Reactie op consultatie
"Online toestemmingsvoorziening: Mitz als bouwsteen"

Aan: Informatieberaad Zorg
Namens: Stichting Nuts

In het Nuts initiatief wordt door softwareleveranciers in de zorg preconcurrentieel samengewerkt aan open standaarden waarmee we de zorg vooruit helpen. Samen ontwikkelen we een robuust netwerk voor gegevensuitwisseling in de zorg, van ons allemaal en voor ons allemaal. Dat doen we aan de hand van het Nuts manifest, dat in acht punten beschrijft hoe wij met elkaar wensen samen te werken.

We zullen in deze reactie de voorgestelde toestemmingsvoorziening en de implementatie daarvan in de vorm van Mitz naast dit manifest leggen. Daarbij zullen we uiteenzetten wat voor problemen één systeem voor heel Nederland volgens ons met zich meebrengt, bespreken we de risico's van het ontwerp voor betrouwbaarheid, privacy en security en zullen we afsluiten met een schets van hoe wij zelf de toekomst van toestemmingsvoorzieningen voor ons zien.

Open voorzieningen voor de patiënt

Om te beginnen: het doet ons deugd te zien dat er op een aantal punten aansluiting is tussen de voorgestelde voorziening en het Nuts manifest. Zoals bijvoorbeeld punt twee uit het manifest:

> **2. Patiënt centraal**
> *Wij geloven dat de patiënt een **actieve plaats verdient**[1] in het netwerk, bijvoorbeeld via haar PGO (persoonlijke gezondheidsomgeving). De patiënt of een gemachtigde mantelzorger of bewindvoerder moet ervoor kunnen kiezen om mee te praten of **toestemmingen te beheren** en kunnen zien welke informatie er wordt uitgewisseld.*

De voorgestelde voorziening organiseert toestemmingen en bezwaren duidelijk rond de patiënt, en plaatst de patiënt daarbij in een actieve regierol.

> **5. Open standaarden**
> *Wij geloven dat toetreden tot dat netwerk frictieloos moet zijn. De gezamenlijke communicatiestructuur moet **open en gestandaardiseerd** zijn en er mogen geen (licentie)kosten verbonden zijn aan het gebruik. Er moet een Open Source referentie-implementatie beschikbaar zijn.*

Het document "Mitz als bouwsteen" maakt heel duidelijk dat de aansluiting op de toestemmingsvoorziening moet geschieden op basis van open standaarden. Vanzelfsprekend zijn we dit met elkaar eens. Wij willen echter nog een stap verder gaan, en op meer vlakken dan alleen de aansluiting gebruik maken van open standaarden. Daar komen we aan het einde van dit document op terug.

[1] De vetgedrukte nadruk in stukken uit het Nuts manifest en het ter consultatie liggende document zijn aangebracht voor de leesbaarheid van deze reactie, en geen onderdeel van die documenten.

Ook erkent het document duidelijk dat er verschillende uitwisselingssystemen en uitwisselingsmechanismen zijn in het land, en dat het daarom wenselijk is om een set aan gezamenlijke voorzieningen in het leven te roepen die voor meerdere uitwisselingen inzetbaar zijn (en zo herbruikbaarheid van investeringen garanderen). Zoals ook stichting Nuts en het samenwerkingsverband Centrale Voorzieningen (dat in 2019 is opgegaan in Nuts) betogen, hoort een gedeelde oplossing voor het organiseren van toestemmingen daar zeker bij. Het voorstel om dit apart te ontwerpen, los van een specifieke use-case of niche in de zorg, kan dus zeker op onze bijval rekenen.

Echter, wanneer we kijken naar de specifieke invulling die in dit voorstel wordt gegeven aan die toestemmingsvoorziening, en het technische ontwerp dat daarbij wordt gehanteerd, dan zien we op verschillende aspecten daarvan overwegende bezwaren die we hieronder toelichten en beargumenteren.

