

# Online Toestemmingsvoorziening:

## Mitz als bouwsteen

<b>Datum:</b>	1 september 2020
<b>Status:</b>	Concept
<b>Versie:</b>	1.0
<b>Classificatie:</b>	Vertrouwelijk
<b>Eigenaar:</b>	VZVZ
<b>Revisie:</b>	

# Inhoudsopgave

<b>1 Inleiding</b>	<b>3</b>
Leeswijzer	3
<b>2 Achtergrond toestemmingskeuzes</b>	<b>4</b>
2.1 Juiste gegevens beschikbaar voor zorgproces, op juiste plek en juiste moment	4
2.2 Gespecificeerde toestemming Wabvpz 15a.2	4
2.3 Ondersteuning behandelaars en zorgprocessen	6
<b>3 Huidige situatie toestemmingen</b>	<b>7</b>
3.1 Probleemomschrijving	7
<b>4 Kaders, randvoorwaarden en uitgangspunten voor een online toestemmingsvoorziening</b>	<b>9</b>
4.1 Uitgangspunten	9
4.2 Verdieping juridisch kader	12
4.3 Verdieping vertrouwensaspecten	13
4.4 Verdieping inpassen in de zorgprocessen	16
<b>5 Online toestemmingsvoorziening Mitz</b>	<b>17</b>
5.1 Opzet Mitz	17
5.2 Werking Mitz-componenten	20
5.3 De toestemmingscatalogus	22
5.4 Werking Mitz via uitwisselingssystemen	25
5.5 Migratie van bestaande toestemmingen	26
5.6 Aansluitproces Mitz	26
5.7 Operationele uitvoering	27
<b>6 De toepassing van DIZRA</b>	<b>29</b>
6.1 Uitgangspunten DIZRA toegepast op Mitz	29
6.2 Principes van DIZRA toegepast op Mitz	31

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 deze 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 vaststellen. 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').

De online toestemmingsvoorziening is een generieke dienst voor burgers, patiënten en cliënten (hierna: patiënten) waarop zorgaanbieders kunnen aansluiten, al dan niet via een systeem ten behoeve van elektronische uitwisselingen en heeft betrekking op de uitwisseling van gegevens tussen zorgaanbieders, waarbij toestemming als grondslag vereist is, of bezwaar gecontroleerd moet kunnen worden.

Dit document beschrijft waar een online toestemmingsvoorziening als generieke dienst aan moet voldoen. De online toestemmingsvoorziening Mitz is hierop gebaseerd.

Het regelen van toestemming en bezwaar hoeft op deze wijze niet door alle zorgaanbieders apart opgepakt te worden, maar kan generiek worden opgezet en onderhouden. Efficiënte inzet van kennis, IT capaciteit en middelen is een ons inziens een bijkomend groot voordeel. Daarnaast komt de patiënt meer in de regie, doordat alle toestemmingen en bezwaren op een overzichtelijke wijze kunnen worden ingezien en beheerd.

#### **Doel van dit document is te bespreken:**

- **of een online toestemmingsvoorziening onder deze beschrijving tegemoet komt aan de wensen en eisen van het zorgveld en voldoet aan de behoefte;**
- **of Mitz als online toestemmingsvoorziening hierin voorziet en toegelaten kan worden als bouwsteen voor de duurzaam informatiestelsel in de zorg.**

#### **Leeswijzer**

In hoofdstuk 2 wordt de achtergrond en recente historie van toestemmingskeuzes beschreven. In hoofdstuk 3 wordt ingegaan op de huidige situatie omtrent toestemmingen. In hoofdstuk 4 volgt een overzicht van de kaders, randvoorwaarden uitgangspunten van een online toestemmingsvoorziening. Hoofdstuk 5 geeft een beschrijving hoe Mitz als online toestemmingsvoorziening hierin voorziet. Hoofdstuk 6 geeft tenslotte een beeld van de wijze waarop een online toestemmingsvoorziening in het algemeen en Mitz specifiek voldoet aan de uitgangspunten en principes van DIZRA.

**De juiste gegevens, op de juiste plek op het juiste moment beschikbaar voor het zorgproces. Een algemene toelichting op de achtergrond van toestemmingskeuzes.**

## 2.1 Juiste gegevens beschikbaar voor zorgproces, op juiste plek en juiste moment

De gegevens die nodig zijn voor het verlenen van goede zorg, komen soms bij andere zorgaanbieders vandaan. Het uitwisselen van gegevens is een vorm van gegevensverwerking. Voor de verwerking van bijzondere persoonsgegevens vereist de AVG een wettelijke grondslag. 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 of het beroepsgeheim doorbroken mag worden?

De afgelopen jaren zijn hiervoor uitwisselingssystemen ontstaan: met een lokalisatieregister (ook wel index genoemd) 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 ('geef me alle relevante informatie over deze patiënt') weet de raadpleger niet welke bron(nen) bevraged 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 zorgaanbieders er gegevens opgevraagd kunnen worden. Als de index onder gegevensverwerkingsverantwoordelijkheid van de (dossierhoudende) zorgaanbieder blijft, is er voor het aanleggen van een index geen uitdrukkelijke toestemming nodig en kan de index zowel voor verzenden worden gebruikt als voor opvragen (waarbij dan de toestemming voor uitwisseling ook geldt voor het bevragen van de index door de raadpleger).

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 dat de dossierhouder (op wie het beroepsgeheim rust) met de patiënt kan overleggen en de patiënt een mogelijkheid tot bezwaar kan geven. Om de juiste gegevens dan 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.

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 lid 1 gaat over deze manier van toestemming verlenen. Een uitdrukkelijke toestemming is vereist als een dossierhouder op wie het beroepsgeheim rust, gegevens beschikbaar stelt aan een op dat moment nog onbekende raadpleger die via een elektronisch uitwisselingssysteem gaat raadplegen. Deze bepaling is op 1 juli 2017 in werking getreden.

## 2.2 Gespecificeerde toestemming Wabvpz 15a.2

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 uit 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 technische, juridische en praktische haalbaarheid van artikel 15a lid 2 heeft de minister van VWS in 2015 na afloop van een Bestuurlijk Overleg met de KNMG, de KNMP, de LHV, de Patiëntenfederatie en Nictiz, besloten de inwerkingtreding van artikel 15a, tweede lid, destijds met 3 jaar uit te stellen.

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. 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. Een balans moet worden gezocht tussen enerzijds niet teveel toestemmingsmogelijkheden omdat de toestemming dan niet meer begrijpelijk is, en anderzijds voldoende toestemmingsmogelijkheden om de toestemming specifiek te houden. Dat is het inzicht uit de analyse naar aanleiding van Wabpz art. 15a lid 2. Ook al zou dat artikel helemaal niet meer in werking treden, dit inzicht is waardevol, omdat de AVG aangeeft dat een toestemming die als grondslag voor een gegevensverwerking dient, zowel specifiek moet zijn, als begrijpelijk (naast goed geïnformeerd, in vrijheid gegeven etc.).

Op het Informatieberaad van 21 april 2020 is besloten dat Mitz moet aansluiten op het advies dat de minister in juni 2020 of erna aan de Tweede Kamer stuurt (omtrent gespecificeerde toestemming en Wabvpz). Op het moment van verschijnen van dit consultatiedocument is deze ministerbrief nog niet beschikbaar. Echter, indien in de komende periode op basis van deze brief blijkt dat toch wijzigingen noodzakelijk zijn, zullen deze uiteraard worden doorgevoerd.

Vooruitlopend op dit advies, is Mitz als volgt ingericht.

1. Op dit moment is de Wabvpz art. 15a lid 1 van artikel 15a van de Wabvpz (over de uitdrukkelijke toestemming voor beschikbaar stellen) ruim drie jaar in werking en lid 2 van dat artikel (over de gespecificeerde toestemming) nog niet in werking getreden. Indien het advies deze lijn continueert, dan betekent dat, dat een online toestemmingsvoorziening vooral de uitdrukkelijke toestemming moet ondersteunen en niet gericht moet zijn op de gespecificeerde.
  - a. Mitz heeft het gespecificeerde losgelaten en is gebaseerd op het huidige wettelijk kader, zodat er, conform ATR advies, een brede toestemming mogelijk is, waarbij de patiënt achteraf kan controleren of de raadplegers wel zijn behandelaren zijn.
  - b. Mitz is zo ingericht dat uitdrukkelijke toestemmingen die op grond van het eerste lid nodig zijn, ondersteund worden.
2. Op dit moment is voor sommige uitwisselingen, op grond van Wgbo, een uitdrukkelijke toestemming nodig (niet iedereen en niet alle gegevens kunnen op basis van een veronderstelde toestemming bij een actuele behandeling worden betrokken). Indien het advies deze lijn continueert, dan betekent dat, dat een online toestemmingsvoorziening de uitdrukkelijke toestemming voor deze situaties moet ondersteunen.
  - a. Een dergelijke toestemming moet conform de AVG specifiek zijn, dus moet het mogelijk zijn om een specifieke zorgaanbieder te kiezen die zijn beroepsgeheim mag doorbreken.
  - b. Mitz is zo ingericht dat uitdrukkelijke toestemmingen die op grond van Wgbo (soms) nodig zijn, ondersteund worden bij het versturen van gegevens.
3. Op dit moment is het zo dat in sommige situaties de toestemming, die nodig is vanwege de Wgbo, verondersteld mag worden. Indien het advies deze lijn continueert, dan betekent dat, dat een online toestemmingsvoorziening een eventueel expliciet bezwaar moet kunnen ondersteunen als daar behoefte aan is (bv. bij een geautomatiseerd herhaald versturen van gegevens).
  - a. Mitz is zo ingericht dat uitdrukkelijk bezwaar die op grond van een veronderstelde toestemming gegeven moet kunnen worden, ondersteund wordt als een zorgaanbieder dat nodig heeft.
4. Op dit moment is het zo dat de wet- en regelgeving geen specifieke uitwisselingssystemen (US-en) verplicht stelt of uitsluit. Het in alle zorgsituaties beschikbaar krijgen van de relevante gegevens (100% dekking), vereist dat alle uitwisselingssystemen betrokken moeten kunnen worden. Indien het advies deze lijn volgt, dan betekent dat, dat een online toestemmingsvoorziening alle systemen moet kunnen ondersteunen. Zowel US-en die alleen uitwisselen conform Wabvpz, alsook US-en die alleen uitwisselen conform Wgbo met uitdrukkelijke toestemming, alsook uitwisselingssystemen die alleen uitwisselen conform Wgbo o.b.v. veronderstelde toestemming (en uiteraard US-en die combinaties leveren).

