Voorstel voor werkgroep Toestemming requirements:

Categorieën van functies binnen een OTV ten behoeve van splitsing van requirements

Waar de Nen norm over generieke functies gaat waartegen leveranciers voorzieningen kunnen certificeren, gaan de werkgroepen van VWS over voorzieningen die nodig zijn om de afspraken in Wegiz en IZA te realiseren.

Bij het opstellen van requirements voor voorzieningen, kan ook een onderscheid worden gemaakt in functionaliteiten. Doel daarvan is dat onbedoelde, onnodige of ongewenste functionele koppelingen in de requirements worden gemaakt, waardoor die functies in één voorziening gerealiseerd moeten worden. Dus overal waar functionele ontkoppeling zinvol is, vanuit juridisch, technisch of privacy perspectief, zouden de requirements hiervoor ook apart gecategoriseerd moeten worden.

Dan kan bij de implementatie op applicatiearchitectuur niveau, nog steeds een keuze gemaakt worden of de verschillende functies in aparte voorzieningen gerealiseerd worden, of dat het wenselijk is om, vanwege juridische, technische, economische, beheersmatige, of privacy overwegingen sommige functies samen in een voorziening te realiseren.

De functionaliteiten die vanuit oogpunt van menselijke gebruikers (patiënten en zorgaanbieders) onderscheiden kunnen worden, zijn:

1. **Registratie** van toestemmingkeuzes, inclusief logging/transparantie en machtigingen.
2. **Effectuering/gebruik** van toestemmingskeuzes bij de uitwisseling van gegevens (via het uitwisselen van toestemmingskeuzes en/of een **PDP**, inclusief logging/transparantie)
3. **Lokaliseren** van dossierhouders obv toestemmingskeuzes, inclusief logging/transparantie en autorisatie: wie mag welke lokalisatie informatie zien / ontvangen?
4. **Inzage**/transparantie met betrekking tot (de logging van) transacties t.b.v. transparantie, bijv. via een portaal of een PGO

De eerste drie functies: **Registratie**, **Effectuering/PDP** en **Lokalisatie**[1] zijn de primaire functies van Mitz op dit moment. **Inzage**/transparantie is afgeleid, want heeft betrekking op informatie over het gebruik van de eerste drie functies.

Omdat transparantie-vereisten op alle drie functies: registreren, uitwisselen/PDP, en lokaliseren betrekking kunnen hebben, kunnen deze requirements deel worden gemaakt van de betreffende 3 categorieën. Er kan ook een vierde categorie voor worden aangemaakt, die dan de 3 andere categorieën omvat. In bovenstaand overzicht is gekozen om inzage/transparantie (van logging) deel te maken van zowel de categorieën 1-3, zodat eisen per functie kunnen worden uitgewerkt, als een aparte categorie 4 "**Inzage**" voor requirements m.b.t. inzage, die overkoepelend zijn.

Nota bene: logging/transparantie kan bij punt 2 mogelijk ook via een "doorkijk" naar de uitwisselingssystemen/bronsystemen gerealiseerd worden, met name als daar PDP functionaliteit in wordt geïmplementeerd.

Genoemde functies **Registratie**, **Effectuering/PDP**, **Lokalisatie** en **Inzage** lijken de belangrijkste functies voor het opsplitsen van de requirements.

[1] Lokalisatie is eerder in de werkgroep (voorlopig) buiten scope geplaatst, omdat het een andere generieke functie is dan een/het OTV, de primaire focus van de werkgroep.

Onderstaande functies zijn ook relevant maar kunnen voorlopig waarschijnlijk buiten de scope van de disussie gehouden worden:

5. **Informatievoorziening** aan betrokkenen en aan zorgaanbieders, bijv. over de reikwijdte van toestemmingen (mgl. betrokken uit een toestemmings-catalogus), maar ook informatie over de werking (doel en middelen) van de OTV: verantwoordelijke, klachtenprocedures, klantenloket etc.
6. **Spoed**: mogelijkheden voor het organiseren van toestemming en/of toegang tot gegevens in geval van spoed.

Uitleg bij de categorieën:

Hieronder korte toelichting op de vier hoofdcategorieën 1-4, gevolgd door een behandeling van categorie 5 m.b.t. informatievoorziening, en we sluiten af met een aantal opmerkingen over de requirements voor (toestemming bij) spoedsituaties in 6. Spoed.