Vrije marktwerking en innovatie

Alleen wanneer een toestemmingsvoorziening zoals beschreven in het voorstel **volledige dekking** geeft kan de patiënt echt ontzorgd worden:

> ***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*

Echter, er zijn momenteel meerdere, verschillende “toestemmingsvoorzieningen”, en dat zal in de toekomst ook niet snel veranderen. Dat wordt erkend in het voorstel in §4.3.5:

> *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.*

Voor de patiënt zal dit voorstel tot een lappendeken van verschillende (deel)oplossingen leiden. En dan wordt er uitgegegaan van het scenario dat **alle** landelijk afgestemde uitwisselingen inderdaad via de voorgestelde toestemmingsvoorziening zullen lopen. Ook dat lijkt ons onwaarschijnlijk, gegeven hoe de sector zich de laatste jaren heeft bewogen. Het is daarmee de vraag of het beoogde voordeel voor de patiënt daadwerkelijk behaald wordt. Dit terwijl er richting de patiënt de indruk kan worden gewekt (bijvoorbeeld in marketinguitingen zoals de filmpjes met “Mitzie”) dat de invloed en het overzicht van de toestemmingen volledig dekkend is.

Omgekeerd zou het welslagen van de voorgestelde toestemmingsvoorziening (eventueel geholpen door de wetgever) leiden tot een monopoliepositie. Dan komen we in conflict met het vierde punt van het Nuts manifest:

4. Gedistribueerd netwerk
*Wij geloven in een gedistribueerd model van communicatie, vergelijkbaar met het Internet. Wij willen niet investeren in een netwerktechnologie met **één leverancier**, of één partij die direct of indirect alle gezondheidsdata van Nederland beheert. We willen een robuust netwerk van iedereen en voor iedereen, zonder **central point of failure** of **monopolist**.*

Niet alleen zou een toestemmingsvoorziening zoals hier wordt voorgesteld, indien succesvol, toegang tot alle gezondheidsdata van Nederland beheren en daarmee in onze definities indirect die data beheren. Het zou ook een product zijn dat in handen is van **één leverancier**, en daarmee zowel een *central point of failure* als ook een monopolie vormen. Het feit dat in het voorstel elke zorginstelling van Nederland een verwerkersovereenkomst met de leverancier zou moeten sluiten is daarvan eigenlijk al het bewijs.

Wat gebeurt er als de voorziening om wat voor reden dan ook niet bereikbaar is? Kunnen er dan in heel Nederland geen gegevensuitwisselingen meer plaatsvinden? Wat als de responstijden van de voorziening onacceptabel zijn? Wat gebeurt er als de uitbater van zo'n voorziening beslissingen neemt waar de belangenorganisaties, zorginstellingen of ICT leveranciers zich niet in kunnen vinden? Wat als de voorgestelde toestemmingsvoorziening op enig moment niet meer door-innoveert en stil komt te staan? Of als deze wordt overgekocht door een buitenlandse investeerder?

Als we omwille van het gemak van de patiënt accepteren dat één partij op dit vlak een monopolie krijgt, dan kan er door alle andere stakeholders niet meer met de voeten gestemd worden door naar een andere leverancier te gaan. Er is immers maar één database. We belanden dan in een ***vendor lock-in*** waar we heel erg moeilijk weer uit geraken. En zoals we in het laatste hoofdstuk zullen beschrijven: we kunnen de patiënt datzelfde gemak bezorgen zonder een monopoliepositie te introduceren.

Herbruikbaarheid en onweerlegbaarheid

Dit brengt ons op een volgend punt van zorg. Er wordt in het voorstel gesproken over het migreren van toestemmingen van bestaande systemen naar deze toestemmingsvoorziening, maar er wordt niet gesproken over de mogelijkheid om toestemmingen te migreren **naar een alternatief** of te kunnen **hergebruiken** voor andere systemen.

Er wordt, met andere woorden, vanuit gegaan dat de voorgestelde voorziening "leidend" wordt, en dat alle uitwisselingssystemen van Nederland gaan luisteren naar dit systeem. Elke zorginstelling en elke zorgverlener moet er dus op kunnen vertrouwen dat wat dit systeem zegt over het mogen doorbreken van het beroepsgeheim geheel juist, tijdig en volledig is. Maar dat staat of valt met:

a) Het vertrouwen in de toestemmingsvoorziening zelf, en haar ontwikkelaar en beheerder;
b) Het vertrouwen in de waarachtigheid van gemigreerde toestemmingen, en de partijen waar die toestemmingen vandaan komen (zorginstellingen en diens ICT leveranciers);
c) Het vertrouwen in de authenticatiemiddelen die gebruikt worden om toestemmingen te registreren.

