdeel van de dossiervoering die conform de behandelovereenkomst moet plaatsvinden, dus zonder uitdrukkelijke toestemming. Daarbij geldt dat die index voor andere zorgaanbieders niet raadpleegbaar is, zonder uitdrukkelijke toestemming (het wordt immers beschouwd als onderdeel van het dossier). Hierbij geldt: *aanmelden* bij de index is *zonder* toestemming en *raadplegen* van de index is *met* toestemming.
b. Type 2 waarbij de gegevensverwerking van de index plaatsvindt onder verantwoordelijkheid van een aparte rechtspersoon waarin zorgaanbieders verenigd zijn. In dat geval is er toestemming nodig voor die rechtspersoon als grondslag om gegevens te verwerken. Indien deze toestemming tegelijk gevraagd wordt met de toestemming voor uitwisseling, hoeft er voor het raadplegen van de index bij de uitwisseling niet apart toestemming geregeld te worden. Hierbij geldt: *aanmelden* bij de index is *met* toestemming en *raadplegen* van de index *zonder* aparte toestemming.

Voor de interpretatie van de wetteksten die de toestemmingen beschrijven, zijn de volgende documenten van VWS van belang:

- Brief aan Tweede en Eerste kamer over toetsing wet aan praktijk (22 december 2015)
- Memorie van Toelichting op de wet met nieuwe cliëntenrechten (Wabvpz)
- Juridisch kennisdocument over het wettelijk kader voor toestemmingen (www.programma-otv.nl)

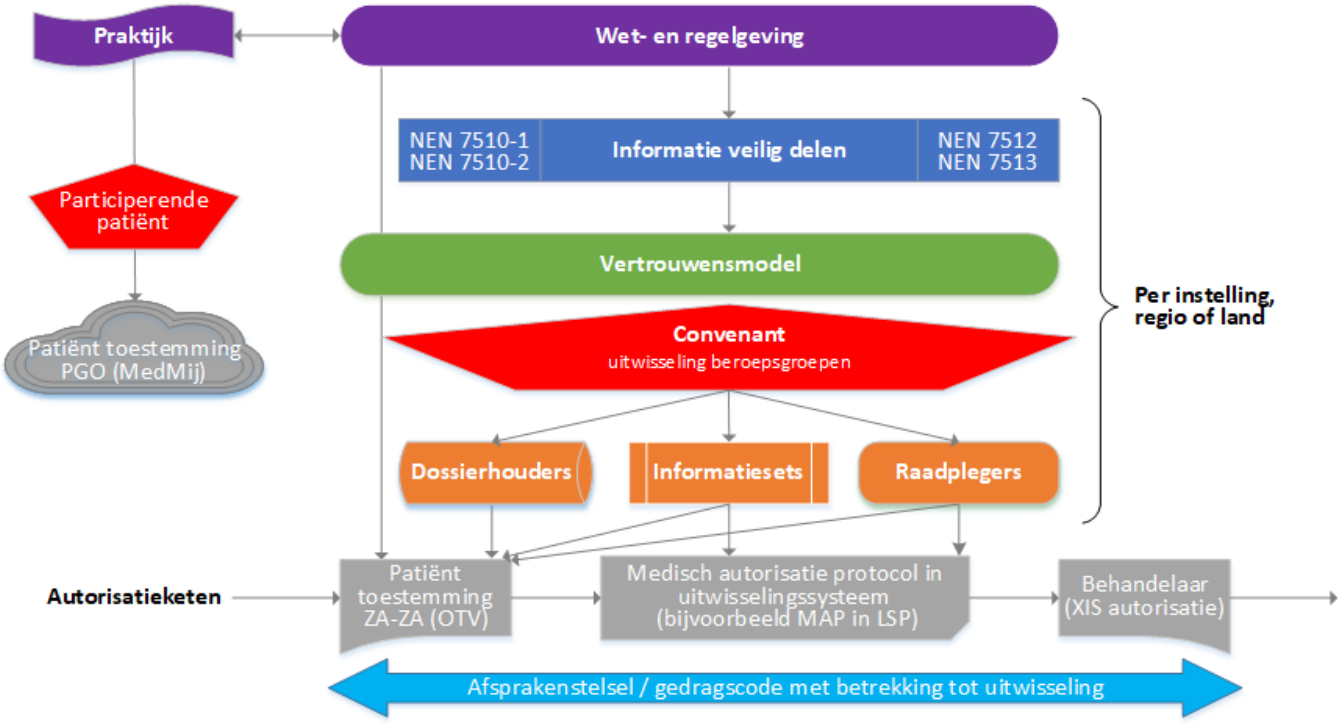
4.2 Uitgangspunten ten aanzien van vertrouwensaspecten

Mitz faciliteert het registreren en beheren van toestemmingkeuzes voor het wel of niet delen van gegevens via een elektronisch uitwisselingssysteem.

4.2.1 Vertrouwensmodel

Het vertrouwensmodel dat hoort bij het betreffende US is de basis voor het vertrouwen in een veilige en adequate elektronische gegevensuitwisseling. Er zijn diverse ‘modellen’ opgesteld om het vertrouwen te borgen dat er zorgvuldig met medische gegevens wordt omgegaan. Ondanks deze diversiteit, is elk vertrouwensmodel een geheel van afspraken en (controlerende) procedures, waardoor het beoogde niveau van privacybescherming en veiligheid bereikt wordt. In een vertrouwensmodel kan bijvoorbeeld beschreven worden:

- welke personen welke verantwoordelijkheden hebben.
- op welke basis er voldoende vertrouwen bestaat om onderling informatie uit te wisselen.
- welke afspraken er gemaakt worden over de omgang met privacy- en informatiebeveiliging.
- hoe de omgang en spelregels ten aanzien van architectuur vorm gegeven worden.
- hoe de uitwerking van wetgeving en NEN-normen in processen en techniek wordt vormgegeven.
- wat voor afspraken en contracten etc. nodig zijn alvorens informatie uit te wisselen.



Figuur 1: Vertrouwensmodel

Op basis van de beschreven wet- en regelgeving kan iedere zorginstelling, iedere regio of ieder land een vertrouwensmodel opstellen voor elektronische gegevensuitwisseling. Op basis van zo'n vertrouwensmodel worden veelal concrete afspraken opgesteld, met regels waar men zich aan houdt als men aansluit op het betreffende US.

In een vertrouwensmodel kunnen afspraken opgenomen zijn, die het geheel van technische, organisatorische en juridische waarborgen beschrijven voor het vertrouwen in de landelijke elektronische uitwisseling van medische gegevens.

Om te voorkomen dat een patiënt voor alle mogelijke afzonderlijke uitwisselingen gevraagd wordt om toestemming te geven, waardoor het voor een patiënt niet meer te overzien of te begrijpen is, wordt gezocht naar een praktisch optimum van het aantal toestemmingsmogelijkheden. Dat houdt in dat de toestemmingsmogelijkheid die aan de patiënt getoond wordt in een toestemmingsvoorziening, ruimer kan zijn dan dat wat daadwerkelijk uitgewisseld wordt. NB de toestemmingsmogelijkheid die getoond wordt kan nooit specifieker zijn dan een bepaalde uitwisseling. Immers als de patiënt zou aangeven dat pillen wel uitgewisseld mogen worden en chemokuren niet, terwijl dat in een uitwisseling in één groep of bouwsteen zit (bv. 'medicatie'), kan de uitwisseling niet gemapt worden op een toestemming.

De eerste stap in de autorisatieketen (zie figuur 1) is dan ook de toestemmingskeuze van de patiënt, die niet te fijnmazig mag zijn (vanwege begrijpelijkheid en overzichtelijkheid) maar wel specifiek genoeg moet zijn. Het streven is om voor alle uitwisselingen in de zorg te starten met een beperkt aantal toestemmingsmogelijkheden en toe te groeien naar maximaal 30.

In de tweede stap worden de gegevens waarvoor toestemming is verleend, verder ingeperkt tot datgene wat nodig en relevant is voor de raadplegende zorgaanbieder. Dat is in lijn met het juridisch kader, omdat deze inperking zowel in de WGBO staat, als in de AVG (daar vloeit het voort uit het proportionaliteitsbeginsel). In lijn met deze wetgeving kan een toestemming deze beginselen niet overrulen. Dus als een patiënt toestemming geeft om behandelgegevens vanuit een ziekenhuis te delen met apothekers, dan zal er in de uitwisseling een filtering plaatsvinden op basis van beroepsrichtlijnen en kwaliteitsstandaarden. De beroepsrichtlijnen kunnen in een convenant worden afgesproken en bepalen wat in een bepaalde uitwisseling noodzakelijk en relevant is voor welke beroepsgroep. Door dit filter wordt een uitwisseling rechtsgeldig. Een uitwisselingssysteem moet nagaan of de ondersteunde uitwisselingen in zit opzicht rechtsgeldig zijn. Bij het Landelijk Schakelpunt heeft dat geleid tot meerdere Medische Autorisatie Richtlijnen (MAR's) welke geëffectueerd worden in een Medische Autorisatie Protocol (MAP). Toestemmingen vallen binnen de kaders van een vertrouwensmodel, maar kunnen de overige kaders (waaronder de autorisatieafspraken die gemaakt zijn binnen, bijvoorbeeld een MAP, niet overrulen.

Na de eerste stap in de autorisatie keten waarbij de patiënt online toestemming geeft, en de tweede stap waarbij een uitwisselingssysteem een autorisatieprotocol implementeert om relevante informatiesetjes te koppelen aan de beroepsgroep van de opvrager, is er een derde stap waarbij in de lokale systemen van de zorgaanbieder een verdere

autorisatie plaatsvindt. Bij het inzien van de uitgewisselde gegevens binnen de muren van een zorginstelling, wordt bepaald welke personen direct bij de behandeling betrokken zijn (bijvoorbeeld het behandelteam). Ook kan lokaal desgewenst een verdere filtering van gegevens plaatsvinden op basis van de rol of beroepsgroep van de betreffende medewerker binnen het behandelteam. Tenslotte heeft de patiënt nog de mogelijkheid om stukken van zijn dossier af te schermen bij de zorgaanbieder (dus ook lokaal), zodat deze delen, los van de toestemming, nooit uitgewisseld kunnen worden.

Met de introductie van Mitz wordt het geheel van partijen die aan het vertrouwensmodel over gegevensuitwisseling deelnemen groter, omdat alle zorgaanbieders die via welk US dan ook kunnen uitwisselen, kunnen gaan vertrouwen op Mitz waar het de toestemming van de patiënt betreft.

Dat betekent dat de patiënt voldoende vertrouwen moet kunnen hebben in de privacy- en informatiebeveiliging van de zorgaanbieders die gegevens van de patiënt verwerken ongeacht of deze zorgaanbieder is aangesloten op het ene US of het andere US. Ook moet er vertrouwen zijn in de rechtmatigheid van de toestemming in Mitz en er moet zekerheid zijn over de identificatie van de patiënt. Daarom zal Mitz een vertrouwensmodel opstellen voor dit overkoepelende deel. De beheerder van een US dat op Mitz aansluit zal deze afspraken moeten onderschrijven en waar nodig verwerken in hun afspraken met zorgaanbieders die bij hen aansluiten.

4.2.2 Voldoen aan NEN-normen en BSN gebruik

Bij oplevering zal Mitz moeten voldoen aan de beveiligingsnormen voor elektronische uitwisselingssystemen (NEN 7510 en NEN 7512 voor informatiebeveiliging en NEN 7513 voor logging van toestemmingregistratie handelingen). Zie het besluit elektronische gegevensverwerking in de zorg.
Mitz verwerkt de toestemminggegevens namens de dossierhoudende zorgaanbieder en heeft daarmee een wettelijke grondslag om het burgerservicenummer (BSN) te verwerken (art. 8.2 Wabvpz).

Mitz zal, conform de NEN 7513, de metadata van de transacties met betrekking tot de toestemmingsregistratiefaciliteit (registreren, wijzigen, verwijderen) loggen. Ook van de transacties met betrekking tot raadplegen van toestemmingen (bevraging Mitz en antwoord van Mitz) zullen de metadata worden gelogd. De transacties met betrekking tot delen en raadplegen van gegevens verloopt via elektronische uitwisselingssystemen en wordt aldaar gelogd.

4.2.3 Privacy- en informatiebeveiligingsaspecten

Privacybescherming is bij uitwisseling van medische gegevens een eerste vereiste. Wanneer de patiënt in staat wordt gesteld deze bescherming steeds meer zelf te reguleren draagt dat ook bij aan de beleving ervan. Mitz is in die zin een onderdeel van de privacy bij gegevensuitwisseling.

De betreffende uitwisselingssystemen moeten er op hun beurt ook op kunnen vertrouwen dat de via Mitz geregistreerde toestemmingen:
- te vertrouwen zijn,
- voldoen aan de privacy-by-design regels en
- goed beveiligd zijn.

