# Rapportage Push Autorisatie

## Managementsamenvatting

Autorisatie bepaalt of een zorgmedewerker informatie mag raadplegen op basis van zijn rol in het zorgproces. Hierbij moet de te raadplegen informatie proportioneel zijn. Dat betekent dat de inhoud en omvang van de informatie moet passen bij het doel waarvoor en de context waarin hij de informatie wil gebruiken. Het betreft hier de autorisatie voor het raadplegen van informatie van buiten de eigen instelling.
Push autorisatie gaat uit van autorisatie door de bronhouder van de data. Deze bronhouder geeft autorisaties - gecombineerd met lokalisatie - uit door middel van een URL bij het beschikbaar maken van informatie. Push autorisatie biedt voldoende ruimte om zo in te richten dat uitdrukkelijke toestemming niet verplicht is. Push autorisatie is specifiek ontworpen om gegevens gericht beschikbaar te stellen.
De URL kan via een gemeenschappelijke voorziening worden omgezet in een code, wat flexibiliteit in het proces brengt. De patiënt kan m.b.v. de code bijvoorbeeld zelf bepalen met wie gegevens worden gedeeld. Doormiddel van doorautoriseren is het gebruik van push autorisatie in ketens en netwerken in theorie mogelijk.
Bij push autorisatie bepaalt de bron (de grens van) welke gegevens beschikbaar gemaakt (kunnen) worden.
Push autorisatie ligt dicht bij het Twiin uitwisselconcept notified pull maar er zijn ook verschillen. Zo kan de patiënt kan d.m.v. delen van de autorisatie(code) zelf bepalen met wie gegevens worden gedeeld en is doorautoriseren een onderdeel van push autorisatie.
Push autorisatie is niet geschikt voor beeldbeschikbaarheid – bij de huidige implementaties - aangezien deze zijn gebaseerd op het IHE XDS/XCA-i profiel en push autorisatie internationaal onbekend is.
Het toepassen van push autorisatie voor het versturen van beelden als in het Twiin portaal is wel kansrijk.

Push autorisatie is technisch te combineren met andere autorisatie methoden en hiermee kan recht worden gedaan aan burgers die principiële bezwaren hebben tegen het geven van toestemming in een gemeenschappelijke voorziening. Immers push autorisatie kan zo ingericht worden dat uitdrukkelijke toestemming niet verplicht/ nodig is. Aandachtspunt bij het combineren van push autorisatie met andere autorisatie mechanismen is gebruikersgemak en toenemende kosten voor implementatie van meerdere mechanismes. Deze aspecten zijn in dit onderzoek niet geanalyseerd/meegenomen, de impact zal in (de voorbereiding op) praktijktoetsen moeten worden onderzocht.

# 1. Onderzoeksvragen

De onderzoeksvragen die in de opdracht zijn meegegeven:

- Toepasbaarheid van push autorisatie naast andere autorisatie mechanismes, zoals:
  - Twiin, Nuts en AORTA
  - Decentrale en centrale oplossingen

  Compatibiliteit met andere manieren van autoriseren, en combineren van de verschillende manieren van autoriseren (in de keten)
- Mogelijkheden voor andere startpunten dan de huisarts bij gebruik van push autorisatie in de keten
- Impact van push autorisatie op het zorgveld (zorgaanbieders en leveranciers) op alle lagen van interoperabiliteit

Deze vragen dienen te worden beantwoord op basis van een drietal use cases, waarbij gedacht wordt aan de use cases medicatie overdracht, beeldbeschikbaarheid en geboortezorg.
Het onderzoek betreft nadrukkelijk niet het beproeven van de methode van push autorisatie. De resultaten van dit onderzoek kunnen de basis zijn voor een vervolg in de vorm van een beproeving.