- a. Mitz is zo ingericht dat al deze type US-en de benodigde grondslag aan de hand van de geregistreerde toestemmingskeuzes kan bepalen.
5. Op dit moment is de beschikbaarheid van gegevens in sommige situaties afhankelijk van een toestemming die vooraf gegeven had moeten worden aan de zorgaanbieder die het dossier beheert. Als de opvragende zorgaanbieder wel toestemming krijgt om gegevens in te zien, is daarmee nog geen toestemming gegeven aan de dossierhouder om het beroepsgeheim te doorbreken. Het ontbreken van die ‘toestemming vooraf’ is dan een bottleneck in de beschikbaarheid van de gegevens voor het zorgproces. Indien het advies dit probleem erkent en wil aanpakken, kan een goed ingerichte online toestemmingsvoorziening hiervoor een oplossing bieden. Een online toestemmingsvoorziening zou dan in staat moeten zijn om bij de opvrager een toestemming te regelen die voldoende waarborgen bevat om door de dossierhouder vertrouwd te worden.
- a. Mitz is zo ingericht dat een raadplegende zorgaanbieder namens de patiënt een dergelijke toestemming onweerlegbaar kan organiseren, zodanig dat die bij de juiste bron terecht komt, vertrouwd wordt, en gegevens door die bron beschikbaar gesteld kunnen worden. De patiënt geeft daarvoor ter plekke uitdrukkelijke toestemming en kan via Mitz controleren wie de toestemming namens hem/haar heeft gezet en wie t.b.v. van een specifieke uitwisseling de toestemming heeft gecheckt. De dossierhouder kan er op vertrouwen, omdat de onweerlegbaarheid in de techniek (‘cryptografisch’) is geborgd aan de hand van een zorgaanbiederstoken, een mandaattoken en een bsn-token.

### 2.3 Ondersteuning behandelaars en zorgprocessen

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 toestemming vergt die op dat moment niet verondersteld kan worden. Dan is er een uitdrukkelijke en specifieke toestemming nodig (zowel om het beroepsgeheim te mogen doorbreken, als om een grondslag te hebben voor de uitwisseling zelf). Immers, als de WGBO geen grondslag levert, kan de uitdrukkelijke en specifieke toestemming uit de AVG een grondslag vormen voor dit type uitwisseling. Afhankelijk van de gekozen inrichting (bv. beschikbaar stellen via een uitwisselingsstelsel) is een dergelijke toestemming ook vereist door Wabvpz art. 15a lid1. *Zorgaanbieders moeten daarom voor het ‘ongericht’ beschikbaar stellen van gegevens een uitdrukkelijke toestemming van de patiënt organiseren.*

En voor het gericht delen van gegevens met andere zorgaanbieders op basis van een veronderstelde toestemming, moet er voor de patiënt een bezwaar mogelijkheid zijn. Steeds vaker wordt een aanvullende verzending van gegevens (op basis van deze veronderstelde toestemming) geautomatiseerd en dan is registratie van bezwaar nodig. *Zorgaanbieders willen daarom voor het gericht beschikbaar stellen van gegevens een uitdrukkelijk bezwaar van de patiënt organiseren.*

Om wildgroei van systemen voor registratie van toestemming en bezwaar te voorkomen en om te voorkomen dat er een wildgroei ontstaat aan toestemmingskeuzes, is de noodzaak ontstaan om het organiseren van toestemmingen (verondersteld of uitdrukkelijk) 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, waar iedereen zijn toestemming voor digitale gegevensuitwisseling tussen zorgaanbieders kan beheren, wordt in dit document beschreven.

Nota bene: Een zorgaanbieder die alleen maar gegevens verstuurt op basis van veronderstelde toestemming, hoeft geen expliciete toestemmingen te organiseren en als het versturen eenmalig gebeurt hoeft een eventueel bezwaar ook niet geregistreerd te worden. Een online toestemmingsvoorziening faciliteert de informatie uitwisseling voor zorgprocessen die het checken van een expliciete toestemming of een expliciet bezwaar wel nodig hebben.

**Hoe verleent de patiënt momenteel toestemming aan de zorgaanbieder. Bezwaren worden nog niet breed geregistreerd. Een probleemomschrijving als basis voor de benodigde en gewenste functionaliteit van een online toestemmingsvoorziening.**

### Toestemming

In de huidige situatie stelt iedere zorgaanbieder vaak maar één toestemmingsvraag (voor de uitwisseling met andere zorgaanbieders) en kan de patiënt daarop maar één keuze maken (ja op alles of nee op alles). In het bijbehorende informatiemateriaal is dan beschreven welke gegevens worden gedeeld met welke zorgaanbieders, bijvoorbeeld huisartswaarneemgegevens met huisartsenposten, medicatie met apotheken (via het LSP) of medische beelden met andere ziekenhuizen in de regio (via een regionaal XDS netwerk). Vaak wordt in de toestemmingsvraag ook het uitwisselingsstelsel genoemd. Per zorgaanbieder en/of uitwisselingsstelsel kunnen er variaties op bovenstaande zijn.

### 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 beschikbaar gesteld 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 web-portaal, waarna de toestemming wordt verzonden aan de betreffende zorgaanbieder.

Bij alle drie de varianten is het belangrijk dat de patiënt de voorlichtingsfolder heeft doorgenomen.

Soms is het mogelijk om voor iemand anders toestemming te regelen en om online toestemmingen in te trekken (bijvoorbeeld via [volgjezorg.nl](http://volgjezorg.nl)). Het is niet altijd mogelijk om voor kinderen toestemming te regelen.

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

### Acceptatie door patiënt en zorgaanbieder

Patiënten en zorgaanbieders accepteren de huidige situatie. Alle patiënten kunnen werken met het geven van mondelinge toestemming of het invullen van een analogo formulier. Hiernaast kunnen de patiënten die dit willen ook op digitale wijze hun toestemming verlenen. Indien de zorgaanbieder schriftelijk toestemming ontvangt voor het beschikbaar stellen van patiëntdata, dan kan de zorgaanbieder deze verkregen toestemming bewaren. Soms kan deze toestemming worden geregistreerd, bijvoorbeeld indien het zorginformatiesysteem (XIS) hiervoor een mogelijkheid biedt. Bij sommige uitwisselingsystemen wordt op basis van deze toestemming een index bijgewerkt (vergelijk de verwijzingsindex (VWI) van het LSP).

## 3.1 Probleemomschrijving

Het is voor een patiënt in de huidige situatie in veel gevallen 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.

### 3.1.1 Knelpunten en oorzaken

Het is voor een patiënt in de huidige situatie moeilijk te begrijpen 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 ('de raadpleger'), toestemming te geven aan zorgaanbieders die de gegevens in het dossier hebben staan ('de dossierhouder'). Wettelijk gezien moet immers de dossierhouder het beroepsgeheim doorbreken op basis van de toestemming van de patiënt. Waar een patiënt vaak denkt dat er alleen maar een toestemming gegeven 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 beschikbaar te stellen. 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 beschikbaar gesteld 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 niet overal 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.



# Kaders, randvoorwaarden en uitgangspunten voor een online toestemmingsvoorziening

**De kaders, randvoorwaarden en uitgangspunten voor een online toestemmingsvoorziening worden nader toegelicht met een verdieping op het juridisch kader, vertrouwensaspecten en het inpassen in de zorgprocessen.**

## 4.1 Uitgangspunten

Voor een online toestemmingsvoorziening worden de volgende uitgangspunten gehanteerd:

- Een patiënt heeft overzicht over zijn hele zorg;
- Een gemeenschappelijke dienst moet voor alle patiënten toegankelijk zijn;
- Een toestemming of bezwaar moet voor alle uitwisselingen beschikbaar zijn;
- Een toestemming of bezwaar moet direct geldig zijn / effect hebben;
- Een toestemming of bezwaar moet betrouwbaar zijn en rechtsgeldig;
- Een toestemming of bezwaar vereist eenheid van taal en techniek.

Wij lichten deze uitgangspunten nader toe.

### 4.1.1 Een patiënt heeft overzicht over zijn hele zorg

In de zorg is vaak gezegd dat de patiënt ‘centraal’ moet staan. In de praktijk werd dit gerealiseerd door een zorgaanbieder die de patiënt centraal stelde. Als een patiënt dan van de ene zorgaanbieder naar de andere moest, was er toch een probleem (ook al stond de patiënt bij de andere zorgaanbieder ook ‘centraal’): in het zorgproces tussen zorgaanbieders was de patiënt nog steeds op zichzelf aangewezen. Een online toestemmingsvoorziening stelt de patiënt centraal in het hele zorgproces over alle zorgaanbieders heen. Dat pas geeft de patiënt overzicht en regie mogelijkheden. De impact is dat voor elke patiënt er een voorziening moet zijn waar alle zorgaanbieders gebruik van moeten kunnen maken. Omdat er geen wettelijke verplichting is voor het gebruik van een bepaalde online toestemmingsvoorziening, zal elke online toestemmingsvoorziening zodanig ontworpen moeten worden dat alle zorgaanbieders er gebruik van moeten kunnen maken.

Daarnaast komt de patiënt pas echt in de regie als niet alleen alle toestemmingskeuzes vanaf één plek beheerd kunnen worden, maar als het effect van die toestemmingskeuzes ook transparant is. Ook hier geldt: vertrouwen in behandelaars en hun systemen is goed, maar controle is beter. Een online toestemmingsvoorziening zal de patiënt inzage moeten geven in de zorgaanbieders die gegevens hebben uitgewisseld en daartoe de toestemmingskeuzes van de patiënt geraadpleegd hebben. Welke zorgaanbieders de toestemmingskeuzes hebben gebruikt en op welke tijdstippen moet vanaf één plek zichtbaar zijn. Idealiter moet de patiënt die dat wil hierover per email direct een notificatie kunnen ontvangen. Daarnaast moet het transparant zijn voor de patiënt die is ingelogd in een online toestemmingsvoorziening, wie van alle zorgaanbieders in Nederland, dossiergegevens van deze patiënt hebben en of die zorgaanbieders gebruik maken van de toestemmingen uit die online toestemmingsvoorziening. Tenslotte: ook als vertegenwoordigers van de patiënt toestemmingskeuzes registreren in opdracht van of onder mandaat of machtiging van de patiënt moet het mogelijk zijn een email-notificatie te ontvangen van elke wijziging in het toestemmingsprofiel van de patiënt.

### 4.1.2 Een gemeenschappelijke dienst moet voor alle patiënten toegankelijk zijn

Hoewel ‘de patiënt’ een erg generiek term is, zal een online toestemmingsvoorziening als gemeenschappelijke dienst geschikt moeten zijn voor verschillende doelgroepen om een zo groot mogelijke inclusie te realiseren. Het gaat bij online diensten in ieder geval om:

- Digitaal vaardige burgers met een DigiD;
- Personen die geen digitale middelen willen of kunnen gebruiken;
- Kinderen jonger dan 12 jaar of tussen 12 en 16 jaar.