Toestemmingen (met name toestemmingen aan een individuele dossierhouder) zijn te beschouwen als een bijzonder soort persoonsgegevens en zullen door Mitz als zodanig behandeld en beschermd worden. Mitz past derhalve, conform de ‘Algemene verordening gegevensbescherming’ (AVG), de volgende principes toe:
- privacy-by-design (toepassen van privacy enhancing technologies (PET) en pseudonimiseren BSN)
- privacy-by-default (uitgangspunt is dataminimalisatie: pas attributen opnemen als je ze nodig hebt)

4.3 Uitgangspunten ten aanzien van de zorgprocessen

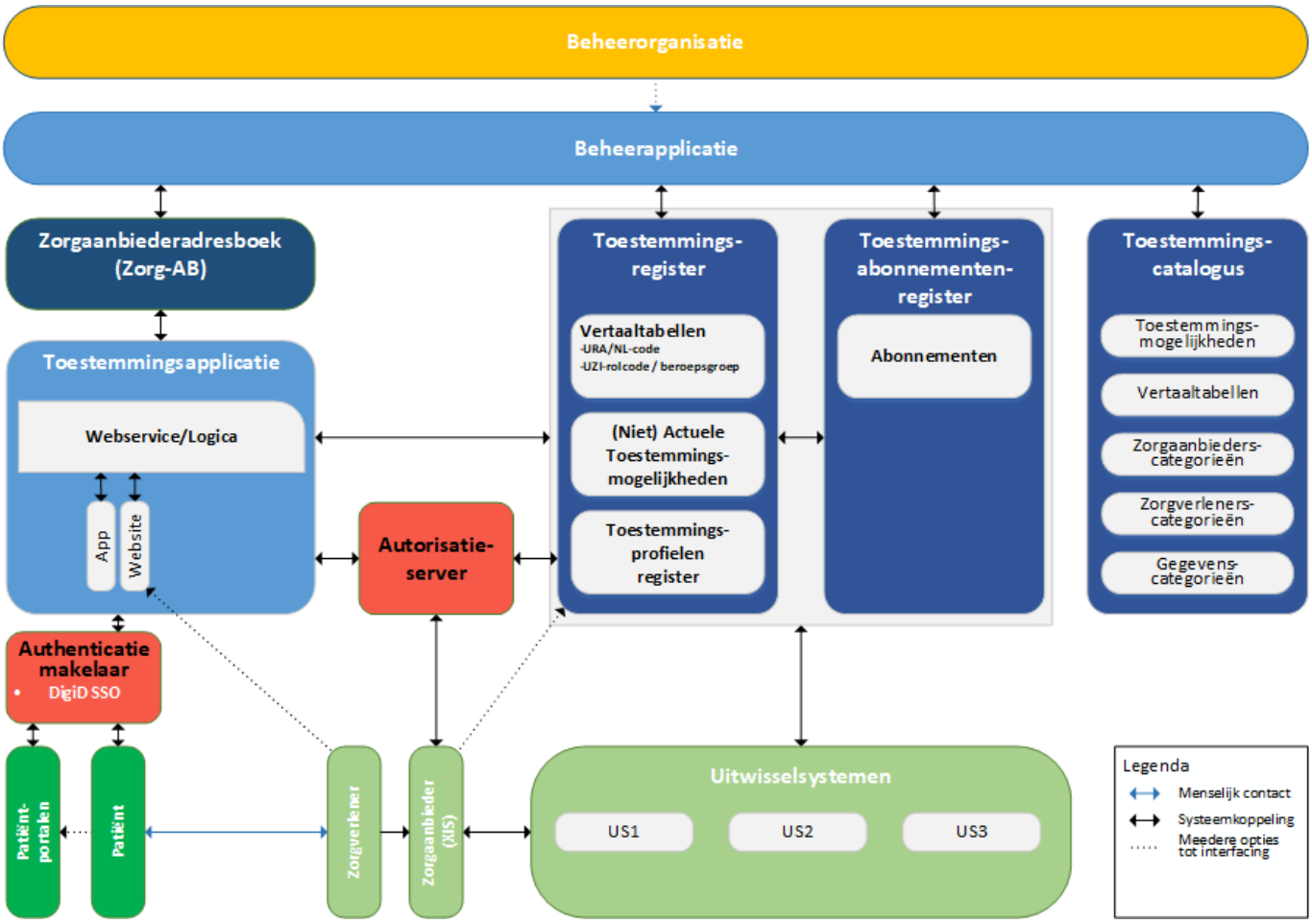
- Voorkomen dat er technologie-gedreven oplossingen komen die wel de nieuwe gegevensuitwisseling faciliteren, maar niet aansluiten bij de eigenlijke verandering in taken, rollen en verantwoordelijkheden.
- Voorkomen dat er fundamentele vergezichten of politiek correcte compromissen ontstaan die geen ondersteuning bieden aan de dagelijkse praktijk.
- Een oplossing die te ingewikkeld is voor de gebruikers (patiënten en zorgaanbieders) zal niet of niet goed worden gebruikt of worden omzeild en is daarmee onveilig. De nadruk bij het ontwikkelen van de oplossing zal dus liggen op gebruiksgemak voor patiënten en voor zorgaanbieders (bron: convenant OTV).

4.4 Uitgangspunten ten aanzien van de Mitz-architectuur

4.4.1 Concept op hoofdlijnen

Op hoofdlijnen bestaat Mitz uit vier onderdelen:

1. Een 'toestemmingsapplicatie' (TAP) waarmee patiënten hun toestemmingskeuzes kunnen vastleggen via een (responsive) website, smartphone of vanuit een externe omgeving zoals een patiëntportaal.
2. Een toestemmingsregister waarin de toestemmingskeuzes op een veilige en beveiligde manier worden opgeslagen in een toestemmingsprofiel en geschikt gemaakt voor zorgaanbieders die moeten kunnen vaststellen of er toestemming is verleend. Informatie uit de toestemmingscatalogus kan (bv. om performance redenen) in het register worden overgenomen.
3. Een toestemmingsabonnementenregister waarop zorgaanbieders zich kunnen abonneren, zodat de zorgaanbieders kunnen vaststellen of er toestemming aan hun is verleend.
4. Een toestemmingscatalogus waarin de informatiemodellen (waaronder de categorieën) van een toestemmingsmogelijkheid worden beheerd. Dat is de bron waar een systeembeheerder toegang toe heeft via de beheerapplicatie.



Figuur 2: Mitz architectuur schematische weergave

De 2 hoofdprocessen die door Mitz ondersteund worden voor het vastleggen van toestemmingskeuzes zijn:

1. Een patiënt krijgt de mogelijkheid om waar dan ook (dus ook thuis of bij de zorgaanbieder) toestemmingen te registreren voor de elektronische uitwisseling van zijn gegevens, waarbij een (dossierhoudende) zorgaanbieder gegevens deelt met een (raadplegende) zorgverlener. Iedere patiënt krijgt hierdoor de mogelijkheid om 'proactief' toestemmingen vast te leggen via de TAP (via een app op zijn mobiel, een patiëntenportaal of een website).

2. Een patiënt stelt een hulpvraag aan een zorgverlener en die zorgverlener heeft vervolgens gegevens nodig van een andere zorgaanbieder, terwijl de patiënt nog geen toestemming daarvoor geregistreerd heeft.
   De patiënt doet dat ter plekke alsnog (al dan niet via de zorgverlener of een baliemedewerker bij de zorgaanbieder) en de betreffende gegevens worden door de betreffende (dossierhoudende) zorgaanbieders *meteen* gedeeld, zodat de behandelende zorgverlener de gegevens direct tijdens het consult kan raadplegen.

Een patiënt zit in de gebruikersrol op het moment van gebruik van de TAP. Hij gebruikt dan de Mitz-faciliteiten om een toestemmingskeuze te registreren, wijzigen of verwijderen.
Een dossierhoudende zorgaanbieder (die via een uitwisselingssysteem op Mitz aangesloten is) zit in de gebruikersrol op het moment van dossiervoering.
Een raadplegende zorgverlener (die via een uitwisselingssysteem op Mitz aangesloten is) zit in de gebruikersrol op het moment van behandeling waarbij aanvullende gegevens van andere zorgaanbieders nodig zijn.

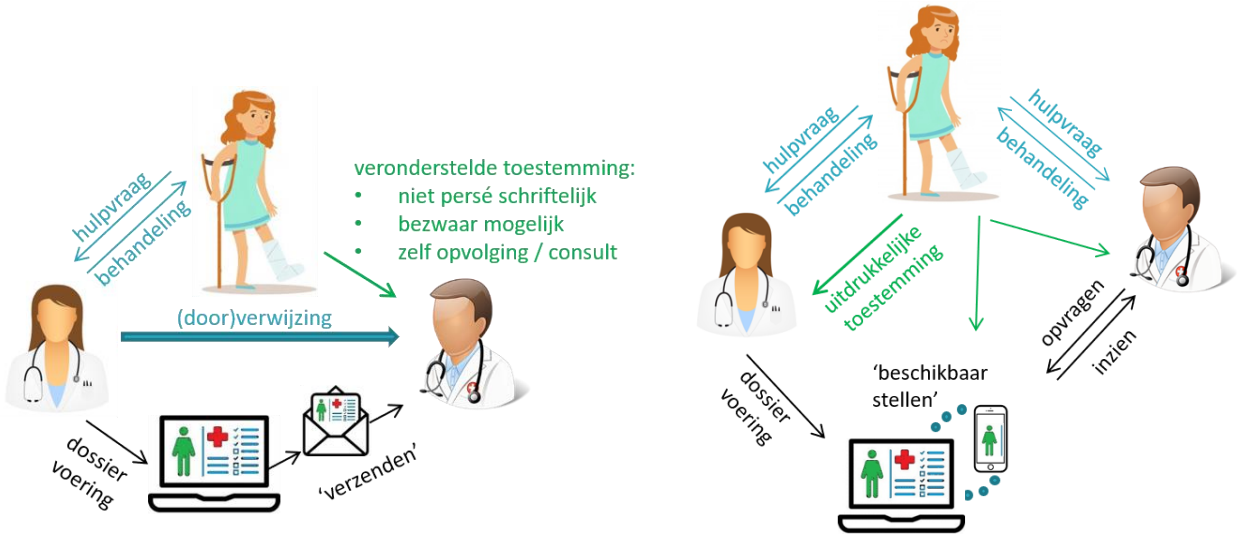
Bij opvraging via een US dat aangesloten is op Mitz, mag de raadplegende zorgverlener er van uitgaan dat eerst vastgesteld wordt of de patiënt uitdrukkelijk toestemming heeft gegeven, alvorens de gegevens bij andere zorgaanbieders (al dan niet via een index) worden opgevraagd.

In alle gevallen, maar zeker als de patiënt bij een raadplegende zorgaanbieder is, is het van belang dat een toestemmingskeuze direct na registratie (of wijziging of intrekking) effect heeft. Dat houdt in dat een patiënt die via een app of een website toestemming geeft om gegevens te delen, er van uit mag gaan dat de dossierhoudende zorgaanbieder(s) de betreffende gegevens direct deelt als een raadplegende zorgaanbieder daarom vraagt[2]. Als de dossierhoudende zorgaanbieder op dat moment niet in de zorginstelling aanwezig is, bijvoorbeeld in de 'avond / nacht / weekend' (ANW) of tijdens vakantie, is het uitgangspunt om de systemen zodanig in te richten dat de toestemmingskeuzes automatisch worden verwerkt, rekening houdend met de belangen en verantwoordelijkheden van de betrokken mensen. Cruciaal is dat alle betrokken personen een gemeenschappelijke set van afspraken omarmen, zodat het vertrouwen in de zorgvuldige en correcte wijze waarop iedereen te werk gaat, er altijd is.

4.4.2 Toepassingsgebied

In Mitz kunnen patiënten zowel toestemmingen (toestemmingskeuze = 'ja') en bezwaren (toestemmingskeuze = 'nee') vastleggen. De toestemmingen zijn noodzakelijk voor uitwisselingen die een uitdrukkelijke toestemming als grondslag hebben. De bezwaren moeten gehonoreerd worden bij een gegevensuitwisseling op grond van een veronderstelde toestemming. Artikel 15a lid 1 van de Wabvpz geeft aan dat het elektronisch beschikbaar stellen van medische gegevens in ieder valt onder de uitwisselingen waar een uitdrukkelijke toestemming voor vereist is (zie ook figuur 3).
In de discussie en interpretatie hierover hanteert men soms de vuistregel: push (verzenden) vereist geen toestemming en pull (opvragen) wel. Dat dient echter op 2 aspecten genuanceerd te worden. In de eerste plaats gaat het bij push ook om een toestemming, alleen die mag verondersteld worden, tenzij de patiënt bezwaar heeft kunnen maken en daarvan geen gebruik heeft gemaakt. In de tweede plaats moet de term push en pull bij een interpretatie van de wet juridisch worden beschouwd en niet technisch. Zo kan een juridische push technisch worden uitgevoerd als een push of als een pull (bijvoorbeeld ophalen uit een mailbox) en kan een juridische pull technisch worden uitgevoerd als een technische pull of als een push (bijvoorbeeld het geautomatiseerd updaten van een eerdere oplevering). Als gegevens (technisch) beschikbaar worden gesteld en op dat moment is niet bekend aan welke individuele zorgaanbieder beschikbaar wordt gesteld, dan is er sprake van een (juridisch) beschikbaar stellen zoals bedoeld in het wetsartikel. Als gegevens (technisch) beschikbaar worden gesteld aan een zorgaanbieder die met de patiënt besproken is en waar geen bezwaar tegen is gemaakt, dan betreft dat geen (juridische) beschikbaar stelling. We kunnen dit onderscheid aanduiden als het 'gericht' of 'ongericht' beschikbaar stellen van gegevens.
NB Dit dient niet verward te worden met gericht of ongericht bevragen, want dat is vanuit de raadpleger geredeneerd en hier gaat het om de toestemming aan de bron (dossierhouder).