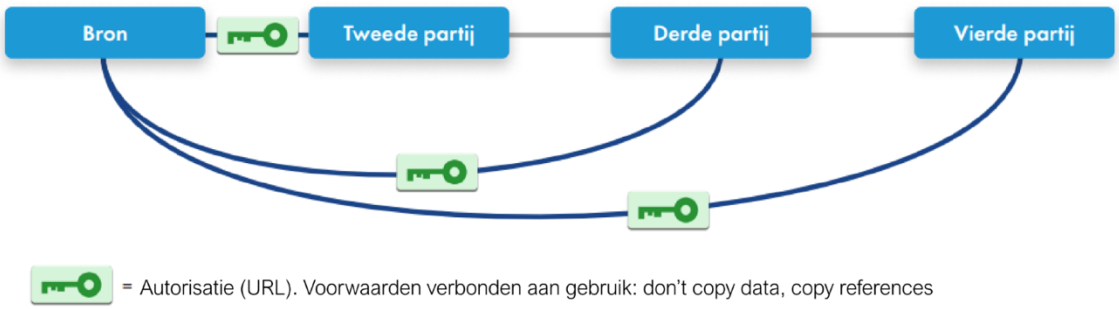
# 2. Push Autorisatie

## 2.1 Concept van Push Autorisatie

Push Autorisatie gaat uit van autorisatie door bronhouder van de data. Deze bronhouder geeft autorisaties uit bij een verwijssituatie en/of bij het delen (vrijgeven) van historische informatie. De bronhouder van data kan de huisarts zijn maar ook andere bronhouders zijn mogelijk (bijv. een ziekenhuis).
Het concept push autorisatie bestaat uit twee stappen:

- Stap 1 : Bronhouder pusht autorisatie voor bepaalde data
- Stap 2 : Degene die de autorisatie ontvangt (raadpleger) haalt de data op

De push van de autorisatie gaat door middel van een URL waarmee de raadpleger de gegevens (geïdentificeerd en geauthentiseerd door middel van een UZI pas) kan ophalen bij de bron. Bij de bron is er autorisatie ingericht wie de gegevens mag bekijken.
In plaats van een URL kan ook een autorisatiecode gebruikt worden om toegang te geven; deze kan als onderdeel van stap 2 worden "ingewisseld" voor een URL die door de bron geregistreerd was in verwijscode.nl. Een autorisatiecode kan fysiek en drager onafhankelijk worden meegegeven aan de patiënt, of door de zorgverlener op de verwijsbrief en bijvoorbeeld worden doorgebeld. Een eenmaal ontvangen en gebruikte autorisatie(code) kan niet door een ander dan deze ontvanger gebruikt worden.
Push autorisatie kan de zorg-workflow van ketens ondersteunen doordat het voorziet in een mechanisme om door te autoriseren. De opvrager doet dan een verzoek bij de bron voor het opleveren van een doorautorisatie-URL of -code. De opvrager kan deze vervolgens doorsturen naar een derde partij. Zie onderstaande weergave.




## 2.2 Juridische implicaties

Gegevensuitwisseling gebaseerd op push autorisatie kan - afhankelijk van de inrichting horende bij een use-case - wel of niet kwalificeren als een elektronisch uitwisselingssysteem. Afhankelijk van de inrichting kan bij push autorisatie voorafgaande uitdrukkelijke toestemming verplicht zijn op basis van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg ("Wabvpz").

Een elektronisch uitwisselingssysteem is gedefinieerd in de Wabvpz als een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken. Uit de Wabvpz volgt dat de zorgaanbieder gegevens slechts beschikbaar stelt via een elektronisch uitwisselingssysteem voor zover de patiënt daartoe uitdrukkelijke toestemming heeft gegeven.
Bij push-verkeer ligt het initiatief van het versturen bij de verzender. Bij pull-verkeer ligt het initiatief van ophalen bij de raadpleger. Bij push autorisatie heeft de verzender het initiatief bij het bepalen van de autorisatie. Het initiatief voor het ophalen van de gegevens ligt bij push autorisatie juist bij de raadpleger. Dat maakt dat push autorisatie niet duidelijk te kwalificeren is.
Push autorisatie biedt voldoende ruimte om zo in te richten dat uitdrukkelijke toestemming niet verplicht is. Push autorisatie is ook specifiek ontworpen om gegevens enkel gericht beschikbaar te stellen. Toch zijn verschillende keuzes mogelijk voor de inrichting waarbij push autorisatie ook gebruikt zou kunnen worden voor ongericht beschikbaar stellen. Het gaat om de volgende drie inrichtingskeuzes:

- Push autorisatie ziet in beginsel om gerichte één op één autorisatie. Maar de autorisatie kan worden doorgezet aan andere zorgaanbieders. Verschillende keuzes zijn mogelijk in de inrichting van de mogelijkheid om te kunnen door-autoriseren. Hoe ruimer die mogelijkheid, hoe meer kans dat de door-autorisatie zich niet beperkt tot zorgverleners betrokken bij dezelfde behandelrelatie.
- Er zijn keuzes mogelijk in het aantal zorgmedewerkers dat toegang kan krijgen. De autorisatie kan beperkt zijn tot specifieke behandelaars of (via een tussenstap) worden opengesteld voor alle medewerkers van een organisatie. Het autoriseren van een afdeling (bijv. bij verwijzing) is ook een optie. Verder zijn er nog keuzes mogelijk in de duur van de geldigheid van de autorisatie.
- Hoe langer de duur, hoe meer kans er is dat de geautoriseerde zorgverleners gegevens kunnen ophalen voor een andere behandelrelatie dan waar de autorisatie oorspronkelijk voor was bedoeld.

Ook als geen uitdrukkelijke toestemming vereist is op basis van de Wabvpz, kan toestemming nodig zijn op basis van de WGBO. De WGBO vereist dat gegevens uit het dossier enkel aan een ander mogen worden verstrekt met toestemming van de patiënt, behalve als het gaat om medebehandelaars of vervangers. Alleen in een aantal situaties zoals bij een verwijzing is veronderstelde toestemming afdoende. In andere gevallen is expliciete toestemming nodig. Het gaat hierbij niet om uitdrukkelijke toestemming om gegevens raadpleegbaar te maken, maar om expliciete toestemming die gericht is op een specifieke uitwisseling van gegevens.
Push autorisatie is ontworpen vanuit privacy-by-design. Push autorisatie biedt ruimte om de regie over de autorisatie te beleggen bij de dossierhouder. Dit in contrast met een elektronisch uitwisselingssysteem op basis van XDS/XCA waarbij de raadplegende zorgaanbieder de inrichting van de autorisatie bepaalt om te raadplegen. Ook is de inrichting van de autorisatie bij push autorisatie meer in lijn met privacy-by-design dan de inrichting van het LSP. Bij het LSP is de autorisatie om te raadplegen gebaseerd op een algemeen geldend medisch autorisatieprotocol. Hierbij is geen ruimte voor maatwerk ten aanzien van de specifieke uitwisseling. De push autorisatie biedt ruimte aan de patiënt om zelf regie te nemen aan wie de autorisatie wordt verstrekt (bijvoorbeeld via het kunnen afgeven van een autorisatiecode/verwijscode aan een specifieke zorgverlener).

## 2.3 Eigenschappen Push Autorisatie

In onderstaande tabel een samenvattend overzicht van de belangrijkste eigenschappen van push autorisatie op de lagen van interoperabiliteit.

| Organisatielaag |
| --- |
| • Push Autorisatie gaat uit van autorisatie door de bronhouder van data als uitgever van autorisaties bij verwijssituatie en/of om het delen (vrijgeven) van historische informatie.<br>• De rol van de huisarts in het proces **wordt gezien als** belangrijk **en** als de enige partij in de zorg die een min of meer compleet historisch overzicht kan hebben van de patiënt - en daarmee in staat is om (decentraal) historische informatie te delen binnen het zorgproces [eventueel gepresenteerd in de vorm van een tijdlijn]. Dit is een belangrijk organisatorisch |

uitgangspunt bij de huidige implementaties van push autorisatie van Whitebox maar dat hoeft niet per definitie zo te zijn.