Het type zorg dat verleend wordt is hierbij breed: alles wat onder de verzorging (‘care’) of behandeling (‘cure’) valt; meer concreet: de zorg zoals bedoeld in de Wkkgz. De reikwijdte van de ‘Wet kwaliteit, klachten en geschillen zorg’ (Wkkgz) is heel

ruim, ruimer dan die van de oorspronkelijke Kwaliteitswet zorginstellingen, de Wet klachtrecht cliënten zorgsector (WKCZ), de Wet BIG en het voormalige wetsvoorstel Wet cliëntenrechten zorg. Onder de Wkkgz vallen alle zorgaanbieders, niet alleen de 'cure', maar ook de 'care', zowel instellingen als solistisch werkende zorgverleners, waaronder de geestelijke gezondheidszorg (ggz), de verpleging, verzorging en thuiszorg (de VVT-sector) en de eerste lijn zoals de huisartsenzorg.

Ook patiënten die eigenlijk geen patiënt zijn omdat ze niet actief behandeld worden, maar alleen ingeschreven zijn bij een huisarts horen tot de doelgroep, maar ook patiënten met een diversiteit aan klachten en behandelingen, tijdelijk of chronisch, intensief of niet-ernstig, die een beroep kunnen doen op planbare zorg of spoedbehandeling.

De informatie verstrekking aan 'de patiënt' moet daarmee in een online toestemmingsvoorziening voor een brede doelgroep begrijpelijk zijn.

#### **4.1.3 Een toestemming of bezwaar moet voor alle uitwisselingen beschikbaar zijn**

Veel patiënten kennen geen onderscheid niet tussen uitwisselingen die op basis van een veronderstelde toestemming verlopen en uitwisselingen die een uitdrukkelijke toestemming vereisen. Ook zijn de meeste patiënten niet bekend met de verschillende inrichtingen van uitwisselingssystemen. De registratie van een toestemming of bezwaar moet daarom aan de ene kant helder en begrijpelijk zijn voor de patiënt en aan de andere kant tevens juridisch rechtmatig en voldoen aan de verschillende voorwaarden voor de verschillende situaties.

Het doel van een online toestemmingsvoorziening blijft: de patiënten een mogelijkheid geven regie uit te oefenen op het uitwisselen van gegevens tussen de zorgaanbieders die hen behandelen. Uitwisseling van relevante gegevens kan bijdragen aan de kwaliteit van de zorgverlening over zorgaanbieders heen, door het borgen van:

- continuïteit in de zorgverlening,
- actualiteit van de gegevens die nodig zijn voor de zorgverlening en
- beschikbaarheid van de gegevens op het juiste moment en de juiste plek van de (be)handeling.

Reeds bestaande uitwisselingen moeten ook via een online toestemmingsvoorziening door de patiënt geautoriseerd kunnen worden. Dat betekent dat een online toestemmingsvoorziening rekening moet houden met de toestemmingen en bezwaren die al eerder door de patiënt zijn gegeven. Bestaande toestemmingen moeten daarom migreerbaar zijn.

#### **4.1.4 Een toestemming of bezwaar moet direct geldig zijn / effect hebben**

Een online voorziening geeft het gevoel dat je als patiënt daadwerkelijk 'achter de knoppen' zit en regie kan voeren. Dat betekent dat er 'achter de schermen' sprake moet zijn van een snel en betrouwbaar communicatie netwerk waardoor de zorgaanbieders, ook als ze dicht zijn, toch gegevens kunnen uitwisselen als dat gewenst en toegestaan is.

Als een behandelaar tegen de patiënt zegt gegevens te willen versturen naar een andere zorgaanbieder en de patiënt maakt ter plekke bezwaar, dan zal de zorgaanbieder afzien van het versturen van die gegevens. Als een behandelaar tegen de patiënt zegt gegevens te willen opvragen bij een andere zorgaanbieder en de patiënt maakt ter plekke bezwaar, dan zal de zorgaanbieder afzien van het opvragen van die gegevens. In beide situaties is het registreren van bezwaar niet relevant: het bezwaar is direct geldig en effectief.

Als een patiënt bij een behandelaar is en geen expliciet bezwaar maakt, mag de behandelaar in bepaalde situaties een toestemming 'veronderstellen' en kan uitwisseling ter plekke worden gerealiseerd. Bij een later verzoek om meer gegevens kan de 'dossierhouder' op basis van dezelfde veronderstelde toestemming extra gegevens opsturen, indien de dossierhouder aanwezig is. Als een patiënt bij een behandelaar is die gegevens wil opvragen bij een andere behandelaar en de patiënt geeft hiervoor expliciet toestemming, dan is dat niet altijd voldoende om de uitwisseling direct te effectueren. Want anders dan veel patiënten denken, is de expliciete toestemming in eerste instantie niet nodig voor het raadplegen of het inzien van de gegevens, maar eerst voor het doorbreken van het beroepsgeheim van de zorgaanbieder die het dossier voert (degene die gegevens moet opsturen). Als deze 'dossierhouder' aanwezig is, kan de uitwisseling direct geregeld worden. Als in deze beide situaties de dossierhouder niet aanwezig is, moet de uitwisseling toch direct geregeld kunnen worden, immers de patiënt heeft in de eerste situatie geen expliciet bezwaar gemaakt en in de tweede situatie zelfs expliciet toestemming gegeven. Om de uitwisseling geautomatiseerd door te laten gaan, ook als de dossierhouder niet aanwezig of niet beschikbaar is, moet de toestemming of het (ontbreken van) bezwaar expliciet worden geregistreerd en deze registratie moet voor de dossierhouder te vertrouwen zijn, zodat de systemen in zijn afwezigheid het kunnen afhandelen. Dat vereist een overkoepelend vertrouwensmodel waarin concrete afspraken over betrouwbaarheid, onweerlegbaarheid of integriteit, en vertrouwelijkheid zijn geborgd (de zogenaamde BIV van privacy- en informatiebeveiliging).

Voor de ondersteuning van het zorgproces levert dit een belangrijke meerwaarde: een online toestemmingsvoorziening moet de 'ad-hoc' functie van toestemming verlenen ondersteunen, zodat de discrepantie van de verwachting van de patiënt ('ik geef de behandelaar toch toestemming om gegevens in te zien') en het vereiste van de wet ('de dossierhouder kan alleen gegevens delen als de patiënt toestemming heeft gegeven om gegevens te delen') beide wordt gehonoreerd. Omdat hiervoor technisch het nodige geregeld moet worden, is dit tot nu toe niet van de grond gekomen, maar het kan met een online toestemmingsvoorziening worden gerealiseerd dat ingebed is in een afsprakenstelsel op basis van geborgd een aantoonbaar vertrouwensmodel.

#### **4.1.5 Een toestemming of bezwaar moet betrouwbaar zijn en rechtsgeldig**

Bij een toestemming of bezwaar wordt vaak alleen bedoeld op de toestemmingskeuze van de patiënt. Een 'ja' is een expliciete toestemming en een 'nee' is een expliciet bezwaar. Het effectueren van een toestemming of bezwaar zou dan 'alleen maar' het communiceren van een 'ja' of een 'nee' zijn.

Echter, een toestemming of bezwaar is bedoeld om een uitwisseling te autoriseren of te blokkeren en daarvoor zijn meer voorwaarden nodig. Zo mag een toestemming niet verondersteld worden als de patiënt geen bezwaar mogelijkheid heeft gehad en de patiënt moet daarover geïnformeerd worden. Wil een expliciete toestemming (een 'ja') een rechtsgeldige grondslag zijn voor het delen van gegevens, dan moet die toestemming (conform AVG):

- eenduidig zijn;
- specifiek zijn;
- onweerlegbaar zijn;
- in vrijheid gegeven;
- gebaseerd op goede informatie;
- die begrijpelijk is;
- net zo makkelijk intrekbaar zijn;
- aantoonbaar zijn.

Deze vereisten stellen serieuze voorwaarden aan de betrokken partijen en hun systemen. Zo vraagt de eis om eenduidigheid om het gebruik van (inter)nationaal unieke identificaties; de eis van onweerlegbaarheid om het gebruik van adequate authenticatie (ook van degenen die de patiënt vertegenwoordigen); de eis van specificiteit en de eis van begrijpelijkheid vragen om een balans tussen niet teveel toestemmingen (onbegrijpelijk) en niet te weinig (dat is niet specifiek). Een online toestemmingsvoorziening dient blijvend te voldoen aan al deze eisen.

#### **4.1.6 Een toestemming of bezwaar vereist eenheid van taal en techniek**

Om te voorkomen dat de wildgroei van toestemmingsformulieren en toestemmingsvragen toeneemt, is het van belang dat bij het verkrijgen van een toestemmingskeuze, of dat nu per formulier, digitaal of via een online toestemmingsvoorziening verloopt, dezelfde taal wordt gebruikt voor de toestemmingsvragen. Dat is niet vanzelfsprekend. Zo moet een patiënt een individuele zorgaanbieder die zijn/haar behandelaar is en in dat kader dossiergegevens beheert, eenduidig kunnen vinden. Omdat artsen zelf een eigen praktijk kunnen starten en, bijvoorbeeld bij pensionering, weer kunnen stoppen en omdat grote instellingen regelmatig fuseren, vereist dit een registratie van 'solisten met een BIG registratie' en van 'organisaties die zorg mogen en kunnen verlenen'. Die registratie moet eenzelfde taal hanteren voor (digitale) vindbaarheid door patiënten online.

Daarnaast moet een patiënt ook een toestemmingskeuze kunnen registeren voor categorieën van zorgaanbieders, omdat niet altijd van te voren bekend is bij welke zorgaanbieders de patiënt terecht komt, bijvoorbeeld bij welke apotheek de medicatie opgehaald wordt, of door bij welke therapeut de patiënt uiteindelijk het beste behandeld wordt. Om van te voren voor de hele zorg toestemmingskeuzes te kunnen bepalen, moet een patiënt dat ook per categorie van zorgaanbieders kunnen doen. Daarbij vergt het vinden van een werkbare en juridisch juiste balans in het aantal toestemmingsmogelijkheden voor de hele zorg eenheid van taal. Het categoriseren van zorgaanbieders op een begrijpelijke wijze die overzichtelijk is en tegelijk specifiek genoeg is, vereist afstemming en uniformering.

Omdat de toestemmingskeuze geldig zijn voor uitwisselingen via de systemen van de zorgaanbieders, moet er ook eenheid zijn in de techniek. Allereerst om de uitwisselingen onder te brengen in de eenheid van taal die voor de toestemmingsmogelijkheden is gebruikt. Immers, een toestemming om medicatiegegevens van de eigen apotheek te delen met andere apotheken die direct bij een behandeling betrokken zijn, is alleen maar geldig voor apotheken en alleen maar voor medicatiegegevens. Zoals de patiënt geïnformeerd is bij het registreren van een toestemmingskeuze, zo moet het ook in de techniek van de uitwisseling geëffectueerd worden. Voor alle duidelijkheid: bij deze eenheid van taal gaat het niet om het

uniformeren van de uitwisselingen zelf, maar om het mappen van de attributen van elke mogelijke uitwisseling op een uniforme set van begrippen die in de toestemmingsvraag worden gebruikt.