[2] De zorgaanbieder kan hierop een uitzondering maken per patiënt.



Figuur 3: Verzenden met veronderstelde en beschikbaar stellen met uitdrukkelijke toestemming

De Mitz-*processen* waarbij gegevens van de stakeholders verwerkt worden zijn:

1. Registratie van zorgaanbieders en zorgverleners in een zorgaanbiederadresboek, zodat een patiënt die een individuele toestemmingskeuze wil registreren, de zorgaanbieder kan opzoeken en selecteren.
2. Registratie van een toestemmingskeuzes op basis van een uniek nummer van de patiënt.
3. Communicatie naar de (dossierhoudende) zorgaanbieders wanneer er toestemmingkeuzes zijn geregistreerd of gewijzigd.
4. Raadplegen van Mitz ten behoeve van een specifieke uitwisseling, waarbij raadpleger-identificatie (UZI), patiënt identificatie, en daarnaast gegevenscategorie uitgewisseld worden om daarmee een antwoord van Mitz te verkrijgen op basis van de geregistreerde toestemmingskeuzes.
5. Communicatie naar de patiënt wanneer te notificeren gebeurtenissen hebben plaatsgevonden.

4.4.3 Verantwoordelijkheden

Verantwoordelijkheid patiënt
Toestemmingskeuzes worden door de patiënt geregistreerd, gewijzigd of verwijderd. De patiënt is in de regie als het gaat om dit '*beheer van toestemmingen*'. Om bij elektronische uitwisseling te kunnen vaststellen of er uitdrukkelijke toestemming is gegeven, dienen de toestemmingskeuzes elektronisch beschikbaar / raadpleegbaar te zijn.
Het elektronisch registreren, wijzigen en verwijderen van toestemmingskeuzes is een verantwoordelijkheid van de patiënt, en deze verantwoordelijkheid kan door de patiënt zelf en/of diens vertegenwoordiger worden uitgevoerd.

De toestemmingsverlening vindt plaats door de patiënt zelf, zijn wettelijke vertegenwoordiger (bijvoorbeeld ouder / voogd bij kinderen of aangewezen personen bij 'onder-curatele-gestelden' of 'wilsonbekwamen') of door de patiënt gemandateerden (bijvoorbeeld een mantelzorger) of, in bepaalde situaties, kan een bekende zorgverlener de uitvoering namens de patiënt ter hand nemen.

Verantwoordelijkheid zorgaanbieder
Het beheer van de *geregistreerde* toestemmingen (in de papieren wereld: het beheer van de toestemmingsformulieren) is een verantwoordelijkheid van de (dossierhoudende) zorgaanbieder[3].

4.4.4 Ruimte voor (regionale) ontwikkelingen

Nieuwe uitwisselingen die nog geen landelijke dekking hebben, en nog niet gevat zijn in een landelijke toestemmingsmogelijkheid van Mitz, kunnen hun toestemmingsvraagstukken desgewenst op eigen wijze organiseren.

Hierdoor blijft er ruimte voor nieuwe (regionale) ontwikkelingen, vernieuwingen en uitbreidingen. Dit betekent dat naast de landelijke toestemmingsvoorziening (Mitz) ook regionale toestemmingsvoorzieningen kunnen bestaan. Dat wil zeggen: voor de landelijk afgestemde elektronische uitwisselingen tussen zorgaanbieders zal er een landelijke aanpak zijn, aangevuld met de mogelijkheden om in kleiner verband te werken met aanvullende toestemmingen, indien deze toestemmingen landelijk

(nog) niet geregistreerd kunnen worden. Deze moeten in later stadium wel gemigreerd kunnen worden naar het landelijke toestemmingsregister.

4.5 Beoogde werking Mitz-componenten

4.5.1 Toestemmingsapplicatie

Met Mitz krijgt de patiënt de mogelijkheid om via een toestemmingsapplicatie TAP (website en mobile app) toestemmingskeuzes te registreren (en te wijzigen en te verwijderen) voor elektronische gegevensuitwisselingen tussen zorgaanbieders die via een US verlopen, zodanig dat deze waar mogelijk direct effect hebben, dus zonder handmatige acties van de zorgaanbieder.

Om de patiënt de mogelijkheid te geven een toestemmingskeuze op een eenduidige manier te registreren (of te wijzigen, of te verwijderen), zal Mitz de TAP als een responsive webpagina opleveren.
De TAP kan niet alleen rechtstreeks door de patiënt worden benaderd, maar de patiënt kan ook via een link op een bestaande website, bijvoorbeeld een patiëntportaal, de Mitz responsive webpagina benaderen om toestemmingskeuzes vast te leggen.
Elke online-omgeving waarin het relevant kan zijn voor de patiënt om zijn / haar toestemmingskeuzes vast te leggen, kan deze link gebruiken. Leveranciers (bijvoorbeeld van informatiezuilen, patiëntportalen of van PGO's) kunnen de link naar de (responsive) webpagina opnemen in hun eigen systemen en webpagina's. Op deze link zal, waar mogelijk, DigiD eenmalig inloggen van toepassing zijn indien de patiënt inlogt.

Zorgverleners kunnen desgewenst ook toestemming vastleggen namens de patiënt. Dat is handig voor patiënten die geen digitale middelen gebruiken, maar ook om bij toestemmingen die de patiënt nog niet had vastgelegd, toch gegevens op te kunnen vragen. Wanneer de patiënt onder behandeling is van een zorgaanbieder die gegevens van een andere zorgaanbieder nodig heeft, is het ontbreken van een toestemming om die bron te ontsluiten vaak een barrière voor de uitwisseling. Met Mitz kan er 'ad-hoc' toestemming worden gegeven en geëffectueerd. De toestemming die een (raadplegende) zorgverlener registreert in opdracht van de patiënt, wordt onder water zodanig cryptografisch bewerkt, dat het systeem van de (dossierhoudende) zorgaanbieder met zekerheid kan vaststellen dat er uitdrukkelijke toestemming is van de patiënt om gegevens te delen. De functie 'zorgaanbieder namens patiënt' kan ingebouwd worden in een zorgaanbiedersysteem en dan kunnen zorgverleners, na het selecteren van een patiënt, 'met één druk op een knop' naar de Mitz toestemmingsapplicatie worden gebracht. Deze 'secure link' naar Mitz maakt onder water gebruik van tokens die (van tevoren eenmalig) met een Uzi-pas zijn ondertekend. Zo kunnen medewerkers die geen UZI-pas hebben, zich laten mandateren en dan op basis van de interne authenticatiemiddelen toegang krijgen tot Mitz. De onweerlegbaarheid van auteur, verantwoordelijke en patiënt wordt cryptografisch geborgd door gebruik te maken van drie tokens.
Het mandaattoken en het inschrijftoken worden eenmalig met de UZI-pas van bijvoorbeeld een verantwoordelijke zorgverlener ondertekend. Het transactietoken bevat de URA van de zorgaanbieder en wordt door de systemen gebruikt voor het opzetten van een beveiligde verbinding met Mitz (vandaar 'secure link'). Voor een medewerker die wil inloggen op Mitz, gebeurt de token-afhandeling onzichtbaar 'achter de schermen'. De patiënt wordt geïnformeerd over alle toestemmingskeuzes die door een zorgverlener of medewerker worden vastgelegd. Indien patiënten dat wensen en (laten) instellen, kunnen ze hier ook elke keer per mail een notificatie over ontvangen.

Het programma OTV ontwikkelt een responsive website met bijbehorende logica en een mobiele app met als doel dat 80% van de beoogde doelgroep er mee kan werken. In tegenstelling tot de huidige praktijk waar zorgaanbieders werken met een toestemmingsformulier, hoeven zorgaanbieders dat dan niet meer te doen.

- *NB1*: de patiënttoestemming in Mitz overrulet niet het medisch autorisatieprotocol (MAP) (dat zou een patiënttoestemming in MedMij via een PGO wel kunnen). Dus als de MAP van het LSP niet ondersteunt dat een tandarts medicatie kan inzien, verandert dat niet als een patiënt in Mitz toestemming geeft aan apothekers om alle medicijninformatie aan alle zorgaanbieders ter beschikking te stellen.
- *NB2*: De gegevenscategorieën die in Mitz aan de patiënt worden getoond bij het registreren van een toestemming, moeten te mappen zijn op de gegevenscategorieën van het US. Als die mapping niet 1:1 is te maken, zullen de consequenties per toestemmingsmogelijkheid of per uitwisseling bepaald worden.
- *NB3*: De smartphone app en de website voor de patiënt zullen gefinetuned worden op gebruiksvriendelijkheid voor de patiënten, zodat de adoptiegraad van het toestemmingsmiddel optimaal is en voor een groter maatschappelijk draagvlak zorgt, zodat de beoogde toename in regiemogelijkheden ook daadwerkelijk gerealiseerd wordt. Functies als machtigen en het gebruik van QR-codes kunnen het beheer van toestemmingen nog makkelijker maken.

Kind / Ouder relaties
Bij het inloggen met DigiD komt wel een BSN maar niet een geboortedatum mee. Daarom wordt aan de ingelogde persoon gevraagd om een leeftijdscategorie vast te leggen. Indien een minderjarige < 16 jaar zijn/haar toestemmingskeuzes zelf vastlegt via DigiD, dienen deze toestemmingskeuzes bevestigd te worden door een ouder/voogd (wettelijk vertegenwoordiger) met een gezagsrelatie. De TAP biedt daarom de mogelijkheid om de opgegeven toestemmingkeuzes te laten bevestigen door de ouder. Technisch wordt dit gerealiseerd middels een koppelcode. Om de toestemmingkeuzes te kunnen bevestigen, logt de ouder/voogd met eigen DigiD in op de TAP en vult de ontvangen koppelcode in. Hierna krijgt de ouder/voogd de mogelijkheid om de toestemmingkeuzes te beoordelen (goed te keuren of af te keuren).
Indien de zorgverlener toestemmingskeuzes vastlegt voor een kind <16j, wordt de koppelcode niet gebruikt. In principe kan worden uitgegaan van de aanwezigheid van een persoon met ouderlijk gezag die mondeling de toestemmingskeuzes van het kind bepaalt (onder de 12 jaar) of bevestigt (12 tot en met 15 jaar). Een ouder/voogd die reclameert, zal zich moeten wenden tot de zorgverlener die de toestemmingskeuzes voor het kind heeft geregistreerd.
Op basis van een geverifieerde geboortedatum van een dossierhoudende zorgaanbieder, kan Mitz vaststellen dat de leeftijdscategorie van een patiënt aangepast moet worden. Indien een leeftijdscategorie aangepast wordt van >=16 jaar naar <16 jaar, wordt contact opgenomen met de betrokkenen om de vastgelegde toestemmingen alsnog te voorzien van een ouderlijke beoordeling.

De *toestemmingsmogelijkheden* in Mitz kunnen breder zijn dan de behandelrelaties die een patiënt heeft, Dus als de patiënt toestemming geeft aan zorgaanbieders, dan betekent dat niet dat de patiënt onder behandeling is van die zorgaanbieder. Mitz bevat geen behandelrelatieregistratie.

Het *uitwisselen van gegevens* blijft te allen tijde wel voorbehouden aan behandelaars (en de door hen gemachtigde medewerkers) en uitsluitend in het kader van een behandelrelatie. Dit wordt vereist vanuit de wet en alle uitwisselingssystemen die op Mitz aansluiten moeten hier aan voldoen.

4.5.2 Het toestemmingsregister

Het toestemmingsregister bevat de door de patiënt (of diens vertegenwoordiger) geregistreerde toestemmingskeuzes welke per patiënt worden opgeslagen. Voor alle vormen van toestemmingsmogelijkheden die landelijk zijn bepaald en vastgelegd in de toestemmingscatalogus, worden de toestemmingskeuzes van de patiënt vastgelegd in het bij de patiënt behorende toestemmingsprofiel in het toestemmingsregister.

Voor toestemmingsmogelijkheden waarvoor (nog) geen landelijke afspraken zijn vastgelegd in de toestemmingscatalogus, kunnen, zoals eerder genoemd, op lokaal niveau decentrale toestemmingsregisters worden bijgehouden door decentrale uitwisselingssystemen.

Het toestemmingsregister moet door de aangesloten uitwisselingssystemen geraadpleegd worden.

Toestemmingsprofiel
Met een toestemmingsprofiel wordt bedoeld: de registratie van toestemmingskeuzes van één specifieke patiënt zodanig dat bij elektronische gegevensuitwisseling gecontroleerd kan worden of de opgeslagen medische gegevens van een ‘dossierhoudende’ zorgaanbieder gedeeld mogen worden met een ‘raadplegende’ zorgverlener.

Het toestemmingsprofiel bevat de toestemmingskeuzes van een patiënt op actuele toestemmingsmogelijkheden en is opgeslagen in het toestemmingsregister. De toestemmingskeuzes (en dus de toestemmingsmogelijkheden) moeten invulling geven aan de wetsartikelen waar het recht voor de patiënt op het registreren (en wijzigen en verwijderen) van toestemmingen is beschreven.