Een relevant punt uit het Nuts manifest is het volgende:

8. Cryptografische basis
*Wij geloven dat de technologie en de tijd rijp zijn voor een systeem gebaseerd op **cryptografische principes**. We willen garanties kunnen geven over identiteiten en **toegang tot data** die verder gaan dan "het is zo geconfigureerd". Wij geloven dat we alleen met zo'n oplossing het **vertrouwen** van de hele markt—en uiteindelijk van de burger—kunnen winnen.*

Op het eerste gezicht is dat in het voorstel goed afgedicht: er wordt beschreven dat de authenticiteit van de toestemming te controleren is aan de hand van drie tokens:

> *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').*

Echter, als we deze passage kritischer lezen, en in de omringende context plaatsen, dan zien we dat deze tokens toch niet de cryptografische waarborgen bieden die we zoeken. Het mandaattoken en het inschrijftoken zijn ondertekend met een UZI pas, zodat een gebruiker van een ICT systeem namens de houder van die UZI pas toestemmingen kan beheren voor zijn of haar patiënten. Het transactietoken is voor de beveiliging van het koppelvlak van Mitz ("heb ik wel de partij voor me die ik denk?"). Geen van die tokens **ondertekent** dus daadwerkelijk de **afgegeven toestemming** met een authenticatiemiddel. Of anders gezegd: het zijn alle drie tokens om de **toestemmingsvoorziening** vertrouwen te geven in de afgifte van de toestemming, niet de **dossierhouder**.

En hier komen we terug op de herbruikbaarheid van de toestemmingen. Om de dossierhouders in staat te stellen om de onweerlegbaarheid van toestemmingen onafhankelijk te kunnen valideren moeten deze **toestemmingen zelf cryptografisch worden ondertekend** met een sterk authenticatiemiddel. Daarmee kunnen de stappen *a* en *b* uit de bovenstaande opsomming over worden geslagen en wordt er alleen vertrouwen gelegd in de gebruikte authenticatiemiddelen. Dit hebben we ook beschreven in de toelichting bij punt acht van ons manifest:

> *Identiteit is iets dat je persoonlijk inbrengt, een unieke sleutel op basis waarvan je te herkennen bent, **toestemmingen kunt ondertekenen**, en jouw eigen gegevens kunt ontsleutelen. Dankzij die unieke sleutel kunnen we **onomstotelijk aantonen door wie toestemmingen zijn afgegeven** en wie het verzoek doet om data op te halen uit een ander systeem.*
>
> *Om die unieke sleutel een hogere betrouwbaarheid te geven lijkt het ons fantastisch als die terug te herleiden is tot een identiteit die is afgegeven door een instantie die erover gaat, zoals bijvoorbeeld een gemeente of het BIG register.*
>
> *Alleen op die manier kunnen we af van het probleem dat softwareleveranciers en zorginstellingen elkaar (terecht) niet vertrouwen in het beheren van identiteiten en **rechten**. Daarom zijn we alleen op zoek naar gedistribueerde technologie die dit mogelijk maakt.*

Deze beschreven oplossing is overigens in principe haalbaar met gebruikmaking van de UZI pas. Alleen vereist dit een set nadere afspraken die we niet teruglezen in het voorstel. Met DigiD is dit momenteel niet mogelijk, wat ook nog een uitdaging presenteert voor het cryptografisch ondertekenen van toestemmingen die door de patiënt zelf worden beheerd.

Toestemmingen die cryptografisch zijn ondertekend en herleidbaar zijn naar een sterk authenticatiemiddel kunnen eenvoudig worden geëxporteerd van en naar elke toestemmingsvoorziening, en ook parallel gebruikt worden door verschillende naast elkaar bestaande toestemmingsvoorzieningen. De toestemmingsvoorziening zelf is dan immers niet meer “leidend”, maar de **ondertekening door de patiënt of zorgverlener**. Dit mechanisme geeft dus veel meer mogelijkheden om de in het vorige hoofdstuk geschetste monopoliepositie te voorkomen, en tegelijkertijd de zorg meer vertrouwen te geven in de rechtmatigheid van de toestemmingen, dan het voorstel dat ter consultatie ligt.