- Push autorisatie kan de zorg-workflow (d.m.**v.** doorautoriseren) volgen

Doorautoriseren: een autorisatie kan een recht omvatten om **een** nieuwe autorisatie of een autorisatiecode op te vragen bij de bron, die naar een volgende partij in de keten kan worden doorgezet.

- Afhankelijk van de use-case is veronderstelde of uitdrukkelijke toestemming nodig voor het doorzetten van autorisatie naar een volgende partij in de keten. (Bijvoorbeeld: medicatie kan waarschijnlijk mee binnen de "veronderstelde toestemming" bij verwijzing naar een ander ziekenhuis, andere historische informatie niet zomaar.)

Proceslaag

- Er zijn 2 stappen:
  - Stap 1: push van autorisatie (v**ergelijkbaar met de 'notify' in notified pul**l) kan als URL of autorisatiecode ondergebracht worden in/ als onderdeel van verschillende 'dragers', zoals een verwijsbrief of recept.
  - Stap 2: inzien of ophalen van bepaalde data. De policy instelling aan de data **bepaalt w**at de raadpleger mag zien afhankelijk van zijn UZI rolcode[i] in combinatie met eventueel vooraf ingestelde parameters die bepalen welke gegevens precies opvraagbaar zijn voor de (beoogd) ontvanger.

- Autorisatiecodes kunnen uitgegeven worden door de dossier- /bronhouder en door de patiënt of diens verzorger. Hierdoor wordt regie gevoerd door te bepalen waar de autorisatie(code) heengaat.
- In geval van doorautoriseren, bepaalt en geautoriseerde partij wie de vervolgautorisatie (autorisatiecode) ontvangt. De regie ligt hier dus bij de partij die de autorisatie in eerste instantie heeft ontvangen.

Informatielaag

- Er wordt een autorisatie-URL of code gebruikt.

- Bij verwijscode wordt een centrale voorziening gebruikt waarin gepseudonimiseerde (niet op persoon herleidbare) autorisatie-URL's worden geregistreerd. Verwerkt geen persoonsgegevens.

Applicatielaag

- Er is geen toestemmingsvoorziening nodig, autorisatie wordt gepusht.

Veronderstelde of expliciete toestemming is mogelijk, gegeven vanuit de bron. Autorisatiecodes geven aanvullende opties voor de patiënt om 'toestemming' te geven door een autorisatiecode te geven aan de zorgverlener/zorgaanbieder die mag opvragen.

- Indien er wel (specifieke) toestemming nodig is, - bijvoorbeeld als een arts meer gegevens wil delen dan strikt noodzakelijk binnen de huidige behandeling) dan nog is geen (centrale) VOORZIENING nodig om de toestemming te registreren (voor meervoudig/later gebruik).
- (push autorisatiebeslissingen worden "lokaal" in het proces genomen).

Technische laag

| |
|---|
| • Push = drager onafhankelijk (URL of code via brief, telefoon, mail, e.d.) |
| • Push autorisatie is gebaseerd op bestaande (internationale) standaarden: WC3 web standaarden, inclusief REST, JSON-RPC, DNS, X.509, mTLS, [ii]. Push autorisatie wordt gestandaardiseerd via een eigen standaardisatie organisatie (**Decozo**), ook voor internationaal gebruik. Technische standaard is ondergebracht bij **deze** onafhankelijke stichting voor beheer en onderhoud. |

## 3. Toepasbaarheid Push Autorisatie

### 3.1 Algemeen

Push autorisatie is geschikt om informatie specifiek beschikbaar te stellen. Uitgangspunt is dat de bron van de gegevens bepaalt wie geautoriseerd wordt en welke gegevens in kunnen worden gezien of opgehaald kunnen worden.