Deze vorm van toestemming doet niets af aan het recht dat een patiënt heeft om delen van het dossier af te schermen voor uitwisseling bij de zorgverlener die het dossier heeft opgeslagen. Zo kan een patiënt een bepaald medicijn of een episode in het dossier bij de huisarts of een volledige laborder blokkeren voor elektronische uitwisseling. Dit afschermen van delen van het dossier vindt bij de dossierhoudende zorgverlener zelf plaats en niet in het Mitz toestemmingsprofiel. Als patiënt wil je in dergelijke situaties immers dat dat ene gegeven alleen bij de betreffende arts bekend is, en ook niet in een toestemmingsprofiel benoemd wordt als zijnde ‘geblokkeerd’. Ook is het bij het blokkeren van een enkel gegeven van belang dat de zorgaanbieder de patiënt kan wijzen op de (mogelijke negatieve) impact die het heeft voor de continuïteit van de zorgverlening.

Aan het toestemmingsregister kunnen door US'en twee soorten vragen worden gesteld:

1) De gesloten autorisatievraag:
   Deze vraag wordt namens de dossierhoudende zorgaanbieder aan Mitz gesteld en geeft antwoord op de vraag of een door een zorgverlener gestelde vraag mag worden beantwoord door het betreffende systeem.
2) De open autorisatievraag:
   Deze vraag wordt aan Mitz gesteld namens raadplegende zorgverleners en geeft antwoord op de vraag welke systemen geraadpleegd mogen en kunnen (als filter om hele lange lijsten te voorkomen) worden voor één of meer gegevenscategorieën (bijvoorbeeld nodig wanneer een US geen index heeft waarin de dossierhoudende zorgaanbieders te vinden zijn).

4.5.3 Het toestemmingsabonnementenregister

Naast het toestemmingsregister is er ook een toestemmingsabonnementenregister. Er zijn verschillende redenen waarom dit toestemmingsabonnementenregister nodig is:

- Om zorgaanbieders in staat te stellen genotificeerd te worden zodra één van hun patiënten toestemmingskeuzes aan hem / haar als dossierhouder heeft bepaald. Met deze notificatie weet een zorgaanbieder dat de patiënt al een toestemmingskeuze in Mitz heeft vastgelegd en hoeft de patiënt niet opnieuw gewezen te worden op Mitz.
- Om (in het kader van ondubbelzinnigheid) een toestemming aan een 'categorie zorgaanbieders' te kunnen vertalen in een concrete opsomming van dossierhouders die op dat moment toestemming hebben gekregen (indien dit via een open autorisatievraag aan Mitz wordt gevraagd);
- Om zojuist geregistreerde toestemmingen direct te (kunnen) effectueren bij zorgaanbieders (indien ze aangesloten zijn op uitwisselingssystemen die als gegevensverwerkingsverantwoordelijke werken met een eigen index).
  Deze uitwisselingssystemen mogen ze pas gegevens verwerken na toestemming van de patiënt. Die kan weliswaar via Mitz verkregen worden, maar pas daarna mag de index worden bijgewerkt.
- Om (in het kader van gebruiksgemak en als onderdeel van privacy wetgeving) aan patiënten te kunnen tonen welke zorgaanbieders zich geabonneerd hebben op toestemmingswijzigingen.

Omwille van deze redenen kunnen dossierhoudende zorgaanbieders zich, onder eigen verantwoordelijkheid (binnen een verwerkersrelatie met Mitz), abonneren op (wijzigingen in de) toestemmingen van de patiënten die bij hen ingeschreven worden met het doel om genotificeerd te kunnen worden. Zodra een patiënt iets wijzigt in het toestemmingsprofiel met betrekking tot deze (dossierhoudende) zorgaanbieder, zal Mitz deze zorgaanbieder notificeren (feitelijk en juridisch: in opdracht van die zorgaanbieder zelf). Het notificeren door Mitz vindt derhalve ook plaats onder verantwoordelijkheid van de zorgaanbieder.

4.5.4 De beheerapplicatie

De beheerapplicatie is de applicatie waarmee de beheerorganisatie de verschillende onderdelen van Mitz kan beheren.

4.5.5 De toestemmingscatalogus

De toestemmingscatalogus definieert welke toestemmingsmogelijkheden er zijn. Alle toestemmingsmogelijkheden hebben de onderstaande structuur:

Figuur 4: Structuur van een toestemming

Zorgaanbiedercategorieën

Een toestemming voor het elektronisch uitwisselen van medische gegevens moet gegeven worden aan de dossierhoudende zorgaanbieder, want

- als er sprake is van het doorbreken van het beroepsgeheim (conform bijvoorbeeld WGBO) dan betreft dat het delen van medische gegevens uit het dossier door de dossierhouder;
- als er sprake is van het beschikbaarstellen van gegevens via een elektronisch uitwisselingssysteem aan andere zorgaanbieders, dan dient de dossierhouder (conform de Wabvpz) vast te stellen of er uitdrukkelijk toestemming is verleend.
- als er sprake is van toestemming als grondslag voor het aanleveren van medische gegevens (conform AVG: verwerking van bijzondere persoonsgegevens), dient de dossierhouder er voor te zorgen dat de toestemming rechtmatig is (dat wil zeggen voldoet aan de eisen uit de AVG). Zie het Juridisch Kennisdocument voor meer uitleg bij deze 3 redenen.

Daarom begint de structuur van een toestemmingsmogelijkheid met de zorgaanbieder die verantwoordelijk is voor de dossiervoering. Dat kan een individuele zorgaanbieder zijn (bv. de eigen huisarts), maar ook een categorie (bv. alle apothekers). In de uitwisselingen wordt gebruik gemaakt van de (meer dan 70) categorieën van ZorgKaart Nederland. In de toestemmingsmogelijkheden zoals ze aan de patiënt worden getoond, kunnen deze categorieën gebundeld worden om te voorkomen dat de patiënt te veel keuzes moet maken. De individuele zorgaanbieders kunnen worden gezocht via een zorgaanbiedersadresboek.

Gegevenscategorieën

Om zo specifiek mogelijk toestemming te geven, is de set van gegevens die uitgewisseld mogen worden, onderdeel van de structuur van de toestemmingsmogelijkheid. Van belang bij de bepaling van 'bepaalde' gegevens zijn de volgende uitgangpunten:

1. de gegevenscategorie die aan de patiënt getoond wordt kan niet fijnmaziger zijn dan de uitwisselingen zelf. Immers, als de patiënt in Mitz een keuze kan maken voor twee gegevenscategorieën, die in de praktijk als één gegevensset worden uitgewisseld, dan kan hij tegen de ene 'ja' zeggen en tegen de andere 'nee' en dan is onduidelijk wat er moet gebeuren.
2. conform het vertrouwensmodel mogen medische gegevens alleen maar uitgewisseld worden als er in de uitwisseling geborgd is dat voldaan is aan de eis 'indien relevant en noodzakelijk' (zie paragraaf 4.2.1 Vertrouwensmodel). Dus ook al geeft de patiënt in Mitz toestemming aan alle huisartsen om alle gegevens uit te wisselen, dan zal het filter van de richtlijnen die de beroepsgroepen onderling hebben opgesteld van kracht blijven. Een toestemming in Mitz overrulet dus niet de zorgvuldig afgestemde informatiestandaarden voor gegevensuitwisseling tussen zorgaanbieders.
3. Indien patiënten bepaalde elementen uit het dossier geheim willen houden, dat wil zeggen willen blokkeren van elektronische uitwisseling, kunnen ze dat met de zorgaanbieder die het betreffende dossier voert bespreken en dat kan in het betreffende systeem van de zorgaanbieder worden vastgelegd. Deze gegevens worden niet uitgewisseld, ook al heeft de patiënt in Mitz toestemming gegeven voor de uitwisseling van 'alle gegevens'.
4. Omdat uitwisselingssystemen eigen procedures hebben om gegevens te filteren conform beroepsrichtlijnen, zal er bij aansluiting van een uitwisselingssysteem op Mitz een vertaaltabel worden afgesproken om de gegevenssets van een uitwisselingssysteem te mappen op de gegevenscategorieën van Mitz.

Raadplegerscategorieën

Om aan te kunnen geven aan wie jouw dossiergegevens opgeleverd mogen worden, zijn de raadplegers ook onderdeel van de structuur van de toestemmingsmogelijkheid. Een patiënt kan desgewenst specificeren met wie gegevens gedeeld mogen worden. Raadplegende zorgverleners (of de gemandateerde medewerkers) werken in een instelling (zorgaanbieder) en zij hebben een specialisme (beroepsgroep). De zorgaanbieder waar de raadplegende zorgverlener werkt is voor de toestemming van belang. De beroepsgroep van de raadplegende zorgverlener is voor de dataminimalisatie en proportionaliteit van de gegevens van belang (zie gegevensfilter in bovenstaande paragraaf). Bij het raadplegen vanuit een grote zorginstelling kunnen veel verschillende beroepsgroepen betrokken zijn en worden de raadplegers niet als instelling, maar op basis van de zorgaanbiedercategorie van de verantwoordelijke behandelaar gecategoriseerd.
Daarbij gelden de volgende overwegingen:

- Om te voorkomen dat de patiënt per raadplegende instelling toestemming moet geven, wordt gebruik gemaakt van categorieën van (raadplegende) zorgaanbieders. Omdat iedere zorgaanbieder volgens de Zorgkaart Nederland is ingedeeld in een categorie, kan Mitz een voor de patiënt begrijpelijke zorgsector aanbieden in de toestemmingsvraag.

Door een vertaaltabel te gebruiken, wordt de zorgaanbiedercategorie van een raadplegende zorgaanbieder vertaald naar de zorgsector waar de patiënt een toestemmingskeuze voor heeft vastgelegd.

- Een raadplegende zorgverlener die bijvoorbeeld vanuit een ziekenhuis gegevens opvraagt, kan deze binnen het ziekenhuis delen met iedereen die bij die behandeling betrokken is. Voor de patiënt is het dus relevant om raadpleging vanuit een instelling toe te staan of te blokkeren. Het is niet nodig en niet wenselijk om voor alle beroepsgroepen die binnen een instelling werkzaam kunnen zijn apart toestemming of bezwaar te regelen. Wel moet er vertrouwen zijn dat technisch geborgd is dat de beroepsrichtlijnen zijn gevolgd, dus dat bijvoorbeeld een behandelaar in een apotheek andere gegevens te zien krijgt dan een behandelaar op een huisartsenpost. En dat er bijvoorbeeld binnen een ziekenhuis een 'role-based-access-control' mechanisme geïmplementeerd is waardoor medewerkers afhankelijk van hun rol (BIG code) bepaalde gegevens kunnen inzien of juist niet kunnen inzien.

In de elektronische uitwisseling wordt er gebruik gemaakt van landelijk beheerde registers (voor zorgaanbieders en beroepsgroepen) en Mitz vertaalt deze naar categorieën die begrijpelijk zijn voor de patiënt. In de toestemmingscatalogus staan de toestemmingsmogelijkheden die dekkend zijn voor de gegevensuitwisselingen die nu en binnen 12 maanden operationeel zijn.

De toestemmingscatalogus bevat onder andere registers voor:

- Zorgaanbiederscategorieën (samengesteld op basis van ZorgKaart Nederland)
- Gegevenscategorieën (te mappen op de gegevenssets die uitgewisseld kunnen worden)
- Toestemmingsmogelijkheden (samengesteld op basis van bovenstaande categorieën)
- Vertaaltabellen (nodig om de Mitz categorieën te mappen op de landelijke registers)

Het Zorgadresboek (ZORG-AB) wordt gebruikt om individuele zorgaanbieders te kunnen opzoeken en de categorie te kunnen bepalen. De Patiëntenfederatie heeft alle zorgaanbieders in Nederland, op basis van ZorgKaart Nederland categorieën, ingedeeld in voor patiënt begrijpelijke categorieën. In een samenwerking met Vektis wordt gecontroleerd of de categorie overeenkomt met het zorgaanbod dat de zorgaanbieder aanbiedt. De categorie van een zorgaanbieder is voor iedereen transparant en kan niet zomaar worden aangepast.

De elektronische gegevensuitwisselingen tussen zorgaanbieders, waar Mitz de toestemmingkeuzes voor faciliteert, hebben een welomschreven doel, namelijk het faciliteren van een kwalitatief goede behandeling, conform de richtlijnen die de beroepsgroep heeft opgesteld. Dat doel geldt voor alle toestemmingsmogelijkheden.

Voor elk van de toestemmingsmogelijkheden afzonderlijk, of voor 'alle' mogelijkheden die getoond worden, kan een patiënt een keuze vastleggen of wijzigen of verwijderen.