Privacy en security

Een groot deel van onze bezwaren hebben betrekking op privacy en security. Dit zijn twee speerpunten uit het Nuts manifest, die we als volgt hebben beschreven:

> **6. Privacy by design**
> *Wij geloven dat privacy by design in dit netwerk van het grootste belang is. Daarom willen we een systeem waarin je **bewust** informatie met elkaar deelt. We vinden het belangrijk dat een mens de keuze maakt om informatie te **delen**, bijvoorbeeld door een **toestemming vast te leggen** of een verzoek om informatie te accepteren.*
>
> **7. Security by design**
> *Wij geloven dat elk systeem dat wil kunnen schalen er al in de ontwerpfase vanuit moet gaan dat er partijen in het netwerk kunnen deelnemen die **niet te vertrouwen** zijn, en dat ook kwaadwillenden steeds slimmer worden. We willen te allen tijde voorkomen dat onze infrastructuur een onbevoegde in staat stelt om medische informatie over mensen te bekijken, te veranderen of te verwijderen.*

Ten eerste maken we ons zorgen om het risico dat de voorgestelde toestemmingsvoorziening een *privacy en security hotspot* kan worden.

In de toestemmingsvoorziening worden relaties opgeslagen tussen natuurlijke personen en (groepen van) zorgaanbieders. Daarnaast worden, ten behoeve van de inzage voor de patiënt, relaties vastgelegd tussen zorgaanbieders die communiceren over een persoon. Dit blijkt onder andere uit §4.1.1:

> *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. [...] 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.*

Uit al die relaties kunnen ziektebeelden worden afgeleid. En deze relaties zijn uniek te herleiden tot een persoon. Er worden dus effectief **bijzondere persoonsgegevens** van (potentieel) alle Nederlanders in de voorgestelde voorziening opgeslagen. Dit maakt de voorziening een *privacy hotspot*.

Daarnaast wordt de voorgestelde toestemmingsvoorziening ontworpen als een centraal *"policy decision point"*, zoals beschreven in het document in §6.1.5. Dit centraal ontworpen systeem zal bepalen welke gegevens gedeeld mogen worden en introduceert daarmee een centraal punt waar hackers zich op kunnen richten. Een *security hotspot*.

Er zijn twee manieren om hiernaar te kijken. Enerzijds levert een centraal punt de mogelijkheid om heel veel tijd, geld en energie te steken in het verdedigen van dat punt. Anderzijds kun je de impact van een aanval reduceren door de informatie verspreid over verschillende systemen te laten staan. Het wordt daarmee minder aantrekkelijk om één van de systemen aan te vallen. Daarnaast is een groot deel van de *hacks* niet het gevolg van een beveiligingslek maar van het handelen van mensen. Te denken valt aan *phishing attacks* of aan medewerkers van ICT leveranciers die om wat voor reden dan ook kwade intenties hebben. Hoe meer invloed één mens kan hebben, hoe schadelijker een aanval kan zijn. Risico wordt vaak gedefinieerd als *kans maal impact*. Door de impact van een hack te verkleinen wordt het risico van het gehele systeem kleiner.

Ten tweede worden er in het voorstel veel beweringen gedaan over de beveiliging van Mitz. Wij willen verzoeken om alle gepresenteerde onderdelen van Mitz, evenals de gebruikte configuraties en de actuele inhoud van de toestemmingscatalogus, **publiek te maken**. Bijvoorbeeld in de vorm van Open Source software. Alleen dan kan door beveiligingsexperts uit het hele land worden vastgesteld of die beweringen ook daadwerkelijk correct zijn geïmplementeerd. Daarnaast zou een onafhankelijke security audit met enige regelmaat moeten uitwijzen of die gepubliceerde code en configuraties ook daadwerkelijk overeenkomen met de versies die in praktijk gebruikt worden.

Ten derde verbazen wij ons over de keuze voor het geven van toestemming aan **categorieën van zorgaanbieders** voor het ophalen van gegevens door **categorieën van zorgaanbieders**, zoals te lezen valt in §4.1.6 en §5.3. Onderstaande figuur uit §5.3 maakt dit het meest expliciet:

Het is dus in het voorstel niet mogelijk om expliciet toestemming te geven voor het delen van medische gegevens met een **specifieke zorginstelling**. Bij elke uitwisseling waar deze toestemmingsvoorziening voor wordt ingezet geldt dat gegevens door **alle instellingen** in die categorie kunnen worden ingezien. Daar is immers expliciet toestemming voor gegeven. Er is niet voorzien in de mogelijkheid om specifieker toestemming te geven.