Als een zorgaanbieder moet kunnen vast stellen of er een juiste grondslag is voor de uitwisseling (bv. een expliciete toestemming of de afwezigheid van een expliciet bezwaar), moet de specifieke uitwisseling door de systemen die de zorgaanbieder hiervoor gebruikt worden gemapt. Voor het gebruik maken van toestemmingskeuzes die in een online toestemmingsvoorziening zijn vastgelegd, moeten systemen weten welke toestemmingskeuze gecheckt moet worden. Om de toestemmingskeuze die in een online toestemmingsvoorziening zijn geregistreerd toegankelijk te maken voor alle systemen, dienen de technische koppelvlakken met een online toestemmingsvoorziening eenduidig gespecificeerd te zijn op basis van open standaarden.

## 4.2 Verdieping juridisch kader

### 4.2.1 Wetgeving met betrekking tot toestemming en bezwaar

Een rechtmatige toestemming moet voldoen aan het huidige wettelijk kader (WGBO, AVG en Wabvpz, zie voor de onderlinge samenhang het 'Juridisch kennisdocument toestemmingen' [www.programma-otv.nl/nieuws/](http://www.programma-otv.nl/nieuws/)). 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.

Nota bene: 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 een online toestemmingsvoorziening 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 onder andere 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)
- Brieven van minister VWS over elektronische gegevensuitwisseling in de zorg (2019 en 2020)

## 4.3 Verdieping vertrouwensaspecten

### 4.3.1 Context

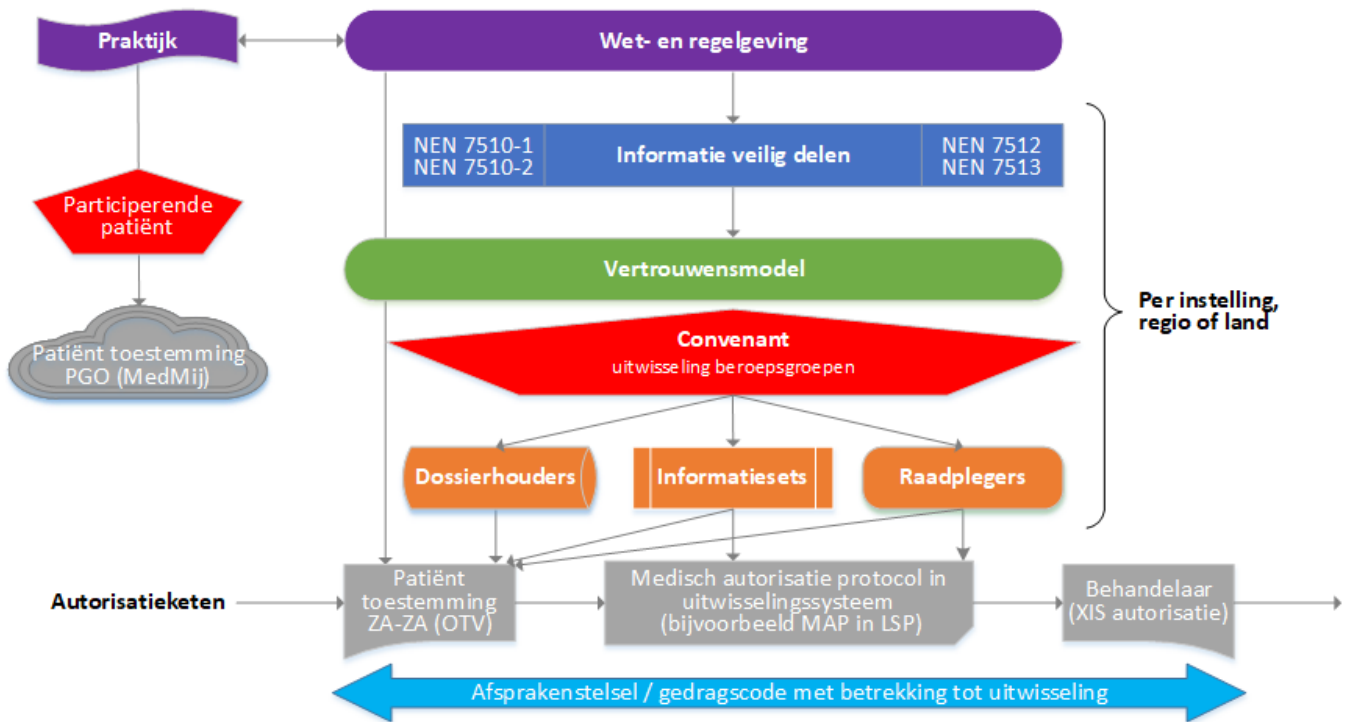
Een toestemming of bezwaar staat niet op zichzelf, maar staat in de context van het (elektronisch) uitwisselen van privacygevoelige gegevens. Zowel de registratie van een toestemming of bezwaar als het gebruik of effect hiervan in de uitwisseling moet het vertrouwen van alle betrokken partijen hebben. Daarbij gaat het om patiënten (als verzamelterm voor personen/burgers/cliënten/patiënten) die betrokken zijn omdat de gegevens over hen gaan en omdat hun privacy beschermd moet worden. Het gaat om zorgaanbieders die voor een kwalitatief goede zorg soms gegevens van andere zorgaanbieders nodig hebben, conform een gezamenlijk opgestelde beroepsrichtlijn, en daarbij afhankelijk zijn van de toestemming (verondersteld of uitdrukkelijk) van de betreffende patiënt. Ook gaat het om de leveranciers die als verwerker van gegevens betrokken zijn bij de opslag, uitwisseling, en inzage en daarbij diverse registraties gebruiken.

Uitwisseling van privacy gevoelige gegevens in een keten van partijen vraagt om een overkoepelend model waarin vertrouwen tussen alle partijen wordt afgesproken, immers de sterkte van de keten wordt bepaald door de zwakste schakel. Het borgen van de afspraken kan via aansluiting op een gemeenschappelijke dienst. Een online toestemmingsvoorziening die voor alle patiënten en voor alle zorgaanbieders en voor alle uitwisselingen (-uitwisselingssystemen) beschikbaar is, kan ook hiertoe dienen.

### 4.3.2 Vertrouwensmodel

Het vertrouwensmodel dat hoort bij zorgaanbieders die via een uitwisselingssysteem gegevens delen, 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 (controleerende) 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 waarbinnen een online toestemmingsvoorziening geïmplementeerd is

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 uitwisselingssysteem.

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 rond de 30 mogelijkheden / toestemmingsvragen.

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 dit opzicht rechtsgeldig zijn. Zo is in de "Richtlijn gegevensuitwisseling huisarts-huisartsenpost" precies bepaald wat in de 'samenvatting patiëntendossier' relevante gegevens zijn voor de huisartsgeneeskunde. In de "Richtlijn Medicatieoverdracht in de keten" bevat een opsomming van wat nodig en relevant is voor een actueel medicatieoverdracht. Bij de implementatie van dergelijke richtlijnen in de uitwisseling heeft dat bv. bij het Landelijk Schakelpunt 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.

Voor een veilige uitwisseling van gegevens, moet de patiënt voldoende vertrouwen hebben in de privacy- en informatiebeveiliging van de zorgaanbieders die gegevens van de patiënt verwerken ongeacht op welke uitwisselingssystemen deze zorgaanbieder is aangesloten. Ook moet er vertrouwen zijn in de rechtsgeldigheid van de toestemmingskeuzes. Daarom is een overkoepelend afsprakenstelsel waar ook een online toestemmingsvoorziening onderdeel van is, van belang. De beheerders van een uitwisselingssysteem dat op Mitz aansluit zal deze afspraken moeten onderschrijven en waar nodig verwerken in hun afspraken met zorgaanbieders die bij hen aansluiten.

#### **4.3.3 Voldoen aan NEN-normen en BSN gebruik**

Bij oplevering zal een online toestemmingsvoorziening 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.

#### **4.3.4 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. Een online toestemmingsvoorziening 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 een online toestemmingsvoorziening 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 een online toestemmingsvoorziening als zodanig behandeld en beschermd worden. Conform de ‘Algemene verordening gegevensbescherming’ (AVG) behoort een online toestemmingsvoorziening de volgende principes toe te passen:

- 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).

#### **4.3.5 Ruimte voor (regionale) ontwikkelingen**

Nieuwe uitwisselingen die nog geen landelijke dekking hebben, en nog niet gevat zijn in een landelijke toestemmingsmogelijkheid, 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 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.

#### **4.3.6 Buiten scope van een online toestemmingsvoorziening**

Een online toestemmingsvoorziening als generieke dienst voor de elektronische uitwisseling tussen zorgaanbieders, gaat niet over:

- MedMij toestemmingen: 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 lab-bepalingen kunnen opvragen rechtstreeks bij de bron. Dit is de enige toestemming voor raadpleging. (artikel 15b uit de Wabvpz is komen te vervallen).

## 4.4 Verdieping inpassen in de zorgprocessen

### 4.4.1 Open standaarden voor raadpleging van een online toestemmingsvoorziening

Om alle zorgaanbieders de mogelijkheid te bieden voor alle uitwisselingen te werken met één online toestemmingsvoorziening, zal een toestemmingsregister via open standaarden raadpleegbaar moeten zijn. Open standaarden kunnen door iedere leverancier van elk (uitwisselings)stelsel worden ingebouwd en is daarmee 'infrastructuur agnostisch'.

### 4.4.2 Kentallen voor beschikbaarheid van een online toestemmingsvoorziening als gemeenschappelijke dienst

Gemeenschappelijke diensten, zoals authenticatiediensten (DigiD) en routeringsdiensten (TVS) moeten eigenlijk altijd beschikbaar zijn. Concrete eisen aan performance (o.a. responstijd) en beschikbaarheid (uptime en uitval) zijn nodig zodat afnemers van deze diensten er op kunnen vertrouwen. Ook voor een voorziening die als bron voor toestemmingen functioneert, moeten de eisen hoog zijn. Niet alleen voor het registreren en intrekken van toestemming en bezwaar, maar ook voor het autoriseren van een uitwisseling. Voor een inschatting van de dimensionering van een online toestemmingsvoorziening die open staat voor alle uitwisselingsystemen, is het nodig dat alle bestaande uitwisselingen minimaal afgehandeld kunnen worden. Omdat de verwachting is dat eerst uitwisselingsystemen die uitwisselen op basis van uitdrukkelijke toestemming gebruik zullen maken van een online toestemmingsvoorziening, moet een online toestemmingsvoorziening gedimensioneerd worden op minimaal de load van deze systemen.

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. Daarmee is DigiD met sms/app een breed beschikbaar authenticatiemiddel voor het BSN domein 'zorg'.

### 4.4.3 Passend in de keten

Ten aanzien van de zorgprocessen gelden de volgende uitgangspunten:

- 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).