Voor de toestemmingscatalogus gelden de volgende uitgangspunten:

- Op basis van de registers in de toestemmingscatalogus is het mogelijk om een (eindige) lijst met zorgaanbiederscategorieën en gegevenscategorieën te tonen, die de betekenis van 'alle' kan laten zien.
- De inhoud van nieuwe toestemmingsmogelijkheden wordt bepaald in onderling overleg tussen de koepels van zorgaanbieders en patiëntvertegenwoordigers.
- Ook wanneer de patiënt 'alle' toestemmingsmogelijkheden heeft gekozen, zullen toestemmingsmogelijkheden die daarna nieuw worden toegevoegd op 'onbeantwoord' blijven staan, totdat de patiënt hier ook een keuze voor registreert.
- Op de koppelvlakken met Mitz wordt gebruik gemaakt van de landelijke registers van zorgaanbieders en beroepsgroepen. Mitz verzorgt de mapping (aggregatie) naar de categorieën die Mitz hanteert voor de toestemmingsregistratie.
- In Mitz kan de patiënt ook aangeven of gegevens uitgewisseld mogen worden in spoed situaties. Indien de patiënt een zorgaanbieder toestemming geeft om gegevens te delen, geldt dat ook in spoed situaties. Als een patiënt geen toestemming geeft (toestemmingskeuze='nee') wordt de patiënt gewezen op de mogelijkheid om voor spoed situatie een uitzondering te maken. In een levensbedreigende situatie waarin er geen mogelijkheid is om toestemming te regelen (bijvoorbeeld omdat de patiënt niet aanspreekbaar is) moet er met spoed gehandeld kunnen worden en moet de juiste informatie op dat moment en op die plek beschikbaar zijn. Daarvoor kan een patiënt in Mitz van tevoren een toestemming vastleggen. Indien de patiënt voor spoed situaties een keuze registreert, zal Mitz deze keuze toepassen op de toestemmingsmogelijkheden die relevant zijn voor spoedzorg. Deze lijst van toestemmingsmogelijkheden voor spoed situaties, wordt in de toestemmingscatalogus onderhouden. Met één toestemmingskeuze voor spoedsituaties wordt de 'spoed-toestemming' alleen voor deze toestemmingsmogelijkheden vastgelegd.

- Het beheer van de toestemmingscatalogus wordt geborgd als een doorlopende activiteit in de beheerorganisatie van Mitz. De mapping van de gegevenscategorieën die door een US worden ondersteund, zullen (in afstemming met Mitz) door een US gemapt moeten worden op de gegevenscategorieën van Mitz.
- In feite is de toestemmingscatalogus een (interne) 'Mitz informatie faciliteit'. De actuele toestemmingsmogelijkheden zijn beschikbaar voor en worden gebruikt door het toestemmingsregister en voor de toestemminsapplicatie.

4.6 Beoogde werking Mitz via uitwisselingssystemen

Zorgaanbieders wisselen gegevens uit via uitwisselingssystemen (US). In (de frontend van) Mitz worden toestemmingen vastgelegd voor het delen van gegevens via uitwisselingssystemen. Het vaststellen of er toestemming is verleend t.b.v. een specifieke uitwisseling kan technisch gerealiseerd worden via een koppeling van een uitwisselingssysteem op (de backend van) Mitz. Vanuit beheer oogpunt is de koppeling met Mitz vanuit een uitwisselingssysteem te verkiezen boven aansluiting van alle zorgaanbieders op Mitz. Daar komt bij dat bestaande uitwisselingen verschillend zijn ingericht en er verschillende afspraken gemaakt kunnen zijn met de zorgaanbieders die op een uitwisselingssysteem zijn aangesloten. De wijze waarop een zorgaanbiedersysteem omgaat met functionaliteit die Mitz biedt, kan per uitwisselingssysteem verschillen. Omdat ook de bestaande uitwisselingen moeten kunnen aansluiten op Mitz wordt hier rekening mee gehouden. Door Mitz te koppelen met een uitwisselingssysteem en niet met zorgaanbiedersystemen kunnen bestaande uitwisselingen vrijwel intact blijven en houdt iedere partij de ruimte om de uitwisseling volgens eigen afspraken in te richten. Het landelijke toestemmingsregister van Mitz kan (ook door één zorgaanbieder) worden geraadpleegd door verschillende uitwisselingssystemen, bijvoorbeeld door het LSP of door regionale 'Cross-enterprise Document sharing' (XDS-)netwerken. Hiervoor zijn koppelingen ontwikkeld op basis van open standaarden, die door ieder US dat daarvoor geaccepteerd is, gebruikt kan worden. Een US kan desgewenst ook een eigen lokaal toestemmingsregister bijhouden, voor de toestemmingsmogelijkheden waarvoor (nog) geen landelijke afspraken zijn vastgelegd in de toestemmingscatalogus.

4.6.1 Omgang toestemmingen: Zorgaanbieders versus Zorgverleners

Er wordt onderscheid gemaakt tussen zorgaanbieders die dossiers voeren (en gegevens kunnen versturen of kunnen delen) en de zorgverleners die raadplegen (en op basis van hun beroep bepaalde gegevens in mogen zien).
Elke zorgaanbieder kan beide rollen hebben, maar per gegevensuitwisseling heeft iedereen maar één rol:

- De dossierhoudende zorgaanbieder is een zorginstelling of een solo-werkende zorgverlener. Die is verantwoordelijk voor de kwaliteit van de zorgverlening. Het voeren van een dossier en het beschermen van de dossiergegevens hoort bij de dossierhoudende rol van een zorgaanbieder. Voor de elektronische identificatie van zorgaanbieders wordt het landelijke URA nummer gebruikt. Het URA register wordt door CIBG beheerd.
- De raadplegende zorgverlener is een individuele behandelaar met een geregistreerde beroepsgroep. In het BIG-register worden zorgverleners geregistreerd en in het UZI-register wordt de geregistreerde beroepsgroep beschikbaar gemaakt voor elektronische communicatie.

4.6.2 Vaststellen toestemming door zorgaanbieders die gegevens delen met andere zorgaanbieders

Zorgaanbieders die moeten kunnen vaststellen of er toestemming is gegeven voor een specifieke gegevensuitwisseling, kunnen dit doen via Mitz. Dat gebeurt 'achter de schermen', dat wil zeggen: zorgaanbieders kunnen dit 'vaststellen' delegeren aan Mitz (via hun US dat op Mitz is aangesloten). Zorgaanbieders spreken af dat het uitwisselingssysteem dat de betreffende uitwisseling realiseert, eerst bij Mitz vaststelt of de betreffende toestemming geregistreerd is, voordat de gegevens worden uitgewisseld. In concreto: zorgaanbieders die een medisch dossier voeren van een bepaalde patiënt, kunnen via Mitz door hun systeem laten vaststellen of er 'uitdrukkelijke toestemming' is verleend voor bijvoorbeeld het 'delen' van alle of bepaalde gegevenscategorieën uit dat dossier door die patiënt.

Daarnaast gaat Mitz er van uit dat toestemmingen automatisch worden verwerkt, in de systemen, indien dat nodig is voor een goede werking van Mitz. Daarbij gaat het niet om een notificatie in een zorgaanbiedersysteem dat er toestemming is gegeven (dat mag een zorgaanbiedersysteem ondersteunen, maar het is niet nodig voor een goede werking van Mitz). Het gaat wel om de verwerking van een toestemming in uitwisselingssystemen die een interne (verwijs)index hebben die alleen op basis van een toestemming gevuld mag worden. Deze uitwisselingssystemen zullen de notificatie van een toestemmingswijziging zodanig moeten verwerken dat de index wordt bijgewerkt (al dan niet via het zorgaanbiedersysteem). Als een uitwisselingssysteem de notificatie van Mitz niet nodig heeft om de eigen index bij te werken, hoeft het 'automatisch aanmelden na notificatie' niet ondersteund te worden. Als het wel nodig is, moet het 'automatisch aanmelden na notificatie' wel ondersteund worden voor een goede werking van Mitz.

Uitgangspunt voor een goede werking van Mitz is immers het delen van medische gegevens waar en wanneer dit nodig is, en dat vereist dat een toestemming direct nadat deze is geregistreerd, gewijzigd of verwijderd ook effect heeft. Een geautomatiseerde aanmelding na een toestemming en een geautomatiseerde afmelding na een intrekking is dan de enige optie.
Wel kan een zorgverlener desgewenst van tevoren een lijst aanleggen met patiënten, die hiervan uitgezonderd zijn, indien het zorgaanbiedersysteem dit ondersteunt.

4.6.3 Vaststellen toestemming door zorgverleners die opvragen

De systemen van de zorgaanbieders worden voor het raadplegen van gegevens via elektronische uitwisselingssystemen aangesloten op Mitz. De toestemmingsraadpleging via Mitz verloopt dus niet rechtstreeks met systemen van zorgaanbieders en dat betekent dat er binnen Mitz geen index van aangesloten zorgaanbiedersystemen bijgehouden hoeft te worden.

De toestemmingsprofielen worden landelijk geregistreerd en leveren voor de aangesloten uitwisselingssystemen een 'ja' of 'nee' op als gevraagd wordt om de toestemming van de patiënt voor een elektronische gegevensuitwisseling.
De patiënt geeft dus toestemming voor een bepaalde gegevensuitwisseling, ongeacht het US dat die uitwisseling realiseert. Daarbij geldt de toestemming van de patiënt voor alle partijen in de uitwisselingsketen die verantwoordelijk zijn voor de gegevensverwerking van de uitwisseling.

4.7 Technische werking bij raadplegen toestemmingsregister

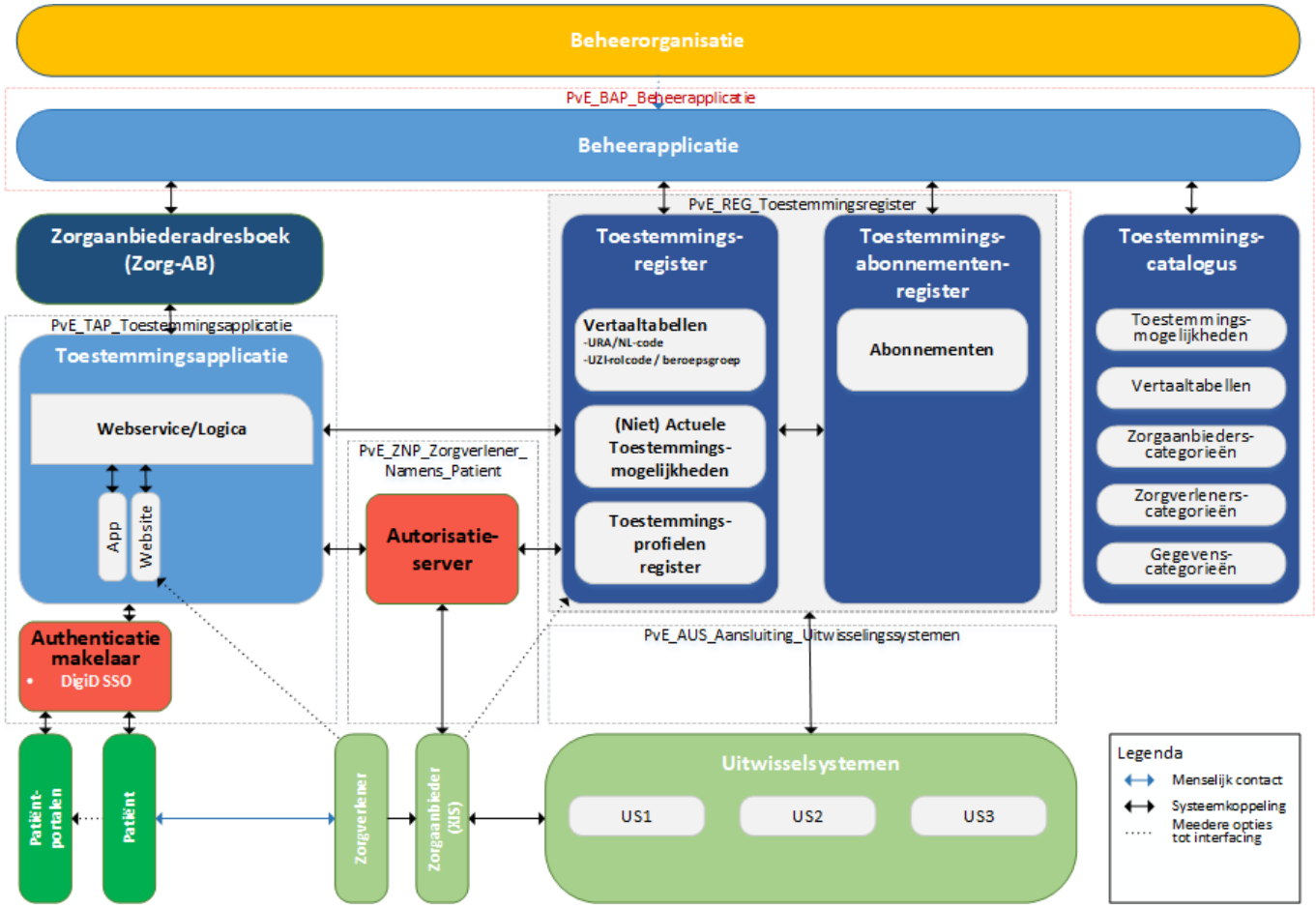
4.7.1 Integratiearchitectuur

Voorwaarde is dat de koppelvlakken waarop de componenten geïntegreerd worden tot een werkende keten, vanuit één architectuur benaderd worden. Deze architectuur wordt voor de koppelvlakken het meest concreet.
Op basis van de Project Start Architectuur (PSA), die tot en met het integratieperspectief is uitgewerkt, kunnen de specificaties voor de afzonderlijke componenten opgesteld worden. Deze "programma's van eisen" (PvE's) zijn onderdeel van de architectuur van Mitz (in TOGAF: 'requirements are core business') en vormen een uitwerking van de PSA (maar zijn zelf geen onderdeel van de PSA).