Uit de toelichting bij punt zes (*Privacy by design*) uit ons manifest:

> *Een andere vraag die we ons moeten stellen is hoe we de hoeveelheid uitgewisselde informatie zoveel mogelijk kunnen beperken. Geef je toestemming om je hele dossier te delen, of alleen wat er relevant is voor je gebroken been?*
>
> *Bij elke stap die we zetten moeten we onszelf de vraag blijven stellen: welke impact heeft deze keuze op de privacy van miljoenen mensen?*

Deze manier van denken is in lijn met de beginselen van dataminimalisatie en proportionaliteit uit de Algemene Verordening Gegevensbescherming (AVG). En naar onze mening staat dit haaks op het werken met categorieën van zorgaanbieders.

Ten vierde maken we ons grote zorgen over de functie “zorgverlener namens patiënt” en de manier waarop dit wordt vormgegeven in het voorstel. We lezen onder andere in §2.2, 5a:

> *Mitz is zo ingericht dat een **raadplegende zorgaanbieder** namens de patiënt een dergelijke toestemming onweerlegbaar kan organiseren, zodanig dat die bij de juiste bron terechtkomt, vertrouwd wordt, en gegevens door die bron beschikbaar gesteld kunnen worden.*

Middels deze functie kunnen toestemmingen worden toegevoegd en gemuteerd uit naam van een patiënt. Daarbij kan ook, terecht of onterecht, toestemming worden verleend aan **andere zorginstellingen** om het beroepsgeheim te doorbreken, en zo informatie te verschaffen aan de vastlegger. Door de constructie waarbij iemand daartoe (eenmalig) **gemandateerd** kan worden door een andere persoon met een UZI pas (zie §5.2.1) krijgen de volgende groepen personen de mogelijkheid om toestemmingen te registreren, en daarmee potentieel **zichzelf toegang te verschaffen** tot patiëntendossiers van andere zorginstellingen:

- Voor een willekeurige patiënt:
    - Zorgverleners met een UZI pas
- Voor patiënten in zorg bij de instelling (waarvoor een inschrijftoken is getekend):
    - Collega-zorgverleners zonder UZI pas
    - Andere medewerkers zonder UZI pas
    - Personen die werken voor het applicatiebeheer van de zorginstelling of bij de betrokken ICT leveranciers en ofwel toegang hebben tot productieservers, ofwel de mogelijkheid hebben om gebruikers in het systeem te *impersoneren*
    - Hackers en andere ongewenste personen die zichzelf toegang verschaffen tot één van de duizenden ICT systemen in Nederland

Deze lijst is waarschijnlijk niet volledig, maar we kunnen zien dat het aantal personen in Nederland dat op termijn deze mogelijkheid krijgt richting de honderdduizenden mensen loopt. En natuurlijk mag er formeel alleen een toestemming worden verleend binnen een smal en duidelijk juridisch kader. Maar het zogenaamde *attack surface*, als we het bijvoorbeeld hebben over *phishing*, wordt enorm. Hoe meer potentiële slachtoffers, hoe groter de **kans op een aanval**. En wederom: het risico is *kans maal impact*.

Ook is het voorstel dat de vastgelegde toestemmingen **onmiddellijk van kracht** zijn. Er is in het voorstel voor zover wij kunnen beoordelen geen sprake van een onafhankelijke bekrachtiging van de wijziging door de dossierhouder of de patiënt zelf, noch van een *cool down period* waarin grootschalige geautomatiseerde aanvallen kunnen worden gedetecteerd en geblokkeerd. Er is geen gelegenheid ingebouwd voor de dossierhouder om het medisch beroepsgeheim naar eigen inzicht in te vullen en er vindt aan de kant van de dossierhouder geen controle plaats op wilsonbekwaamheid, onder curatele stelling of andere overwegingen die mogelijk niet bekend zijn bij de opvrager.

De voorgestelde toestemmingsvoorziening legt dus heel veel macht in een centraal systeem en geeft vervolgens heel veel mensen schrijfrechten die onmiddellijk toegang moeten verschaffen tot medische data. We begrijpen de wens om bij een consult gegevens van een andere instelling in te kunnen zien. We begrijpen ook dat het wenselijk is om dan namens de patiënt een toestemming vast te kunnen leggen, zodat deze ontzorgd wordt. Maar naar onze inschatting brengt het voorstel dat hier ter consultatie ligt een onacceptabel risico met zich mee op de vlakken van privacy en security.