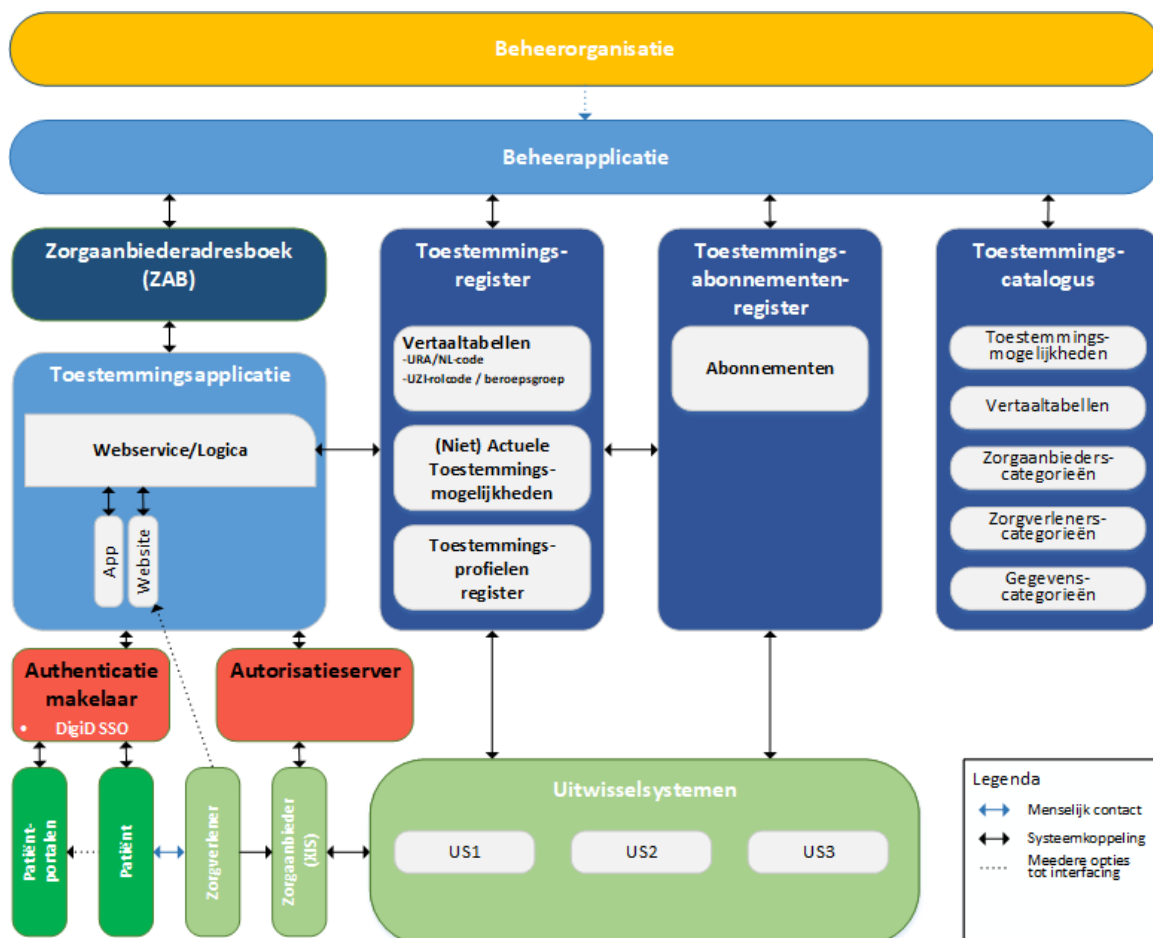


Mitz is een generieke dienst voor patiënten en zorgaanbiders/zorgverleners die voldoet aan de uitwerking van een online toestemmingsvoorziening. Wij lichten de opzet en werking van Mitz nader toe.

## 5.1 Opzet Mitz

Op hoofdlijnen bestaat de online toestemmingsvoorziening '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 zorgaanbiders 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 zorgaanbiders zich kunnen abonneren, zodat ze genotificeerd worden als er een relevante toestemmingskeuze gewijzigd is. Zorgaanbiders 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

### 5.1.1 Hoofdprocessen vastlegging toestemming

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) toestemmingskeuzes te registreren voor de elektronische uitwisseling van zijn gegevens tussen zorgaanbieders. Iedere patiënt krijgt hierdoor de mogelijkheid om 'proactief' toestemmingen vast te (laten) 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* beschikbaar gesteld, zodat de behandelende zorgverlener de gegevens direct tijdens het consult kan raadplegen.

Bij het delen van gegevens via een uitwisselingssysteem dat aangesloten is op Mitz, hebben de zorgaanbieders afgesproken dat via de systemen eerst vastgesteld wordt of de benodigde grondslag aanwezig is (expliciete toestemming of geen bezwaar), alvorens de gegevens elektronisch worden uitgewisseld.

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 beschikbaar te stellen, er van uit mag gaan dat de dossierhoudende zorgaanbieder(s) de betreffende gegevens direct beschikbaar stelt als een raadplegende zorgaanbieder daarom vraagt<sup>1</sup>. Als de zorgverlener die het dossier beheert op dat moment niet in de zorginstelling aanwezig is, bijvoorbeeld in de 'avond / nacht / weekend' (ANW) of tijdens vakantie, worden de systemen zodanig ingericht 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.

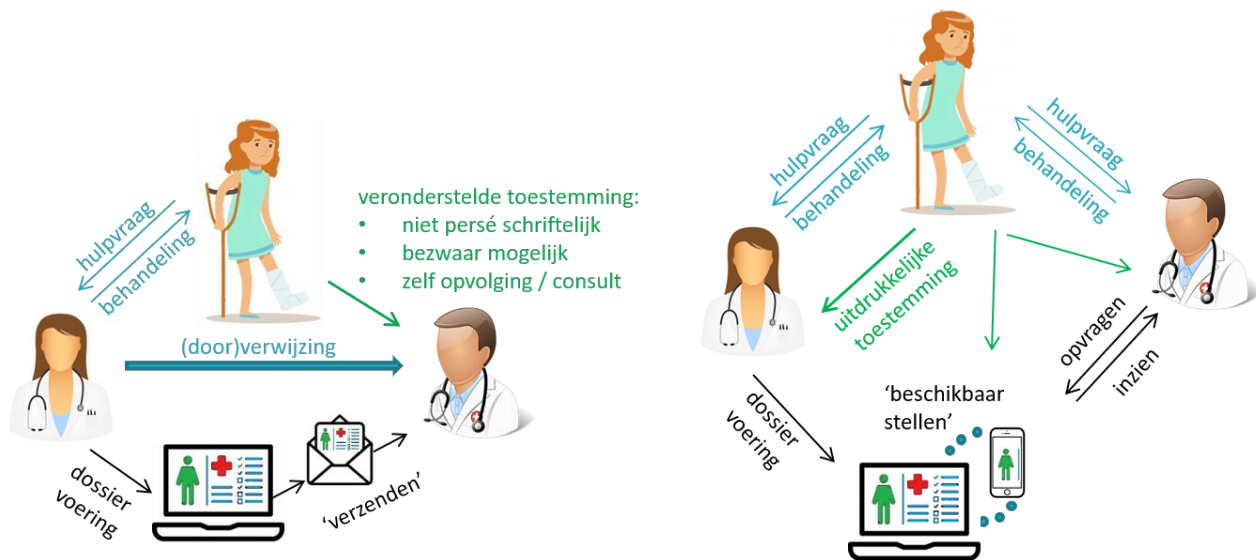
### 5.1.2 Toepassingsgebied

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 (bv ophalen uit een mailbox) en kan een juridische pull technisch worden uitgevoerd als een technische pull of als een push (bv. 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.

Nota bene: 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).

<sup>1</sup> De zorgaanbieder kan hierop een uitzondering maken per patiënt.



Figuur 3: Twee situaties: Verzenden met veronderstelde & 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 toestemmingskeuze op basis van een uniek nummer van de patiënt.
3. Communicatie naar de (dossierhoudende) zorgaanbieders wanneer toestemmingskeuzes 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.

### 5.1.3 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
  1. bijvoorbeeld ouder / voogd bij kinderen of
  2. aangewezen personen bij 'onder-curatele-gestelden' of 'wilsonbekwamen' (zodra de benodigde registers beschikbaar zijn) of
- door de patiënt gemandateerden, bijvoorbeeld een mantelzorger (zodra DigiD-machtigen voor de zorg beschikbaar is)
- of, in bepaalde situaties, door een bekende zorgverlener die de uitvoering namens de patiënt ter hand neemt.

#### Verantwoordelijkheid zorgaanbieder

Het beheer van de *geregistreerde* toestemmingen (in de papieren wereld: het beheer van de toestemmingsformulieren) is een verantwoordelijkheid van de (dossierhoudende) zorgaanbieder. Dat wordt door de zorgaanbieder 'uitbesteed' aan Mitz.

## 5.2 Werking Mitz-componenten

### 5.2.1 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 uitwisselingssysteem 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.

Mitz is 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.

Let wel:

- De patiënttoestemming in Mitz overrulet niet het medisch autorisatieprotocol waarmee de gegevens op basis van een beroepsrichtlijn worden beperkt tot datgene wat nodig en relevant is (dat zou een patiënttoestemming in MedMij via een PGO wel kunnen). Bijvoorbeeld: als het medische autorisatieprotocol 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.
- De gegevenscategorieën die in Mitz aan de patiënt worden getoond bij het registreren van een toestemming, moeten te mappen zijn op de gegevenscategorieën van de huidige uitwisselingen. Als die mapping niet 1:1 is te maken, zullen de consequenties per toestemmingsmogelijkheid of per uitwisseling bepaald worden.
- 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 in de wachtkamer kunnen het beheer van toestemmingen nog makkelijker maken.

## Ouder-Kind 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  $\geq 16$  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.

### 5.2.2 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 benodigde grondslag in de vorm van een aanwezige toestemming of een afwezig bezwaar geregeld is.

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 toestemmingskeuzes is beschreven.

Deze vorm van toestemming of bezwaar doet niets af van het recht dat een patiënt heeft om (in uitzonderlijke situaties) bepaalde elementen 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 lab-order 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 gegevenselement van belang dat de zorgaanbieder de patiënt kan wijzen op de (mogelijke negatieve) impact die het heeft voor de continuïteit van de zorgverlening, omdat andere gegevens wel gedeeld worden.

Aan het toestemmingsregister kunnen (door of via een uitwisselingssysteem) 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 het delen van gegevens met een andere zorgaanbieder is toegestaan. In de gesloten vraag kan een raadpleger aangeven of er sprake is van een spoed situatie of een normale situatie. Ook kan per uitwisseling worden aangegeven of hiervoor een veronderstelde of een uitdrukkelijke toestemming nodig is. Immers, bij een niet beantwoorde toestemmingskeuze, mag er wel worden uitgewisseld in een opt-out situatie, maar niet in een opt-in situatie.