Op basis van de PvE's zal een leverancier van zo'n component een technisch ontwerp maken en aan de hand daarvan ontwerpen, programmeren of configureren, testen en onderhoud plegen. Voor de koppelvlakken tussen Mitz en uitwisselingssystemen geldt dat de specificaties zijn uitgewerkt tot in de technische details, omdat beide partijen precies dezelfde taal moeten spreken. De technische specificatie van de koppelvlakken is beschreven in 'implementatie handleidingen'.

Uitgangspunt: Mitz streeft naar het gebruik van open standaarden, omdat daardoor een open koppelvlak ontstaat waarop de leveranciers van uitwisselingssystemen die dat wensen, hun producten en diensten kunnen koppelen. Daarnaast zijn open standaarden van belang omdat componenten die al gebouwd en gebaseerd zijn op deze standaarden, hergebruikt kunnen worden en dat is efficiënter en goedkoper dan maatwerk ontwikkelen en bouwen. In die situatie zouden bijvoorbeeld bestaande internationale componenten 'slechts' geconfigureerd hoeven te worden voor de Nederlandse situatie, in plaats van volledig opnieuw geprogrammeerd.

De informatiestandaard van de koppelvlakken wordt zodanig gespecificeerd, dat leveranciers aan de zendende en ontvangende kant 'dezelfde taal' spreken. De juiste verwerking van deze 'informatie die over de lijn gaat' is geborgd in de afspraken en eisen die in de PSA en de PvE's beschreven zijn.



Figuur 5: Mitz architectuur en mapping op PvE's

Als het gaat om de standaarden voor integratie, waarbij verschillende systemen de gegevens van elkaar verwerken, is het volgende onderscheid van belang.

Er zijn standaarden voor elektronische medische gegevens:

- openEHR levert bijvoorbeeld informatiestandaarden voor opslag en hergebruik van medische gegevens.
- 'Zorginformatie bouwstenen' (ZIB's) en 'detailed clinical models' (DCM's) leveren basis informatiemodellen voor zorgtoepassingen.

Er zijn standaarden voor elektronische uitwisseling medische gegevens:

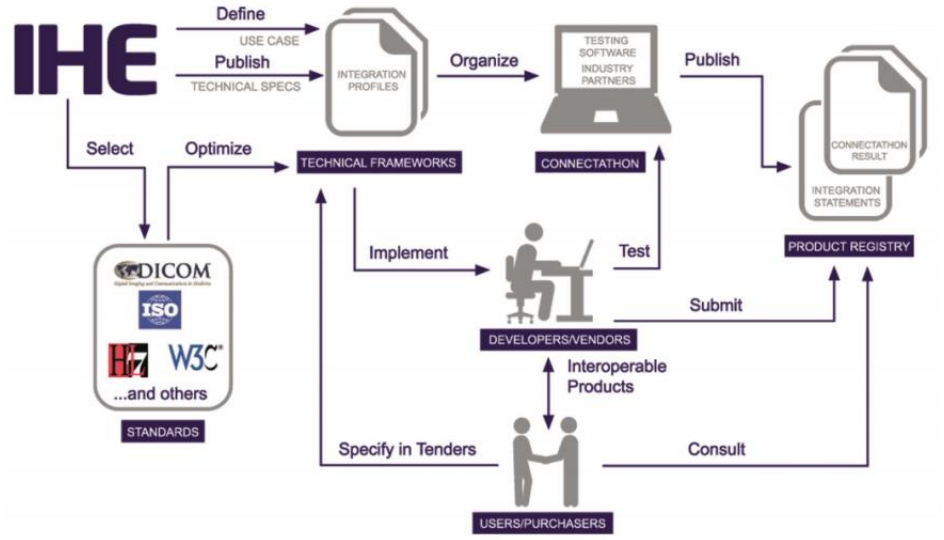
- Health Level 7 (HL7) levert communicatiestandaarden voor de uitwisseling van medische gegevens, bijvoorbeeld HL7v3 waarmee berichtdefinities op basis van HL7 Reference Information Model (RIM) gemaakt kunnen worden. Ook Fast Healthcare Interoperability Resources (FHIR) en Clinical Document Architecture (CDA) zijn HL7 standaarden.
- 'Integrating the Healthcare Enterprise' (IHE) levert profielen voor het implementeren van gestandaardiseerde gegevensuitwisseling. Zo bevat XDS profielen voor het uitwisselen van documenten. IHE gebruikt elders beheerde communicatiestandaarden.

Er zijn standaarden voor elektronische verwerking van toestemmingen:

- OASIS levert XACML (met Policy Enforcement Point (PEP), Policy Retrieval Point (PRP), Policy Decision Point (PDP), etc.) als standaard voor een toestemmingsproces. XACML ondersteunt zowel 'Role Based Access Control' (RBAC) als 'Attribute Based Access Control' (ABAC).
- HL7: consent directives (beschikbaar voor FHIR en CDA).

Er zijn standaarden voor de implementatie van elektronische toestemmingen:

- IHE: Basic Patient Privacy Consent (BPPC) en Advanced Patient Privacy Consent (APPC).



Figuur 6: IHE als integratie standaard

Mitz maakt het voor alle uitwisselingen en uitwisselingssystemen mogelijk om aan te sluiten. Mitz hanteert daarom open standaarden op de koppelvlakken en is in die zin infrastructuur-onafhankelijk. De volgende standaarden worden onder meer gebruikt:

1. De koppelvlakken met uitwisselingssystemen zijn gebaseerd op IHE profielen.
2. Voor de berichtinhoud is FHIR gebruikt (onder andere de 'consent resource').
3. Voor het verkrijgen van toestemming worden de internationale rollen van XACML gebruikt.
4. Voor de authenticatie worden PKIO certificaten ingezet.
5. Voor de autorisatie wordt aangesloten bij internationale 'role-based access control (RBAC)' mechanismes met nationale codes van de BIG-beroepen (van CIBG).
6. Voor de gegevenscategorieën is er een mapping met de ZIB's (bijvoorbeeld van de BGZ) in het model opgenomen.
7. Voor de beveiliging wordt uitgegaan van de NEN-normen.

4.7.2 Implementatie van XACML

In eerdere hoofdstukken is de aanpak beschreven waarbij uitwisselingssystemen in het proces van gegevensuitwisseling een check kan doen bij Mitz alvorens gegevens worden uitgewisseld. Het hoofdproces in de eerste iteratie van de PoC is: nadat een vraag is gesteld of er toestemming is voor de betreffende gegevensuitwisseling, levert Mitz raadpleeg faciliteit een ja / nee op.

Omdat veel regio's IHE gebruiken voor de implementatie van gegevensuitwisseling (XDS), is voor de implementatie van toestemmingsmogelijkheden naar IHE als standaard voor de implementatie gekeken.

Voor de implementatie van de infrastructurele functies kent IHE het IT Infrastructure (ITI) domein met daarin profielen. In het 'ITI Access Control Whitepaper' wordt bij de beschrijving van een 'authorisation request' gebruik gemaakt van de XACML standaardrollen PEP en PDP (zie 0).

Specificatie van de Mitz 'Gesloten autorisatievraag'
Voor de implementatie van de Gesloten autorisatievraag is een internationaal gestandaardiseerde XACML transactie beschikbaar. Deze 'Authorisation Decision Request' is in de actuele versie 3.0 zelfs beschikbaar in een 'multiple decision profile'. Daarmee kunnen meerdere vragen in één transactie gesteld worden. Voor de Gesloten autorisatievraag aan Mitz, kunnen op deze manier alle gegevenscategorieën meegegeven worden in de vraag van de PEP aan de PDP, en dan komt er vanuit Mitz (als PDP) een antwoord terug waarin per gegevenscategorie vermeld wordt of er toestemming is of niet.

Een mogelijke mapping van de Mitz-attributen (van de Gesloten autorisatievraag) op het format van de XACML transactie, zal als bijlage bij het PvE van de Toestemmingsregister beschikbaar zijn (zie implementatiehandleiding *Gesloten autorisatievraag*).

Het antwoord dat Mitz geeft op de Gesloten autorisatievraag, kan 'ja' of 'nee' zijn, afhankelijk van de inhoud van het toestemmingsregister. In de implementatiehandleiding is beschreven hoe bijzondere situaties afgehandeld moeten worden (bijvoorbeeld foutsituaties).

Hoewel XACML een internationale standaard is voor dergelijke autorisatievragen, is er nog geen internationaal profiel voor. IHE Nederland zal daarom de XACML transactie als voorstel voor een nieuw nationaal (en daarna wellicht internationaal) IHE profiel indienen.

4.7.3 Koppeling uitwisselingssystemen

Afbakening
Naast de conformiteit aan de eisen van de koppelvlakken die gespecificeerd zijn voor de Mitz-diensten ten bate van uitwisselingssystemen (US'en), dient een US aan een aantal voorwaarden te voldoen alvorens te kunnen aansluiten. Hiermee worden zaken in de uitwisselingsketen geborgd en wordt voorkomen dat de zwakste schakel een uitwisseling van medische gegevens in gevaar brengt.

Bij aansluiting op Mitz zal de beheerder van Mitz nagaan of aan de aansluiteisen voor een US is voldaan. Het gaat onder andere om de volgende aansluiteisen (zie het PvE Aansluiteisen Uitwisselingssysteem voor een nadere beschrijving van de functionele en technische eisen):

1. Uitwisselingssystemen (en de daarop aangesloten informatiesystemen van zorgaanbieders) voldoen aan vigerende wet- en regelgeving. Het gaat daarbij bijvoorbeeld om de eisen die gesteld worden aan zorgaanbieders en beheerders van elektronische uitwisselingssystemen, zoals verwoord in het 'Besluit elektronische gegevensverwerking in de zorg', (de 'algemene maatregel van bestuur' (AMvB) die per 1 januari 2018 in werking is getreden), met name de conformiteit met betrekking tot NEN 7510, 7512 en 7513.
2. Indien een zorgaanbieder een andere zorgaanbieder wil bevragen die elk van een ander US gebruik maken, dan gaat Mitz niet de routering verzorgen, maar dient het US zelf de verbinding (onder andere op netwerk niveau) met andere US'en te verzorgen, indien dat door de betreffende US'en gewenst wordt. Mitz veronderstelt in dat geval een nationale topologie van US'en die gebruik maken van Mitz. De communicatie tussen zorgaanbieders of uitwisselingssystemen verloopt niet via Mitz.
3. Het US dient het aanroepen van de Mitz-diensten te minimaliseren (onder andere het gebruik van de abonneerfunctie en de Open autorisatievraag dient geoptimaliseerd te worden).
4. In de berichtuitwisseling tussen een US en Mitz kan sprake zijn van UZI-attributen (bijvoorbeeld in de Open - en Gesloten autorisatievraag). De verantwoordelijkheid voor het zekerstellen dat deze UZI-attributen eenduidig behoren bij de betreffende zorgverlener en / of zorginstelling berust bij het US. Mitz doet geen check op de geldigheid en correctheid van de UZI-attributen die in deze berichtuitwisseling is opgenomen. Hier is niet bedoeld het inloggen door zorgverlener die namens patiënt toestemmingen registreert, want daarvoor is inloggen met UZI-pas vereist en zal Mitz de attributen controleren.
5. De verantwoordelijke voor het beheer van een US dient beheerafspraken gemaakt te hebben over de uitwisselingsketen en daarin de Mitz-beheerder op te nemen.
6. De verantwoordelijke voor het beheer van een US dient een overeenkomst te hebben met de aangesloten zorgaanbieder en de aangesloten US'en. Daarin moeten de afspraken met betrekking tot toestemmingsbeheer (zoals die via Mitz gerealiseerd zijn) opgenomen zijn. Het gaat daarbij onder andere om:
   a. op welke wijze de patiënt geïnformeerd wordt (via zorgaanbieder en / of US) waar en vanaf wanneer de zorgverlener vaststelt of er toestemming is verleend;
   b. dat medische gegevens alleen opgevraagd en ter beschikking gesteld mogen worden in het kader van een behandelovereenkomst;
   c. het verstrekken van een overzicht van de functionaliteit die door de zorgaanbieders gebruikt kan worden in hun XIS, in relatie tot de functionaliteit die het US met betrekking tot Mitz ondersteunt (zoals onder andere abonneren, notificeren, gebruik van de noodknop (in geval van spoedzorg));
   d. De controle op de BSN (via WID-controle of vergewissen) is de verantwoordelijkheid van de zorgaanbieder en dient door het US afgesproken te zijn met de zorgaanbieder.
7. De verantwoordelijke voor het beheer van een US dient te borgen dat de raadplegende zorgaanbieder die gegevens krijgt, die relevant en noodzakelijk zijn voor de uitoefening van het beroep.
   Daartoe kan bijvoorbeeld gebruik gemaakt worden van een beroepsrichtlijn met betrekking tot gegevensuitwisseling of een medisch autorisatie protocol dat gegevens per beroepsgroep kan filteren of berichten per beroepsgroep kan autoriseren.

Tenslotte zal de verantwoordelijke voor het beheer van een US een overeenkomst afsluiten met de beheerder van Mitz. Hierin is onder andere beschreven wie de rollen ‘verantwoordelijke’ en ‘verwerker’ vervult voor de verschillende gegevensverwerkingen.