Inclusiviteit

Tenslotte delen wij nog een aantal punten van zorg die betrekking hebben op de inclusiviteit van patiënten en zorgverleners.

Op basis van welke juridische grondslag wordt het BSN van patiënten verwerkt indien er (nog) geen zorginstelling op Mitz is aangesloten waarmee die patiënt een behandelovereenkomst heeft? Hoe kan er een algemene DigiD login worden aangeboden aan alle Nederlanders, als het BSN dat daaruit voortvloeit misschien wel en misschien niet in de context van een aangesloten zorginstelling verwerkt mag worden? Of krijgen sommige gebruikers een scherm gepresenteerd dat ze geen gebruik kunnen maken van Mitz? Hoe rijmt dit met de moeite die in het kader van MedMij wordt gedaan om de authenticatie van patiënten via de zorgverlener te laten lopen?

Ook vragen wij ons af hoe zorgverleners die momenteel geen aanspraak kunnen maken op een UZI pas, zoals nagenoeg alle zorgverleners in de langdurige zorg, toch toegang kunnen krijgen tot de voorgestelde toestemmingsvoorziening. Daar lijkt in het voorstel maar één alternatief voor te worden geboden, en dat is de mandatering van andere gebruikers met een UZI pas. Welke oplossing wordt er geboden voor zorginstellingen waarbij geen van de medewerkers aanspraak kan of wil maken op een UZI pas?

Er zijn ook veel processen in de zorg waarvoor een impliciete of veronderstelde toestemming van toepassing is. Te denken valt aan de registratie van een doorverwijzing of een overdracht, op basis waarvan het beroepsgeheim ook doorbroken mag worden. Ook deze veronderstelde toestemmingen moeten worden vastgelegd en uitgewisseld tussen ICT systemen. In de voorgestelde toestemmingsvoorziening kan alleen een bezwaar tegen uitwisseling worden vastgelegd. Daarmee worden impliciete toestemmingen vanuit het perspectief van de patiënt ondersteund, maar niet vanuit het perspectief van de uitwisselingssystemen en softwareleveranciers. Die hebben dan nog steeds een eigen boekhouding. Het lijkt ons kostbaar en weinig zinnig om voor de registratie van die veronderstelde toestemmingen in alle systemen een apart mechanisme te moeten implementeren. Wat ons betreft moet een voorstel voor toestemmingen daarom ook op dit vlak inclusief zijn.

Tegenvoorstel

In het Nuts initiatief wordt door softwareleveranciers in de zorg preconcurrentieel samengewerkt aan open standaarden waarmee we de zorg vooruit helpen. In dat verband denken wij ook constant na over impliciete en expliciete toestemmingen. Wij willen daarom graag kort vertellen hoe wij naar deze problematiek kijken, in de vorm van een soort “tegenvoorstel”.

We stellen voor dat er niet gedacht wordt vanuit een specifiek product van een specifieke aanbieder, maar vanuit een **set aan gestandaardiseerde protocollen**. Door te werken met protocollen in plaats van een product kunnen we een *vendor lock-in* voorkomen en blijven innoveren. Onderdeel van dit protocol zou moeten zijn dat toestemmingen om het beroepsgeheim te doorbreken worden opgeslagen in het systeem van de zorginstelling die dat beroepsgeheim mag doorbreken. Daar staat immers ook het dossier opgeslagen waarop die toestemming betrekking heeft, en daarmee houden we **data bij de bron**.

Dit heeft een aantal hele concrete voordelen. Eén voordeel is dat toestemmingen altijd beschikbaar zijn wanneer de data ook beschikbaar is (nul extra *downtime*) en dat het ook nagenoeg geen extra tijd kost om die toestemming te raadplegen (nul extra *latency*). Door de toestemmingen, en daarmee de relaties tussen zorgaanbieders en patiënten, bij de relevante dossierhouder op te slaan kan er ook geen nieuwe informatie worden afgeleid door derde partijen. Daarmee lossen we in één klap de meeste van onze eerder genoemde bezwaren op.