### 2) De open autorisatievraag

Deze vraag wordt aan Mitz gesteld namens raadplegende zorgverleners en geeft antwoord op de vraag welke dossierhoudende systemen geraadpleegd mogen en kunnen worden (als filter om hele lange lijsten te voorkomen) voor één of meer gegevenscategorieën. Uitwisselingssystemen die geen eigen index hebben of deze niet meer willen/kunnen/mogen gebruiken kunnen zo een legitieme lokalisatie organiseren.

## 5.2.3 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.

## 5.3 De toestemmingscatalogus

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



Figuur 4: Structuur van een toestemmingsmogelijkheid

### **Zorgaanbiedercategorieën**

Een toestemming of bezwaar 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 beschikbaar stellen 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 uitgangspunten:

- 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.
- conform het vertrouwensmodel mogen medische gegevens alleen uitgewisseld worden als er in de uitwisseling geborgd is dat voldaan is aan de eis 'indien relevant en noodzakelijk' (zie paragraaf 4.3.2 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. De patiënt hoeft hier in de toestemmingskeuze geen rekening mee te houden. Het filter wordt door een uitwisselingssysteem of door het bronsysteem van de dossierhouder toegepast (op basis van de beroepsgroep van de raadplegende zorgverlener). Een toestemming in Mitz overrulet dus niet de zorgvuldig afgestemde informatiestandaarden voor gegevensuitwisseling tussen zorgaanbieders.
- 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'.
- Omdat uitwisselingssystemen verschillende technische implementaties kunnen hebben van de gegevenssets die uitgewisseld mogen worden, 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 aan wie gegevens beschikbaar gesteld mogen worden. Raadplegende zorgverleners (of de door hen 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:

1. 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 zorgaanbieder categorie van een raadplegende zorgaanbieder vertaald naar de zorgsector waar de patiënt een toestemmingskeuze voor heeft vastgelegd.

2. 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 van Mitz staan de toestemmingsmogelijkheden die dekkend zijn voor de gegevensuitwisselingen waarvan verwacht wordt dat deze binnen nu en 12 maanden operationeel zijn.

De toestemmingscatalogus bevat samengevat 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 (bv. 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 uitwisselingssysteem worden ondersteund, zullen (in afstemming met Mitz) door een uitwisselingssysteem 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 toesteminsapplicatie.

## 5.4 Werking Mitz via uitwisselingssystemen

### 5.4.1 Uitwisselingssystemen

Zorgaanbieders wisselen gegevens doorgaans uit via uitwisselingssystemen. In (de front-end van) Mitz worden toestemmingen vastgelegd voor het delen van gegevens via uitwisselingssystemen. Het vaststellen of er toestemming is verleend of bezwaar is aangetekend t.b.v. een specifieke uitwisseling kan technisch gerealiseerd worden via een koppeling van een uitwisselingssysteem op (de back-end van) Mitz. Vanuit beheer oogpunt is de koppeling met Mitz vanuit een uitwisselingssysteem te verkiezen boven aansluiting van alle zorgaanbieders rechtstreeks 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 zorgaanbiederssystemen 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 uitwisselingssysteem dat daarvoor geaccepteerd is, gebruikt kan worden. Een uitwisselingssysteem kan desgewenst ook een eigen lokaal toestemmingsregister bijhouden, voor de toestemmingsmogelijkheden waarvoor (nog) geen landelijke afspraken zijn vastgelegd in de toestemmingscatalogus.

### 5.4.2 Open standaarden voor raadpleging van een online toestemmingsvoorziening

Om alle zorgaanbieders de mogelijkheid te bieden voor alle uitwisselingen te werken met één online toestemmingsvoorziening, is het toestemmingsregister van Mitz via open standaarden raadpleegbaar. Open standaarden kunnen door iedere leverancier van elk (uitwisselings)systeem worden ingebouwd en daarmee is Mitz 'infrastructuur agnostisch'. Mitz ondersteunt de volgende open standaarden:

1. De koppelvlakken met uitwisselingssystemen zijn gebaseerd op IHE profielen
2. Voor de berichtinhoud is FHIR gebruikt (o.a. 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 ZIBs (bv. van de BGZ) in het model opgenomen.
7. Voor de categorieën zorgaanbieders wordt de ZorgKaart Nederland gebruikt (Patiënten Federatie)
8. Voor de beveiliging wordt uitgegaan van de informatiebeveiligingsnormen voor de zorg (NEN).

### 5.4.3 Omgang toestemmingen: zorgaanbieders versus zorgverleners

Er wordt onderscheid gemaakt tussen zorgaanbieders die dossiers voeren (en gegevens kunnen versturen of beschikbaar kunnen stellen) en de zorgverleners die vanuit een zorgaanbieder 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. Een raadplegende zorgverlener werkt vanuit een zorgaanbieder en de patiënt moet toestemming (verondersteld of uitdrukkelijk) hebben gegeven zodat die zorgaanbieder inzage krijgt in gegevens.

#### 5.4.4 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. Mitz is als online toestemmingsvoorziening immers de bron voor toestemmingen en bezwaren: patiënten kunnen op elke moment hun toestemmingskeuze aanpassen. Het vaststellen of er toestemming dan wel bezwaar is gebeurt ‘achter de schermen’, dat wil zeggen: zorgaanbieders kunnen dit ‘vaststellen’ delegeren aan Mitz (via hun uitwisselingssysteem dat op Mitz is aangesloten). Zorgaanbieders spreken af dat het uitwisselingssysteem dat de betreffende uitwisseling realiseert, eerst bij Mitz vaststelt of de benodigde grondslag aanwezig is, voordat de gegevens worden uitgewisseld.

#### 5.4.5 Vaststellen toestemming door zorgverleners die opvragen

De systemen van de zorgaanbieders kunnen voor het raadplegen van gegevens gebruik maken van Mitz via het betreffende uitwisselingssysteem. 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 of bezwaar voor een bepaalde gegevensuitwisseling, ongeacht het uitwisselingssysteem dat die uitwisseling realiseert. Daarbij geldt de toestemmingskeuze van de patiënt voor alle partijen in de uitwisselingsketen die verantwoordelijk zijn voor de gegevensverwerking van de uitwisseling.

#### 5.4.6 Voldoen aan NEN-normen en BSN gebruik

Mitz verwerkt als online toestemmingsvoorziening 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 beschikbaar stellen en raadplegen van gegevens verloopt via elektronische uitwisselingssystemen en wordt aldaar gelogd.

#### 5.4.7 De beheerapplicatie

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

### 5.5 Migratie van bestaande toestemmingen

Een onlinetoestemmingsvoorziening die door een patiënt wordt gebruikt, moet alle uitwisselingen kunnen ondersteunen, om het voor de patiënt overzichtelijk en begrijpelijk te houden. Een online toestemmingsvoorziening die alle uitwisselingen ondersteunt, zal ook de bestaande uitwisselingen met de reeds aanwezige toestemmingen en bezwaren moeten kunnen omvatten. Mitz heeft hiervoor een migratie-procedure ontwikkeld. Zorgaanbieders of regionale portalen die voor het uitwisselen van gegevens al toestemmingen en/of bezwaren 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 bv. 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.

### 5.6 Aansluitproces Mitz

De migratie van bestaande toestemmingen maakt bij Mitz onderdeel uit van het proces Technische Aansluiting Zorgaanbieder, ter onderscheiding van Organisatorische Aansluiting Zorgaanbieder (zie afsprakenstelsel). Het technisch aansluit proces 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.

### 5.6.1 Toestemmingen uploaden in Mitz

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 uitwisselingssysteem 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.

### 5.6.2 Gemigreerde toestemmingen inzien en aanpassen in Mitz

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 toestemmingen (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.

## 5.7 Operationele uitvoering

### 5.7.1 Convenant en dienstverlening

Koepelorganisaties van zorgaanbieders hebben vastgelegd in een convenant, gedateerd 25 maart 2019, dat zij Mitz als generieke, niet-commerciële oplossing wensen om de vereiste toestemmingen vast te leggen op basis waarvan er door een uitwisselingssysteem gegevens uitgewisseld kunnen worden. En hebben aan Stichting Servicecentrum VZVZ de opdracht gegeven de voorziening te realiseren. Inmiddels wordt ook vanuit de BIG5 programma's Mitz als belangrijke randvoorwaarde aangemerkt.

Mitz wordt in opdracht van de zorgaanbieders als dienstverlening door de Stichting Servicecentrum VZVZ als uitvoeringsorganisatie aangeboden. Binnen de Stichting wordt een apart onderdeel ingericht voor de Service en Beheerorganisatie van Mitz. Onder de dienstverlening van de Service en Beheer organisatie valt naast het dagelijks beheer van de applicatie bijvoorbeeld ook het informeren van burgers/patiënten en zorgaanbieders, het beheer / de doorontwikkeling van de toestemmingscatalogus en het begeleiden van het aansluitproces op Mitz. Een starterstoolkit met communicatiemiddelen maakt onderdeel uit van het aansluitproces. Voor de doorontwikkeling van de functionaliteit en het onderhoud van de toestemmingscatalogus wordt een aparte werkgroep ingesteld waarin relevante in- en externe expertise is vertegenwoordigd. Voorafgaand aan het doorvoeren van wijzigingen op de toestemmingskeuzes vindt validatie met zorgkoepels en de patiëntenfederatie plaats. Indien noodzakelijk kan dit leiden tot wijzigingen. Tevens biedt dit de mogelijkheid voor de koepels om tijdig hun leden te informeren. Afhankelijk van de impact van de wijzigingen zullen burgers geïnformeerd worden of moeten zij akkoord gaan voordat de wijziging geëffectueerd wordt. Waar nodig geacht worden, evenals in het initiële ontwikkeltraject, panels met patiënten ingezet om de gebruikersvriendelijkheid te toetsen. Dit geldt tevens voor de toetsing aan de WCAG2.1 AA (toegankelijkheid).

### 5.7.2 Financiering

Mitz kan door patiënten/burgers en zorgaanbieders om niet (gratis) worden gebruikt. De financiering van de activiteiten van Mitz wordt verzorgd door de zorgverzekeraars.

### 5.7.3 Proceswijzigingen

Met Mitz krijgt de patiënt één plek waar toestemmingskeuzes beheerd en ingezien kunnen worden. Tevens kan de patiënt inzien welke van de aangesloten zorgaanbieders een dossier van hem/haar voeren. Ook wordt inzicht gegeven in de zorgaanbieders die een verzoek hebben ingediend om gegevens op te vragen (en dus de toestemmingskeuze gecheckt hebben). Met Mitz heeft de patiënt één duidelijke plek waar hij terecht kan voor uitleg, vragen en nadere informatie over toestemmingen. Voor de patiënt ontstaat tevens uniformiteit in de toestemmingsvragen, omdat de informatieverstrekking en de toestemmingsvragen niet meer per zorgaanbieder of groep van zorgaanbieders ontwikkeld wordt. De patiënt krijgt tenslotte ook de mogelijkheid om zelfstandig, locatie- en tijdonafhankelijk de toestemmingskeuze te registreren. Dit in tegenstelling tot de huidige situatie, waar toestemmingen verdeeld over de informatiesystemen bij de dossierhoudende zorgaanbieders liggen, geen overzicht is bij welke zorgaanbieders wel of niet toestemmingskeuzes geregistreerd zijn en waarvoor in veel gevallen geldt dat deze toestemmingskeuzes niet digitaal toegankelijk of digitaal te wijzigen zijn voor patiënten.