4.7.4 Koppeling smartphone

Afbakening
De Mitz-toestemmingsapplicatie zal als een (responsive) website beschikbaar komen. Vanuit een smartphone kan een snelkoppeling worden gemaakt naar deze website. De website is als een (responsive) website ook aanroepbaar door andere websites.

4.7.5 Koppeling (patiënt)portalen

Afbakening
De Mitz-registratiefaciliteit zal als een (responsive) website worden ontwikkeld en de aanroep naar deze (responsive) website kan in software van anderen (bijvoorbeeld een patiëntenportaal) worden ingebouwd.

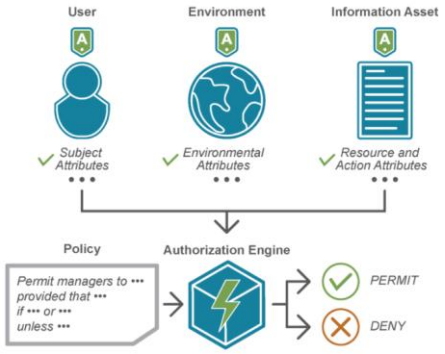
4.7.6 Systeemarchitectuur

Attribuut gebaseerde toegangsverlening (ABAC)

De toestemmingen van de patiënt in Mitz zijn onderdeel van een autorisatie keten. Het filteren van gegevens op basis van beroepsstandaarden is een ander onderdeel van de autorisatie tot inzage en de lokale autorisatie op basis van ‘direct bij de behandeling betrokken’ is een derde onderdeel (zie ook figuur 1). Omdat de raadplegende zorgverlener alleen maar gegevens mag inzien die noodzakelijk en relevant zijn voor de behandeling (ook al heeft de patiënt breder toestemming gegeven), is het in de zorg gebruikelijk om de toegang tot medische gegevens afhankelijk te maken van de rol die de raadplegende persoon heeft: een arts mag meer zien dan een verpleegkundige. Deze vorm van RBAC[4] wordt zowel binnen zorginformatiesystemen gebruikt (een XIS koppelt bepaalde systeemfuncties aan rollen die gekoppeld zijn aan inlogcodes) maar ook tussen zorginformatiesystemen (het LSP autoriseert opvragingen op basis van de rolcode die op de persoonlijke UZI-pas staat).

Met de introductie van Mitz is het mogelijk om toestemmingen te registreren. Er zijn dan meer ‘attributen’ noodzakelijk om te bepalen of iemand toegang krijgt tot gegevens. Naast de rolcode, is ook de gevraagde gegevenscategorie van belang, het type zorgaanbieder dat gegevens deelt, een uniek nummer van de persoon die opvraagt (omdat die als individu uitgesloten kan zijn). Bij een dergelijke vorm van toestemming verlening, wordt gesproken over ABAC.

Het onafhankelijk kunnen beheren van attributen heeft voordelen. Ook de opvolger van de UZI-pas zal een scheiding gaan aanbrengen tussen identificatie (op basis van bijvoorbeeld een commercieel verkrijgbare smartcard) en authenticatie (op basis van publiek beheerde attributen). Internationaal is er ook een beweging zichtbaar waarbij RBAC uitgebreid wordt naar ABAC. Omdat in Mitz diverse attributen bepalen of er toestemming gegeven kan worden, zal ABAC het leidende concept in Mitz zijn. Het gebruik van attributen in een toestemmingsproces wordt beschreven als beleidsregels, ofwel ‘policies’.



Figuur 7: Autorisatie op basis van attributen (ABAC)

[4] De AP stelt rol/werkcontext én behandelrelatie als de verplichte onderdelen van de autorisatie, doordat een behandelrelatie niet of nauwelijks in techniek is te vervatten wordt lokaal bij de zorgaanbieder meestal alleen met RBAC gewerkt. Mitz kan niet op werkcontext en behandelrelatie controleren, dat zal lokaal moeten gebeuren. Hetzelfde geldt voor de controle op of een persoon bij een rol hoort. Dat zal ook een lokale controle en/of een controle vanuit het US moeten zijn. Mitz controleert alleen maar de gegeven rol en identiteit tegen het toestemmingsprofiel, niet de authenticiteit van de combinatie van rol en persoon.

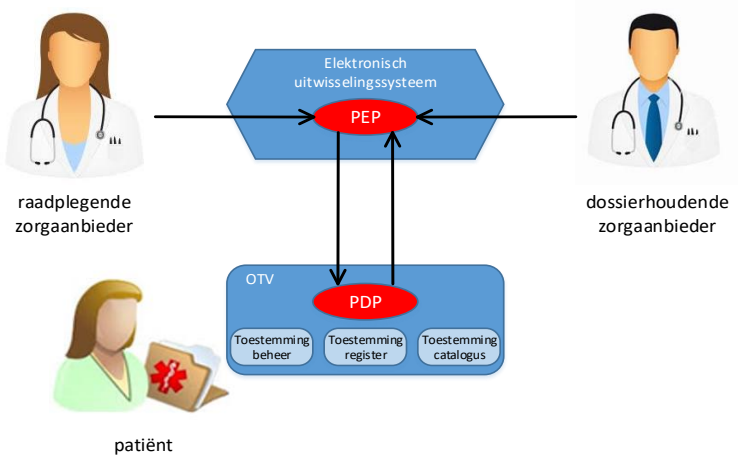
Eenheid van taal voor uitbreidbare toegangscontrole (XACML)

Ook voor de systeemrollen zijn er internationale concepten gedefinieerd die helpen om eenheid van taal te krijgen. Een interessant concept dat past op de rollen die Mitz in de toestemmingsketen onderkend is eXtensible Access Control Markup Language (XACML). Binnen XACML worden policies (hoe je omgaat met toestemmingsverlening op basis van attributen) beschreven in een aantal systeemrollen. Er zijn verschillende punten in de keten om toestemming te verlenen, waar acties nodig zijn.

- Zo is er een punt waar het systeem geforceerd wordt om toestemmingspolicies te raadplegen: PEP.
- Ook is er een punt waar de beslissing wordt genomen of er toestemming is gegeven voor een bepaalde gegevensuitwisseling: PDP.
- Bij deze beslissing dient de toestemming van de patiënt opgehaald te worden en kan er aanvullende informatie nodig zijn.
- De patiënt moet hieraan voorafgaand zijn toestemming geregistreerd hebben en dat zou in XACML termen een PAP worden genoemd.

Binnen Mitz wordt XACML gebruikt als taal voor de rollen die systemen in de keten kunnen vervullen. Het gaat feitelijk alleen om de koppelvlakken tussen Mitz en een elektronisch uitwisselingssysteem. Daarbij zijn vooral PEP en PDP rollen van belang, maar die transacties zijn (nog) niet gestandaardiseerd in XACML.

Eén van de koppelvlakken van Mitz met een elektronisch uitwisselingssysteem is de '***Gesloten autorisatievraag***' (zie 4.3 en 5.1). In onderstaande figuur zijn de XACML concepten toegepast op deze Gesloten autorisatievraag van Mitz. De systeemrollen zijn gemapt op zowel Mitz als op een US dat voor het verkrijgen van toestemming op een bepaalde gegevensuitwisseling alleen Mitz raadpleegt. In een (reeds bestaande) gegevensuitwisseling wordt een PEP geplaatst die naar een PDP van Mitz verwijst om de patiënt toestemming te checken.



Figuur 8: XACML concepten toegepast op de gesloten autorisatievraag

XACML kan zowel voor RBAC als voor ABAC worden ingezet.
Bij deze presentatie van de keten waarin Mitz in een PDP rol optreedt en een zorgaanbieder (via een US) als PEP, sluit niet uit dat een zorgaanbieder of US zelf ook een PDP rol kent. Immers, het is de zorgaanbieder die verantwoordelijk is voor het vaststellen of er uitdrukkelijke toestemming is gegeven. Dat betekent ook, dat voor het bepalen wanneer Mitz geraadpleegd moet worden, de zorgaanbieder hier uiteindelijk voor verantwoordelijk is.

Kengetallen

Voor een inschatting van de dimensionering van de systemen, is het handig te weten hoeveel opvragingen er in de bestaande situatie worden gedaan. Voor het LSP zijn dat er ongeveer 300.000 queries per dag (met pieken van 65.000 per uur), voor een XDS regio 400 onderzoeken per dag. Op basis van deze dimensionering en de operationele metingen in de pilots met andere uitwisselingssystemen, zullen de responstijden en overige systeeminstellingen worden bepaald en gefinetuned.

Bij het bepalen welke digitale middelen in Nederland ingezet kunnen worden, zijn de in januari 2020 gepubliceerde cijfers (orde grootte): >95% van de 17,4 miljoen Nederlanders heeft een mobiel, 80% heeft DigiD en daarvan gebruikt ongeveer 50% DigiD met sms of DigiD app.

4.8 Migratie van bestaande toestemmingen

Zorgaanbieders die voor het uitwisselen van gegevens al toestemmingen hebben geregistreerd, kunnen bij de overstap naar Mitz deze toestemmingen migreren. Uitgangspunt is dat de patiënt niet opnieuw toestemming hoeft te geven, als alleen de toestemming verhuist naar een ander toestemmingsregister.

Omdat de toestemmingen in Mitz rechtmatig en betrouwbaar moeten zijn zodat alle aangesloten partijen er op kunnen vertrouwen, worden bestaande toestemmingen eerst juridisch getoetst en vertaald naar de toestemmingsmogelijkheid in Mitz waar de bestaande toestemming onder valt. Het is aan de zorgaanbieder (al dan niet in een groter organisatorisch verband van bijvoorbeeld een regio of een XIS-gebruikersvereniging), om te zorgen dat de patiënt geïnformeerd wordt. Mitz zal hiervoor basis teksten aanleveren en in Mitz zelf wordt de patiënt geïnformeerd over de werking van Mitz.

Het moment waarop een zorgaanbieder alle toestemmingen migreert naar Mitz wordt bepaald door het aansluitproces.

4.8.1 Aansluitproces

De migratie van bestaande toestemmingen is onderdeel van het proces Technische Aansluiting Zorgaanbieder, ter onderscheiding van Organisatorische Aansluiting Zorgaanbieder (zie afsprakenstelsel). Het technische aansluitproces bestaat uit de onderliggende stappen:

- De zorgaanbieder dient zijn XIS te upgraden naar een Mitz-compatible XIS.
- Technisch aansluiten van het XIS op Mitz via een Mitz-compatible US (indien van toepassing).
- Migreren van de bestaande toestemmingen (indien aanwezig)
- Abonneren (het registreren van de actuele dossiers bij Mitz).
- Notificaties verwerken van de Mitz-toestemmingen in het XIS.

4.8.2 Toestemmingen uploaden

Op een afgesproken tijdstip kan het verzamelen en uploaden van de bestaande toestemmingen worden gestart. Van alle patiënten van wie de zorgaanbieder een dossier voert en van wie een toestemming bekend is, worden de toestemmingen verzameld en in een elektronisch bericht via het US verstuurd naar Mitz.

Indien een patiënt nog geen toestemmingprofiel in Mitz had, wordt deze aangemaakt. Op basis van de geboortedatum wordt de leeftijdscategorie bepaald. Toestemmingen van patiënten jonger dan 16 jaar kunnen gemigreerd worden, zonder dat ouder/voogd (opnieuw) een beoordeling moet uitvoeren.

4.8.3 Gemigreerde toestemmingen inzien en aanpassen

Als een patiënt inlogt op Mitz nadat een migratie heeft plaatsgevonden, wordt de patiënt over deze migratie geïnformeerd. Een patiënt kan er ook voor kiezen om een email te ontvangen bij iedere migratie. Bestaande toestemmingen (toestemmingskeuze=ja) zullen doorgaans gegeven zijn aan een individuele zorgaanbieder (als dossierhouder). Deze worden ook als individuele toestemmingen gemigreerd naar Mitz.

Bij het informeren over de gemigreerde toestemming(en) (toestemmingskeuze=ja) krijgt de patiënt de mogelijkheid om er een categorale toestemming van te maken (vergelijkbaar met de gewone toestemming registratie in Mitz). Als de patiënt dat voor een bepaalde zorgaanbiedercategorie heeft aangegeven, vallen latere migraties van (individuele) toestemmingen automatisch onder deze categorale toestemming. Ook hierover wordt de patiënt geïnformeerd.

Bij een gemigreerde toestemmingskeuze=nee, krijgt de patiënt de mogelijkheid om voor spoedzorg een uitzondering te maken.

Gemigreerde toestemmingskeuzes worden, net als handmatige wijzigingen, als nieuwe versies van het toestemmingsprofiel bewaard, zodat het verloop desgewenst getoond kan worden.

4.9 Foutafhandeling

Voor fouten in de afhandeling van berichten wordt er onderscheid gemaakt tussen verwerking van de berichtinhoud door ontvangende applicaties (bijvoorbeeld wat er moet gebeuren als een veld leeg is of een BSN al bestaat) en verwerking op netwerk niveau (zoals de berichtenontvangst stagneert of andere infrastructurele fouten in de berichtencommunicatie waardoor Mitz-systeembeheer actie moet ondernemen).

Voor de te genereren foutcodes worden zoveel mogelijk de standaard gedefinieerde foutcodes van de gebruikte protocollen gehanteerd. In de auditlog worden de eventuele foutcodes geregistreerd. Fouten moeten correct en tijdig afgehandeld worden.