1. **Registratie** van toestemmingen inclusief machtigen, incl. inzage in logging

De functie registratie van toestemming is in de gekozen categorisering ontkoppeld van de uitwisseling (gebruik / enforcement) van de toestemmingen. Registratie van toestemmingen is het essentiële doel van een OTV. Een (centraal) landelijk toestemmings-registratiesysteem is dus een minimaal noodzakelijke (landelijke) voorziening.

De auteur / registreerder van een toestemming kan patiënt zelf zijn, of een door de patiënt gemachtigde. Een gemachtigde kan een wettelijk vertegenwoordiger zijn (ouder/voogd) of een andere vertegenwoordiger (mantelzorger, familielid) of een zorgaanbieder. Als de machtiging verloopt via een wederzijds authenticatiemiddel (bv DigiD Machtigen) is er geen onduidelijkheid. Als de vertegenwoordiging of machtiging verloopt via een publiek register is er ook duidelijkheid. Een vraag is of en zo ja onder welke voorwaarden de patiënt ook een zorgverlener kan “machtigen” om een toestemming namens de patiënt te registreren, bijv. op het point of care. Als zo’n “machtiging” dan wel registratie van toestemming op het point of care mondeling verloopt omdat patiënt geen authenticatiemiddel kan/wil gebruiken, is het minimaal noodzakelijk om aanvullende eisen aan de auteur en het toestemmingsproces te stellen.

2. **Gebruik/effectuering** van toestemming **dmv een PDP** in uitwisseling, incl. inzage in logging.

De huidige wet- en regelgeving bepaalt, in aanvulling op andere randvoorwaarden, dat er toestemming moet worden vastgesteld voor het beschikbaar stellen van gegevens via een EUS (zie NEN7517 Toestemming). Door vast te stellen wat de toestemmingskeuze is van de patiënt, inclusief de reikwijdte van de toestemming, dwz. op welke bronhouders en welke ontvangers/opvragende partijen heeft de toestemming betrekking, eventueel gecombineerd met autorisatie informatie m.b.t. de uit te wisselen gegevensset, kan een besluit (decision) genomen worden of de uitwisseling van gegevens op grond van de in het PDP gecodeerde policies door kan gaan. Deze beslissing kan genomen worden in een zogeheten policy decision point (PDP).

Een PDP kan op meerdere plekken geïmplementeerd worden, en kan beslissingen nemen op basis van landelijke, regionale of lokale policies (met de term ‘regionaal’ bedoelen we meestal een samenwerkingsverband). Een PDP kan centraal of decentraal (lokaal, door de zorgaanbieder) geïmplementeerd worden, of beiden. Als het PDP niet centraal in het OTV Mitz geïmplementeerd wordt maar (ook of exclusief) in een lokale PDP instantie, zullen technische eisen gesteld moeten worden aan de interactie tussen het centrale OTV en de decentrale/lokale PDP instanties, bijvoorbeeld over of en wanneer en hoe toestemmingskeuzes via berichtenverkeer kunnen worden

uitgewisseld, en/of over de volgorde/prioriteit van de controle van toestemming bij verschillende PDPs waarin op meerdere niveaus toestemmingskeuzes kunnen worden vastgelegd en geëvalueerd.

3. **Lokalisatie** van dossierhouders, inclusief inzage in logging en autorisatie

Als een behandelaar niet weet bij wie gegevens over een patiënt aanwezig zijn, is een lokalisatiefunctie een middel om vast te stellen waar de gegevens zich bevinden. Bij push kunnen lokalisatiegegevens naar de ontvanger verstuurd worden, bij pull situaties zullen de lokalisatiegegevens bij een 'well-known' endpoint opgehaald moeten worden.

Mitz kan een well-known endpoint zijn in de eerste stap van een lokalisatieproces, die antwoord geeft op de vraag: "waar zijn (lokalisatie) gegevens van deze patient beschikbaar?"[2] Met het resultaat van de eerste stap kan een verdere lokalisatie plaatsvinden door de bronsystemen te bevragen, om uit te vinden welke dossiers precies beschikbaar zijn en hoe deze opgevraagd kunnen worden. Deze oplossing vereist dat Mitz een lokalisatieregister bevat. Een alternatief is om lokalisatie informatie mee te sturen met een elektronische verwijsbrief of een recept, om te vermijden dat eerst uitdrukkelijke toestemming gevraagd moet worden voor het delen van de lokalisatie informatie (zie NEN7519 Lokalisatie). In een pull situatie kan (de eerste stap van) lokalisatie niet overgeslagen worden, omdat een broadcast onder alle zorgaanbieders inclusief zorgaanbieders die de patiënt niet behandelen, onrechtmatig is.