Voor zorgaanbieders ontstaat met Mitz een situatie waarbij enerzijds de uitvoering van de registratie van toestemmingskeuzes (inclusief de informatievoorziening) en anderzijds de controle op de toestemmingskeuze wordt uitbesteed aan Mitz. Mitz voorziet hiermee tevens in het onderhoud en beheer van de toestemmingscatalogus in relatie tot vigerende wet- en regelgeving, waardoor de actualiteit van toestemmingen beter gewaarborgd kan worden. Bij aansluiting op Mitz zal de dossierhoudende zorgaanbieder zijn/haar patiënten op passende wijze moeten informeren. Tevens zal bij de aansluiting de dossierhoudende zorgaanbieder moeten bepalen op welke wijze patiënten worden gestimuleerd/gemotiveerd en ondersteuning krijgen bij het vastleggen van toestemmingskeuzes. Voor de zorgaanbieder betekent de inzet van Mitz een vermindering van de administratieve lasten, omdat de patiënt zelf zijn keuzes vastlegt. Indien de patiënt niet digitaalvaardig is, geldt de afspraak dat de dossierhoudende zorgaanbieder hierbij ondersteunt (zorgverlener namens patiënt). Nieuw is dat een raadplegende zorgaanbieder eveneens toestemmingskeuzes kan verwerken (ook alleen in het bijzijn van de patiënt), waardoor gegevens direct beschikbaar gemaakt kunnen worden.

**Om Mitz als generieke voorziening voor toestemming in Nederland beschikbaar te maken, worden de uitgangspunten en principes van DIZRA gehanteerd bij de ontwikkeling van Mitz.**

## 6.1 Uitgangspunten DIZRA toegepast op Mitz

Iedere betrokken partij die een rechtspersoon is, zal aan alle vigerende wet- en regelgeving moeten voldoen. Naast deze algemene eis zijn er een aantal uitgangspunten beschreven voor een duurzaam informatiestelsel voor de zorg dat functioneert als een referentie architectuur (dizra). Generieke diensten zoals een online toestemmingsvoorziening moeten aan deze uitgangspunten voldoen (zie <https://dizra.gitbook.io/dizra/manifest>). Deze paragraaf bevat een kort overzicht op welke wijze de DIZRA uitgangspunten passen bij de eerder beschreven uitgangspunten voor een online toestemmingsvoorziening in het algemeen en voor Mitz in het bijzonder.

### 6.1.1 Regie op de eigen gezondheidsdata

De patiënt krijgt meer regie als voorzieningen voor de patiënt niet per zorgaanbieder maar zorgbreed worden georganiseerd. Overzicht van de relevante en noodzakelijke toestemmingskeuzes en transparantie wat er met de gezondheidsdata gebeurt zijn voor een patiënt het best te organiseren vanaf één plek (een online toestemmingsvoorziening). Mitz faciliteert het vastleggen van toestemmingskeuzes voor alle zorgaanbieders via één applicatie (TAP), waarmee voor de patiënt de regie op de eigen gezondheid wordt verbeterd.

### 6.1.2 Gemeenschappelijke taal

Een toestemmingskeuze ('ja' voor een expliciet toestemming en 'nee' voor een expliciet bezwaar) wordt gegeven op een toestemmingsvraag of toestemmingsmogelijkheid. Het formuleren van de vraag en de daarin gebruikte begrippen (bv. welke zorgaanbieders en welke gegevenscategorieën) moet uniform zijn over alle toestemmingsvoorzieningen.

Mitz heeft een toestemmingscatalogus opgesteld die voor alle gebruikers (patiënten en zorgaanbieders) toegepast wordt. Deze toestemmingscatalogus kan ook voor andere toestemmingsvoorzieningen ingezet worden.

### 6.1.3 Data blijft onder verantwoordelijkheid van de bronhouder

Voor de uitwisseling van medische gegevens is het in Nederland goed gebruik om deze gegevens niet centraal op te slaan, maar onder verantwoordelijkheid van de bronhouder te houden. Dat is niet altijd eenvoudig, zeker niet bij het direct beschikbaar stellen van deze gegevens nadat een patiënt toestemming heeft gegeven. Een online toestemmingsvoorziening zal daar rekening mee moeten houden en dat proces moeten ondersteunen. Specifiek voor de toestemmingen zelf geldt dat deze gegevens weliswaar door een patiënt (of diens vertegenwoordiger) kan worden geregistreerd, maar het zijn de bronhoudende zorgaanbieders die moet vast stellen of er een juiste grondslag is voor het delen van gegevens (anders mag bv. het beroepsgeheim niet doorbroken worden). Dat de bronhouders het registreren van een toestemmingskeuzes via een online toestemmingsvoorziening regelen, doet daar niets aan af. Ook de registratie van zorgaanbieders die zich abonneren om genotificeerd te worden, zodra een van hun patiënten een toestemmingskeuze heeft geregistreerd voor deze zorgaanbieder, blijft onder verantwoordelijkheid van de bronhouder. Deze 'abonnement registratie' is dan ook niet in te zien door anderen dan de betreffende bronhouder en de patiënt, tenzij met toestemming van de patiënt.

Mitz werkt conform bovengenoemde uitwerking.

### 6.1.4 Gelijk speelveld voor alle leveranciers

Alle leveranciers van zorginformatiesystemen en van systemen voor de uitwisseling van medische gegevens tussen zorgaanbieders moet gebruik kunnen maken van een online toestemmingsvoorziening. Het werken met open standaarden op de koppelvlakken is daarom vereist. Daarnaast is er geen wettelijke verplichting om een specifieke online toestemmingsvoorziening te gebruiken, maar vereist de regie functie voor de patiënt (eerste uitgangspunt) o.a. dat er eenduidigheid is in de taal en techniek. Daarom zal een online toestemmingsvoorziening hier aan moeten voldoen.

Mitz biedt alle zorgaanbieders de mogelijkheid voor alle uitwisselingen te werken met één online toestemmingsvoorziening, het toestemmingsregister van Mitz is via open standaarden raadpleegbaar (zie 5.4.2.).

### 6.1.5 Duurzaamheid in een veranderend informatiestelsel

De toenemende informatisering en automatisering van de uitwisseling in de zorg en de politiek-bestuurlijke en juridische perspectieven hierop zijn ook aan verandering onderhevig. De afgelopen periode is er gediscussieerd over de grondslag voor de verschillende uitwisselingen in de diversiteit aan zorgprocessen waar deze uitwisselingen hun nut hebben. Dat heeft geleid tot nieuwe en aangepaste wet- en regelgeving. De discussie is daarmee niet geëindigd. Zorgaanbieders moeten hun systemen voortdurend aanpassen op nieuwe inzichten. Het belang van duurzame concepten en voorzieningen is daarom ook bij een online toestemmingsvoorziening groot. Of een specifiek uitwisseling een veronderstelde dan wel een uitdrukkelijke toestemming nodig heeft en of een specifieke uitwisseling in een normale situatie of in een spoed situatie plaatsvindt (wellicht nog met de bijzondere situatie van 'niet aanspreekbaar en levensbedreigend') wordt in Mitz configureerbaar gemaakt. Daarmee is de voorziening duurzaam en kan meebewegen met de veranderende inzichten hierin.

Daarnaast functioneert Mitz ook als een zogenaamd 'policy decision point'. Dat is een begrip uit de internationale XACML standaard voor toestemmingssystemen, het is het punt waar het besluit om uit te wisselen wordt bepaald. Door deze 'pdp' in een online toestemmingsvoorziening te positioneren, zoals Mitz doet, wordt het aanpassen en onderhouden van de toestemming als autorisatie voor uitwisseling duurzaam en hanteerbaar. Feitelijk komt het hier op neer: een 'ja' is een 'ja' en een 'nee' is een 'nee', maar geen toestemmingskeuze is voor de autorisatie soms een 'ja' en soms een 'nee' (bij een veronderstelde toestemming mag uitgewisseld worden, als een uitdrukkelijke toestemming nodig is niet). Met betrekking tot spoed: voor het opvragen van gegevens in een spoed situatie is een uitdrukkelijke toestemming vereist. Hierbij geldt dat alle toestemmingen die voor normale situaties zijn gegeven, ook voor spoed situaties gelden; en dat een 'nee' tegen uitwisseling in normale situaties kan samengaan met een 'ja' voor spoedsituaties.

De discussie over de bijzondere situatie 'niet-aanspreekbaar en levensbedreigend' loopt nog: wat als de patiënt niet van te voren deze toestemmingskeuze heeft gemaakt? Als voor deze uitzonderlijke situatie een veronderstelde toestemming geldt, is dat in Mitz op één plek configureerbaar. Omdat Mitz fungeert als 'pdp' hoeven de systemen voor de uitwisseling niet aangepast te worden.

### 6.1.6 Data wordt enkelvoudig geregistreerd t.b.v. van meervoudig gebruik

Ook toestemmingsgegevens worden op één plek onder verantwoordelijkheid van de bronhouder geregistreerd. Dat is de enige en actuele bron voor toestemmingen. Die bron wordt door de patiënt actueel gehouden. Deze ene registratie van toestemmingskeuzes wordt in een online toestemmingsvoorziening beschikbaar gesteld om gebruikt te worden door alle systemen voor alle uitwisselingen.

Mitz voldoet aan bovengenoemde uitwerking.

### 6.1.7 Data is machineleesbaar

Een online toestemmingsvoorziening is niet alleen digitaal aan de 'voorkant' waar de patiënt toestemmingskeuze registreert, maar ook digitaal aan de 'achterkant' waar systemen van zorgaanbieders kunnen vaststellen welke uitwisselingen er toegestaan zijn en welke niet. De data die via de koppelvlakken worden uitgewisseld zijn ook conform internationale open standaarden gespecificeerd en dus machineleesbaar. De patiënt krijgt inzage in deze gestructureerde gegevens, na het inloggen op Mitz als online toestemmingsvoorziening.

Mitz voldoet aan bovengenoemde uitwerking.

### 6.1.8 Federatieve samenwerking

Een online toestemmingsvoorziening moet ontworpen en ontwikkeld en onderhouden worden door de betrokken partijen: zorgaanbieders, patiënten, leveranciers.