5 Fasering Mitz

5.1 Gewenste situatie

De gewenste eindsituatie is een omgeving waarin patiënten hun toestemmingskeuzes kunnen vastleggen. Deze omgeving is dusdanig opgezet, dat deze makkelijk aanpasbaar en uitbreidbaar is. De gewenste situatie wordt gefaseerd ingevoerd in verschillende releases.

5.2 Releases

5.2.1 Release 1: Minimal Viable Product (MVP)

MVP

- dat voldoende functionaliteit bevat om de gegevensuitwisselingen van het eerste aangesloten US en zorgaanbieders te continueren,
- waarbij de patiënt meer in de regie komt, aangezien hij in één overzicht inzicht krijgt in zijn toestemmingen (nu is dat per US en niet altijd online in te zien),
- de patiënt zijn toestemmingskeuzes te allen tijde kan registreren zonder een noodzakelijke handmatige stap bij de zorgaanbieders die lang kan duren,
- een toestemmingskeuze net zo makkelijk gewijzigd of verwijderd kan worden als een nieuwe toestemmingskeuze geregistreerd kan worden (nu wordt er vooral geattendeerd op het belang van toestemming geven en is de procedure van intrekken vaak anders).

Wat kan het MVP van Mitz?

- Mitz moet een voorziening zijn, waarmee patiënten op een eenduidige manier zelfstandig toestemmingskeuzes kunnen registreren, wijzigen en verwijderen, via een smartphone, of via een website.
- Patiënten moeten kunnen inloggen op een niveau dat past bij de verwerking van bijzondere persoonsgegevens, maar het mag niet te ingewikkeld zijn.
- Voor een patiënt die geen gebruik kan of wil maken van Mitz en waarbij zorgverleners bereid zijn om namens die betreffende patiënt de toestemmingskeuze te registreren, zal een inlogvoorziening beschikbaar komen voor de zorgverlener in de website van Mitz.
- Bestaande uitwisselingen moeten gecontinueerd kunnen worden. Eind 2019 zal een lijst met uitwisselingen (interacties) opgesteld worden die de MVP van Mitz gaat ondersteunen.
- Aansluiting van een uitwisselingssysteem moet technisch mogelijk zijn via de afgesproken standaarden uit de PSA, PvE's, en implementatiehandleidingen van de koppelvlakken.
- MVP moet voldoen aan wettelijk kader:
  - Toestemming zoals AVG die beschrijft (uitdrukkelijk, specifiek).
  - Toestemmingskeuzes zijn rechtsgeldig (vrij, geïnformeerd, ondubbelzinnig, aantoonbaar).
  - Toestemmingsmogelijkheid moet categorieën van zorgaanbieders en gegevens bevatten.
  - Toestemmingsmogelijkheid moet heldere omschrijving van bepaalde gegevens bevatten.
  - Toestemmingssysteem moet zodanig gestructureerd zijn dat er geanticipeerd kan worden op een variërend aantal toestemmingsmogelijkheden.

Scope afbakening van het MVP van Mitz

Functionaliteit die in de scope is van een goed beveiligde en goed beheerde Mitz (zie voor detaillering de volgende hoofdstukken):

1. Patiënt kan een profiel aanmaken in Mitz.
2. Patiënt moet minimaal met DigiD met sms inloggen om de eigen toestemmingskeuzes vast te leggen (registreren, wijzigen of intrekken).
3. Patiënt kan een categorie van zorgaanbieders of een individuele zorgaanbieder een toestemmingskeuze registreren om gegevens te delen.
4. Patiënt kan zorgaanbieders vanuit het Zorgaanbiedersadresboek selecteren om voor een individuele zorgaanbieder toestemmingskeuzes te bepalen.

5. Patiënten worden door Mitz genotificeerd als toestemmingskeuzes zijn geraadpleegd, er wijzigingen zijn in zorgaanbieders die wijzigingen in keuzes volgen, toestemmingskeuzes door een ander zijn aangepast en in de functionaliteit van Mitz zelf. Als de patiënt een geldig e-mailadres heeft opgegeven in het persoonlijke profiel en deze notificaties heeft aangezet, wordt de patiënt per email op de hoogte gebracht van deze notificaties.
6. Patiënt kan aangeven dat zijn of haar Mitz-profiel verwijderd moet worden, inclusief alle bijbehorende persoonlijke gegevens. De patiënt kan per e-mail een bevestiging hiervan krijgen, indien de patiënt hiervoor gekozen heeft.
7. Zorgaanbieder kan via een US
   7.1. zich abonneren bij Mitz op notificaties dat toestemmingskeuzes zijn gewijzigd van patiënten van wie ze gegevens kunnen delen,
   7.2. vaststellen of de noodzakelijke grondslag aanwezig is voor het elektronisch delen van bepaalde gegevens.
8. Zorgverlener kan met de eigen UZI pas (op naam) toestemmingen namens patiënt registreren, of een mandaat(token) ondertekenen voor medewerkers, zodat medewerkers toestemmingen namens de patiënt kunnen registreren, nadat de identiteit van de patiënt is vastgesteld en de geverifieerde BSN van de patiënt is doorgegeven aan Mitz.
9. Uitwisselingssystemen kunnen gebruik maken van vier functies van Mitz (via de zogenaamde koppelvlakken): abonneren, notificeren, open – en/of gesloten autorisatievraag.
10. De toestemmingsmogelijkheden in Mitz zijn configureerbaar zodat steeds de best mogelijke fit met het maatschappelijke draagvlak, gebruiksgemak voor de patiënt en de technische haalbaarheid voor de leveranciers, die al verschillende gegevensuitwisselingen ingebouwd hebben, gerealiseerd kan worden.
11. De ouder / voogd kan in de MVP van Mitz voor een kind (dat jonger is dan 12 jaar), toestemmingskeuzes registreren of (voor kinderen van 12 tot 16 jaar) al dan niet bevestigen
    Zolang er geen verificatie mogelijk is bij de registers met ouderlijk gezag en voogdij en bij de 'Basisregistratie Personen' (BRP) voor een leeftijdscheck, moeten beide personen zich authenticeren met DigiD en wordt er een eenduidige link gelegd met een koppelcode.
12. De MVP van Mitz gaat van start met toestemmingsmogelijkheden waarmee de elektronische uitwisselingen van het eerste aangesloten US en zorgaanbieders gecontinueerd kunnen worden.
13. In de scope van het MVP zit ook de aanroep vanuit een zorgverlenersinformatiesysteem naar de (responsive) website van Mitz om het beheer van toestemmingen voor een patiënt uit te voeren. Ook de SSO waarbij een zorgverlener die al met een UZI-pas is ingelogd, zonder opnieuw in te hoeven loggen, wordt doorgeleid naar Mitz.

In de scope van het MVP zit de aanroep vanuit een externe digitale omgeving, zoals een patiëntenportaal naar de (responsive) website van Mitz, inclusief de single sign-on (SSO) waarbij een patiënt die al met minimaal DigiD met sms is ingelogd, zonder opnieuw in te hoeven loggen, wordt doorgeleid naar de Mitz-diensten.

Ook in scope van MVP is de ondersteuning van spoedzorg: zorgaanbieders die in spoed situaties zorg moeten verlenen en daarbij gegevens nodig hebben, en bij het opvragen van gegevens aangeven dat er sprake is van een spoed situatie, krijgen van Mitz toestemming indien de patiënt in Mitz toestemming heeft geregistreerd voor spoedzorg.

'Hidden features' die wel in Mitz ingebouwd zijn, maar nog niet in de keten ondersteund hoeven te worden:

- De MVP van Mitz heeft wel al een koppeling met DigiD Machtigen, maar het machtigen van iemand anders door de patiënt is nog niet mogelijk, want DigiD Machtigen bevat nog niet de zorgdiensten en / of zorgaanbieder(categorieën).

5.2.2 Latere releases

Niet in de scope van de MVP van Mitz (maar wel gepland voor een latere release):

- Het moet mogelijk zijn om bestaande geregistreerde toestemmingen te migreren naar Mitz.
- Patiënt kan zorgverleners vanuit het Zorgaanbiedersadresboek selecteren om geen toestemming te geven voor het raadplegen van het toestemmingenregister via een US. Individuele zorgverleners kunnen zo worden geblokkeerd voor alle opvragingen. Dit heeft geen effect op de intramurale autorisaties en toegang tot medische informatie binnen een zorgaanbieder waar de betreffende zorgverlener werkzaam is. (Zie 4.4.2)
- Het aanroepen van Mitz-diensten vanuit externe patiënt- en/of zorgaanbiedersportalen.
- Het gebruik van een QR-code om versneld toestemmingskeuzes te bepalen voor een selectie van toestemmingsmogelijkeden, na het inloggen met DigiD, wordt in latere release ondersteund. Bijvoorbeeld te gebruiken om een patiënt bij een (raadplegend) zorgaanbieder op locatie te ondersteunen.
- Naast de secure link kan een zorgaanbieder ook toestemmingskeuzes namens de patiënt registreren, door een toestemmingsknop (de 'smart link'). Daarmee worden de voor die zorgaanbieder relevante toestemmingen geregistreerd.

- Als een zorgaanbieder op basis van een notificatie van Mitz (waarin een beperkt aantal gegevens van de toestemming zit) de hele toestemming van die patiënt voor hem / haar (als dossierhoudende zorgaanbieder) wil ophalen, vereist dat een aparte interactie (berichtdefinitie met koppelvlak). Dat is voor een volgende release voorzien.
- Het zorgaanbiederadresboek kan in een volgende release ook gebruikt worden om allerlei kenmerken van een zorgaanbieder op te halen, zodat de koppelvlakken met de uitwisselingssystemen vereenvoudigd kunnen worden.
- Authenticatie in het kader van verwerking bijzondere persoonsgegevens vereist een niveau substantieel (zie VZVZ Verklarende Woordenlijst) en dat is hoger dan DigiD met sms of DigiD app (beide niveau midden (het laagste eIDAS niveau)). Niveau substantieel zal door Mitz ondersteund worden, zodra deze beschikbaar zijn (en door 'het ministerie van Binnenlandse Zaken en Koninkrijksrelaties' (BZK) in het kader van de wet Digitale Overheid aangewezen). Om het overschakelen naar andere authenticatiemiddelen makkelijker te maken wordt er een 'Routeringsfunctie' door BZK gerealiseerd, die fungeert als een 'authenticatiemakelaar'. Een koppeling met deze dienst zal in een volgende release opgenomen worden, zodra de dienst door BZK beschikbaar wordt gesteld voor de zorg.
- Toestemmingskeuzes kunnen snel geregistreerd worden door de lijst met geabonneerde zorgaanbieders uit te breiden met deze functionaliteit.
- In een later stadium is het denkbaar dat zorgaanbieders aangeven geen notificaties te willen ontvangen of een bepaald soort notificatie niet meer willen te ontvangen.
- In een volgende release kunnen de technisch beheerders van Mitz de meest voorkomende beheeracties geautomatiseerd uitvoeren in de beheerapplicatie.
- Bepaalde (benoemde) non-functionele eisen in toestemmingsbeheer worden in de MVP nog niet gerealiseerd, maar dat kan in een vervolg release wel worden gedaan.
- Zodra er nationale registers zijn voor wilsonbekwamen, gemachtigden, voogdijschap, ouder met gezag, leeftijdscategorie die benaderbaar zijn voor Mitz, zal Mitz daarmee koppelen en extra functionaliteit, gebruiksgemak of beveiliging kunnen realiseren. Tot die tijd gaat Mitz het niet zelf bouwen.
- Overige wensen en eisen van andere partijen, die in de loop van 2020 en 2021 relevant kunnen worden, zullen geprioriteerd worden en kunnen onderdeel gaan uitmaken van Mitz, die de wettelijke verplichting van toestemming voor elektronische gegevensuitwisseling zal ondersteunen.

6 Keuze oplossingsrichting

6.1 BIA en DPIA

Omdat Mitz de principes volgt van privacy-by-design, is al tijdens de ontwerpfase, op basis van de eerste PSA een “Gegevensbescherming door ontwerp” uitgevoerd door een externe partij. Deze aanbevelingen zijn verwerkt in de PSA.

Samen met security management zal, voorafgaand aan de go-live van Mitz, een Business Impact Analysis (BIA) en Data Protection Impact Assessment (DPIA), worden uitgevoerd, inclusief data classificaties en beschikbaarheidsvereisten, om alle risico’s en mitigerende maatregelen goed in beeld te krijgen.

7 Overdracht aan Project Management

Het projectmanagement van OTV wordt uitgevoerd door VZVZ.

7.1 Overdracht voorwaarden en - moment

De uitvoering van het programma OTV wijkt af van de standaard aanpak van VZVZ. Normaal gesproken wordt eerst het definitieve PSA opgeleverd en dan pas wordt gestart met de ontwikkeling. Gezien de snelle opleverdatum is voor het programma OTV gekozen voor een iteratieve oplevering van het MVP.

Dit houdt in dat de uitwerking van de PSA en de ontwikkeling van de Mitz-dienst parallel verlopen. Tijdens elke iteratie wordt een gedeelte van het desbetreffende onderwerp opgeleverd. Elke iteratie kent daardoor eigen overdracht voorwaarden en –momenten. Dit wordt voor elke iteratie door Project Management bepaald.