Aangezien het uitwisselen (registreren) van lokalisatie-gegevens in een (landelijk) register een grondslag behoeft (bv toestemming), dient deze vastgesteld te worden voordat lokalisatie-gegevens in een register geplaatst en doorzoekbaar gemaakt worden. Daarnaast zal ook inzichtelijk moeten zijn hoe autorisaties ingeregeld worden m.b.t. lokalisatie-gegevens voor specifieke (soorten) zorgverleners/zorgaanbieders, en de hierop gebaseerde uitwisseling.

In beginsel is de lokalisatie functie buiten scope geplaatst voor de OTV requirements. Echter zodra lokalisatie in het OTV geïntegreerd wordt, zullen hiervoor requirements moeten worden opgesteld. Dit geldt overigens ook wanneer lokalisatie informatie die in een OTV geregistreerd wordt om een abonneerfunctie te implementeren.

4. **Inzage** door betrokkene en gemandateerde of zorgverlener - overkoepelende requirements

Zeggenschap en vertrouwen vergen transparantie. Dat betreft transparantie over de toestemming, de verwerking van die toestemming, de reikwijdte van de toestemming, en het effect van die toestemming op de uitwisseling van gegevens op basis van deze toestemming. Daarnaast is er (operationele) informatie over wie de toestemmingskeuze wanneer heeft ontvangen cq gebruikt.

Inzage / transparantie m.b.t. deze informatie kan voor elke functie (registratie, PDP, lokalisatie) apart georganiseerd worden. Veelal betreft het inzage een "doorkijkje naar" de logging informatie die beheerd wordt door de betreffende (sub)component. Eisen met betrekking tot overkoepelende aspecten, bijvoorbeeld het inzichtelijk zijn van loggegevens op 1 plek, al dan niet via een "doorkijk functie", kunnen onder deze categorie geplaatst worden.

Optionele categorieën:

5. **Informatievoorziening** naar de burger/betrokkene

[2] Het scheiden van 'eerste trap' en 'tweede trap' is niet noodzakelijk als gebruik gemaakt wordt van een index (of een push bericht) waarin de metadata voor elke bron direct wordt opgeslagen, zie NEN7519 Lokalisatie.

Naast een inzage/transparantiefunctie, is ook informatie nodig voor het kunnen geven van een valide toestemming, bijvoorbeeld over de reikwijdte van de toestemming (wie kunnen o.b.v. de toestemming bij welke gegevens?). Dit betreft veelal statische informatie die apart van andere functies kan worden aangeboden aan betrokkene (al dan niet geïntegreerd in een inzageportaal of PGO). Dit geldt meestal ook voor (tekstuele) informatie over de verantwoordelijke die doel en middelen van het OTV en van de voor de uitwisseling gebruikte infrastructuur bepaalt. De afspraken waaronder een toestemming geregistreerd of geraadpleegd moet worden en hoe die gebruikt moet worden in de uitwisseling (policies) zijn hier ook onderdeel van.

6. **Spoed** requirements

Omdat keuzes m.b.v. bovenstaande kunnen afwijken voor spoedsituaties, kan voor spoed een aparte set requirements gedefinieerd worden. Alternatief kunnen deze spoed-requirements bij alle drie de hoofdcategorieën (Registratie, PDP/effectuering, Lokalisatie) meegenomen worden. Echter, omdat de WOGS (en mogelijk de EHDS) alles wat met grondslagen voor spoedzorg te maken heeft verandert, en omdat hiervoor mogelijk specifieke (systeem)inrichtingen en/of voorzieningen moeten worden ingericht en omdat de eisen voor spoed sowieso sterk verschillen van 'reguliere' toestemmings- of uitwisselings-scenario's, lijkt het het beste om in een aparte set requirements voor spoed te voorzien.

Een uitspraak is belangrijk over wanneer we de requirements voor spoed kunnen gaan uitwerken: kan dit al voor de wijzigingen van de huidige wet- en regelgeving, of kunnen we dit pas serieus doen nadat duidelijk is hoe de WOGS eruit ziet en wat de implicaties van EHDS zijn? Is de NEN werkgroep Acute Zorg (met borging vanuit de Wegiz) een goede plek voor dit proces?

Het is overigens niet op voorhand duidelijk dat een OTV zoals Mitz in de inrichting van systemen voor spoed een rol zal spelen - immers, een opt-in (toestemming) onder de Wabvpz is iets heel anders dan een opt-out in de context van spoed, en het kan zelfs zijn dat voor *opt-outs* een heel ander (separaat) registratiesysteem moet worden ingericht.