Mitz is in een dergelijke federatieve samenwerking ontwikkeld. De ontwikkeling van Mitz dat door het Servicecentrum van VZVZ wordt uitgevoerd, werkt onder een convenant van zorgaanbieders (via hun koepels), heeft de Patiënten Federatie vanaf het eerste begin betrokken, en werkt nauw samen met de experts van leveranciers. Daarnaast wordt met enige regelmaat gewerkt met patiëntenpanels, individuele zorgaanbieders en de leveranciers van uitwisselingssystemen. Juridische toetsing en externe (beveiligings) audits vinden voortdurend plaats om de kwaliteit van de implementatie te kunnen aantonen.

### 6.1.9 Open internationale standaarden

Een online toestemmingsvoorziening hanteert zowel voor de taal als de techniek open standaarden. Daarbij geldt dat internationale standaarden het uitgangspunt zijn, en dat als die aangepast moeten worden, er een nationale variant

internationaal wordt afgestemd. Als er helemaal geen internationale standaard is of een internationaal codesysteem door zorgaanbieders helemaal niet gebruikt wordt, dan wordt een nationale standaard gebruikt die mapbaar moet zijn op internationale standaarden (zie ook 5.4.2).

Open internationale standaarden zijn het uitgangspunt voor alle architectuurkeuzes die Mitz heeft gemaakt. Deze zijn met de betrokken leveranciers afgestemd en worden voortdurend in een beheerproces besproken, omdat ook daar op het terrein van toestemming nog veel ontwikkeling in zit. Vanuit de realisatie van Mitz wordt samen met Nictiz, meegewerkt met landen die de internationale standaarden voor 'consent' implementeren in zorgbrede uitwisselingen.

## 6.2 Principes van DIZRA toegepast op Mitz

Op basis van deze uitgangspunten zijn de hierop gebaseerde basisprincipes goed te beschrijven.

1. Juist een online toestemmingsvoorziening zorgt er voor dat bij het verstrekken van gegevens rekening gehouden kan worden met de wensen en mogelijkheden van de patiënt.
2. Juist een online toestemmingsvoorziening maakt het mogelijk om gegevens te delen als de patiënt daar geen bezwaar tegen heeft of expliciet toestemming voor heeft gegeven als dat vereist is.
3. Juist met een online toestemmingsvoorziening kan een patiënt regie nemen op de gezondheidsgegevens.
4. Mitz voldoet aan de bovenbeschreven eisen voor een online toestemmingsvoorziening, met name ook met betrekking tot beveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) borgt het vertrouwen dat nodig is bij gegevensuitwisseling.
5. In Mitz is altijd duidelijk welke zorgaanbieder verantwoordelijk is voor de dossiervoering en voor het delen van gegevens uit dat dossier.
6. In Mitz is het toestemmingsprofiel van de patiënt (alle geregistreerde toestemmingskeuzes) eenvoudig door die patiënt in te zien en bij te houden.

Ook wordt voldaan aan de afgeleide principes:

1. De componenten van Mitz zijn ontworpen vanuit de eindgebruiker: de voorkant vanuit patiëntperspectief en de achterkant vanuit zorgaanbieder perspectief ter ondersteuning van de zorgprocessen.
2. De functionaliteit van Mitz is bruikbaar voor alle zorgaanbieders, patiënten en hun systemen. De gebruiksvriendelijkheid van de 'user-interface' wordt met gebruikerspanels gevalideerd. Een gebruikersacceptatie test is vast onderdeel van deze componenten.
3. Mitz is ontworpen in lijn met de uitgangspunten en principes van de gemeenschappelijke afspraken over het informatiestelsel voor de zorg.
4. Mitz is federatief ontworpen en ontwikkeld.
5. De verantwoordelijkheden voor de verschillende gegevensverwerkingen zijn transparant en eenduidig beschreven.
6. De diversiteit aan uitwisselingen en behandelsituaties is op de informatielaag geharmoniseerd (eenheid van taal) en wordt tot en met de technische koppelvlakken gestandaardiseerd (eenheid van techniek).
7. Toestemmingsgegevens worden beschouwd als bijzondere persoonsgegevens en als medische gegevens beschermd.
8. De kwaliteit van de dienstverlening wordt extern getoetst en de verantwoording daarover is transparant voor de deelnemers.
9. Mitz wordt als 'minimal viable product' gelanceerd met alle functionaliteiten die nodig zijn om aan de uitgangspunten recht te doen. Doorontwikkeling met extra functionaliteiten om het makkelijker te maken (bv. aansluiting op de diensten van BZK voor alle burgers) en innovaties die mogelijk worden naarmate er meer via wet- en regelgeving wordt afgedwongen (bv. Wegiz en handhaving op de NEN-normen) staan op de roadmap.
10. De toestemmingsgegevens blijven onder decentrale verantwoordelijkheid en worden onder verantwoordelijkheid van de bronhouder gebruikt voor de uitwisseling. Een raadplegende zorgaanbieder kan via zijn systemen (informatiesysteem en/of uitwisselingssysteem) gegevens opvragen bij bronhouders, en de bronhouders stellen via Mitz vast of de benodigde toestemming hiervoor aanwezig is. Hoe de zorgaanbieder zijn systemen organiseert (lokale pc onder het bureau, regionale of landelijke service providers) maakt niet uit zolang voldaan wordt aan de beveiligingsnormen voor de zorg.
11. Er is één bron voor toestemmingskeuzes en de patiënt houdt die actueel. Andere zorgaanbieders kunnen voor alle uitwisselingen deze toestemmingskeuzes steeds opnieuw gebruiken / checken.
12. De patiënt / cliënt / burger komt echt in de regie als het gaat over het delen van gegevens tussen zorgaanbieders.
13. De publiek beschikbare gegevens (bv. naam/adres/woonplaats van zorgaanbieders) zijn open en vindbaar voor de patiënt en de private gegevens (bv. naam/leeftijdscategorie/email van de patiënt) en welke zorgaanbieders zich op de toestemmingskeuzes van deze patiënt hebben geabonneerd) zijn gesloten en alleen met toestemming van de patiënt breder beschikbaar (bv. voor vertegenwoordigers of andere zorgaanbieders).

14. Mitz hanteert in de formulering aan de patiënt begrijpelijke teksten die gerelateerd zijn aan nationale codes. De eenheid van taal wordt gehanteerd waar die beschikbaar is (bv. de zorgaanbieder categorieën van ZorgKaart Nederland) en waar Mitz aanvullende codestelsels heeft gerealiseerd (bv. een begrijpelijke en overzichtelijke groepering van deze zorgaanbieder categorieën) zijn die open voor consultatie en verdere normering.
15. Machineleesbare gegevens geldt in Mitz zowel voor de voorkant (als een patiënt een zorgaanbieder selecteert om toestemming te geven, wordt achter de schermen een landelijk unieke code en systeemadressering gebruikt) als voor de achterkant (alle vertaaltabellen om uitwisselingen op de juiste toestemmingen te mappen zijn in de toestemmingscatalogus opgenomen).
16. Mitz hanteert het persoonlijk netwerk voor de gezondheid alleen voor de zorgverlening, omdat de scope van Mitz zich (op dit moment in de Minimal viable product fase) tot toestemmingskeuzes voor het delen van gegevens tussen zorgaanbieders. In later stadium is voorzien dat ook toestemmingskeuzes voor het delen van gegevens met als doel 'kwaliteitsbevordering en onderzoek' worden opgenomen en 'toestemmingskeuzes om het PGO als bron te bevragen'. Daarmee kan het persoonlijk netwerk voor de gezondheid desgewenst verder uitgebreid worden.
17. Het aantal toestemmingsmodelijkheden wordt zo beperkt mogelijk gehouden om het voor de patiënt begrijpelijk en overzichtelijk te houden. Om recht te doen aan de specificiteit is het noodzakelijk met meerdere toestemmingsmogelijkheden te werken, zodat de specifieke (categorie) van zorgaanbieders en de specifieke gegevens van die zorgaanbieder apart kunnen worden toegestaan of geblokkeerd. Daarnaast hanteert Mitz een strikt beleid met betrekking tot dataminimalisatie. Zo is een gemakkelijke 'broadcast naar alle zorgaanbieders om te kijken of ze gegevens van een patiënt hebben' niet toegestaan en wordt door Mitz niet ondersteund. Het abonnementenregister kan voor de noodzakelijke inperking en lokalisatie zorgen, maar is alleen toegankelijk na toestemming. De combinatie van toestemmingregister en abonnementenregister maakt de noodzakelijke performance (gegevens beschikbaar op het moment van behandeling) technisch ook haalbaar. Ook wordt de dataminimalisatie doorgevoerd in het persoonsprofiel en toestemmingsprofiel van de patiënt: alleen wat functioneel nodig is (in de MVP of in de geplande versies van de roadmap) wordt opgenomen. Het verwijderen van gegevens loopt conform de toepasselijke bewaartermijnen. Het inperken van de gegevens die door de patiënt worden toegestaan, op basis van wat 'relevant en noodzakelijk is voor de zorgaanbieder die de gegevens nodig heeft', hoeft de patiënt te weten bij het verlenen van toestemming, maar moet wel geïmplementeerd worden in de uitwisseling. Immers, toestemming als grondslag voor gegevensuitwisseling overrulet niet het proportionaliteitsbeginsel. Dus als de beroepsgroepen van zorgaanbieders hebben bepaald welke gegevens relevant zijn (proportioneel) dan mag een toestemming van de patiënt dat niet overrulen. Daarom zijn systemen van een zorgaanbieder (informatiesysteem of uitwisselingsstelsel) verplicht om de beroepsrichtlijnen (of kwaliteitsstandaarden zoals de Wegiz ze beschrijft) te implementeren, wil een uitwisseling rechtsgeldig zijn. Systemen die Mitz als online toestemmingsvoorziening gebruiken worden hierop getoetst.
18. Los van de toepassing van wet- en regelgeving, gaat de beheerorganisatie van Mitz (die namens de zorgaanbieders gegevens verwerkt) uitermate respectvol om met de gegevens. Het opbouwen van vertrouwen vergt veel aandacht maar is de basis voor uitwisseling van privacygevoelige gegevens in zorgnetwerken.
19. Gegevens van de patiënt zijn te allen tijde door de patiënt inzichtelijk via een web-portaal. Patiënten die zelf geen digitale middelen willen of kunnen gebruiken, kunnen via een vertegenwoordiger deze inzage organiseren. Bijvoorbeeld door het aan de zorgaanbieder te vragen.
20. De eenheid van taal wordt gerealiseerd los van transport van de data en de eenheid van techniek. De afstemming van de eenheid van taal vindt plaats direct met eindgebruikers en niet via leveranciers.
21. Open internationale standaarden zijn het uitgangspunt voor alle architectuurkeuzes die Mitz heeft gemaakt. Deze zijn met de betrokken leveranciers afgestemd en worden voortdurend in een beheerproces besproken, omdat ook daar op het terrein van toestemming nog veel ontwikkeling in zit. Vanuit de realisatie van Mitz wordt samen met Nictiz, meegewerkt met landen die de internationale standaarden voor 'consent' implementeren in zorgbrede uitwisselingen.