Een deel van deze protocollen zou opgenomen kunnen worden in het MedMij stelsel. De patiënt kan dan **vanuit het eigen PGO** bij zorginstellingen opvragen welke toestemmingen daar geregistreerd staan, en die toestemmingen eventueel muteren indien de zorgverlener dit toestaat. Daarmee geven we de patiënt vanuit diens perspectief **één volledig overzicht** van afgegeven en veronderstelde toestemmingen bij verschillende zorginstellingen, maar behouden we marktwerking. De zorgverlener heeft in dit voorstel het laatste woord, en kan er ook voor kiezen om (bepaalde) patiënten géén schrijfrecht te geven. Hiermee lossen we meteen alle vraagstukken rondom wilsonbekwaamheid, onder curatele gestelde patiënten en minderjarige patiënten op.

Het enige dat een gestandaardiseerd protocol dan nog moet oplossen is het notificeren van andere zorginstellingen over het feit dat zij toestemming hebben om gegevens op te vragen. Dit zou bijvoorbeeld kunnen geschieden op de manier zoals wij die nu in Nuts-verband voor de eOverdracht aan het specificeren zijn. Wij zijn hierover als leveranciers in gesprek met elkaar en met Nictiz, en er ligt al een **concreet voorstel**. Ons inziens zou zo’n protocol een hele waardevolle investering zijn omdat hetzelfde mechanisme gebruikt kan worden voor zowel expliciete toestemming van de patiënt, als ook veronderstelde toestemming waarbij data het zorgproces mag volgen.

Het vastleggen van toestemmingen door zorgverleners die niet ook de dossierhouder zijn (“zorgverlener namens patiënt”) is wat ons betreft een verkeerde ontwerpkeuze. Dit proces zou moeten worden vervangen door een gestandaardiseerd protocol om als zorgverlener een **“verzoek tot inzage”** te doen bij een dossierhouder. Dat verzoek moet kunnen leiden tot een expliciete of impliciete toestemming, of een afwijzing van het verzoek. Daarmee houdt de dossierhouder het **laatste woord**, en doen we recht aan diens zeggenschap over zijn eigen medische beroepsgeheim. Ook hier geldt dat we op deze manier recht kunnen doen aan zaken als wilsonbekwaamheid, onder curatele stelling en andere overwegingen die mogelijk niet bekend zijn bij de raadplegende zorgverlener.

Dit alles is geheel in lijn met ons manifest. Uit de toelichting bij punt zes (*Privacy by design*):

> *Wij zijn van mening dat we de privacy van patiënten alleen kunnen waarborgen door een systeem te bouwen waar toestemmingen al in het ontwerp zitten ingebakken. Het zou nooit mogelijk moeten zijn om informatie op te halen waar je niet **expliciet** toestemming voor hebt gekregen door een mens.*
>
> *Om dat mogelijk en gebruiksvriendelijk te maken willen we actief informatie delen met een andere persoon in het netwerk. Dit betekent in de praktijk dat je een toestemming klaarzet dat die andere persoon gemachtigd is om de betreffende informatie te bekijken, waarvan de ander ook wordt genotificeerd. Ook willen we gebruikers in staat stellen om aan anderen in hun netwerk het **verzoek** te sturen om zo'n toestemming af te geven.*

Het is dan nog steeds waardevol om toestemmingen cryptografisch te ondertekenen, maar het is niet meer noodzakelijk voor het valideren van de geldigheid van de toestemming **aan de kant van de dossierhouder**. Die geldigheid heeft de dossierhouder immers zelf kunnen vaststellen bij vastlegging. Het cryptografisch ondertekenen van toestemmingen is dan vooral nog nuttig om achteraf onweerlegbaar vast te kunnen stellen door **wie** toestemmingen zijn vastgelegd, of eventueel in de toekomst te **migreren** naar een andere toestemmingsvoorziening. Een goed ontwerp houdt immers altijd rekening met in de toekomst veranderende inzichten.

We zouden de ontwerpers van Mitz graag langs deze weg willen **oproepen** om hier nader met ons over na te denken, en om de reeds opgedane inzichten op het vlak van *user experience design*, de formulering van toestemmingsvragen en de mappings van toestemmingsvragen op zorginformatiebouwstenen open (*public domain*) beschikbaar te stellen. Dit zijn waardevolle inzichten die hergebruikt kunnen worden in andere vergelijkbare toestemmingsprojecten in de zorg.

Ook op dat vlak zou wat ons betreft moeten gelden: redeneer niet vanuit een specifiek product van een specifieke leverancier maar vanuit **samenwerking in de gehele markt** en het maken van open afspraken waar iedereen vrijelijk bij kan aansluiten.