Afhankelijk van de use-case kan bij push autorisatie voorafgaande uitdrukkelijke toestemming verplicht zijn. Daarnaast kan een patiëntenportaal of een PGO fungeren als een autorisatie hub via welke de patiënt zelf (of diens verzorger) autorisaties kan uitgeven aan bepaalde zorgverleners/zorgaanbieders. In die zin kan met push autorisatie een (decentrale) toestemmingsvoorziening geïmplementeerd worden, die uitgaat van de principes van actieve push autorisatie vanuit de bron, via een patiënt naar de ontvanger.
Voordelen bij het toepassen van push autorisatie:
Er wordt gericht voor bepaalde gegevens autorisatie gegeven. Toestemming kan door een patiënt gegeven worden specifiek aan bij de behandeling betrokken zorgverlener(s).
Kantekening bij het toepassen van push autorisatie:
Het leidend principe bij push autorisatie is dat de bron bepaalt wie wat mag inzien, uitgaande van de verplichtingen die het beroepsgeheim oplegt. Dit is in tegenstelling tot het principe dat de (raadplegend) zorgverlener zelf zou moeten kunnen bepalen welke informatie voor hem van belang is.1

### 3.2 Push Autorisatie als uitwisselconcept in Twiin

Twiin kent 4 uitwisselconcepten voor databeschikbaarheid voor verschillende functionele use-casus:

1. Push – Versturen van data
2. Notified pull : Verstuur notificatie en ontvanger haalt data op
3. Gerichte bevraging: zorgaanbieder A vraagt data op bij zorgaanbieder B
4. Geïndexeerde bevragingen: zorgaanbieder A bevraagt via een index alleen de zorgaanbieders die data voor de patiënt beschikbaar hebben.

Bij 1 en 2 geldt: het is bekend met wie de data gedeeld wordt en om welke data het gaat. In beide gevallen zou push autorisatie ingezet kunnen worden.
Het concept van push autorisatie ligt dicht bij het Twiin uitwisselconcept Notified Pull gebaseerd op de Technical Agreement (TA) Notified pull met FHIR. Immers: hier wordt geen data naar een ontvanger gestuurd, maar wordt een specifieke ontvanger geattendeerd op specifieke data die van belang is. Om deze reden is een analyse uitgevoerd naar verschillen en overeenkomsten tussen deze twee. Zie tabel bijlage 1.
Uit de analyse blijken de volgende verschillen tussen push autorisatie en notified pull:

- Patiënt kan d.m.v. delen van de autorisatie(code) zelf bepalen met wie gegevens worden gedeeld.
- Autorisatie en lokalisatie zijn bij push autorisatie gecombineerd in een URL die desgewenst ook nog via een autorisatiecode kan worden gedeeld;
- Use case van push autorisatie is uitgebreider: doorautoriseren is integraal onderdeel van de push autorisatie standaard, hierdoor bestaat de mogelijkheid van het delen van meerdere bronnen binnen ketens en/of netwerken van bij de behandeling betrokken

zorgverleners/zorgaanbieder. Notified pull daarentegen gaat (net als Nuts) primair uit van 1-op-1 autorisaties/transacties.

### 3.3.1 Beeldbeschikbaarheid in de huidige implementatie

De huidige implementatie voor beeldbeschikbaarheid is gebaseerd op het IHE XDS-I/XCA-I integratieprofiel. De leveranciers die deze infrastructuren mogelijk maken houden zich vast aan het concept van IHE waarbij de integratieprofielen beschreven worden door de community en vervolgens getoetst op een Connectathon.
Push autorisatie is internationaal niet bekend bij IHE en om deze reden is het momenteel niet haalbaar om push autorisatie toe te voegen in de Nederlandse setting. Dit zou veel flexibiliteit vereisen van (ook internationaal) de IHE XDS-I/XCA-Leveranciers.

### 3.3.2 Push Beelden (functionaliteit Twiin Portaal)

Voor push van beelden ziet de werkgroep een goede toepassingsmogelijkheid. Dit is nader uitgewerkt in het werkdocument twiinportaal x push autorisatie. Indien push autorisatie wordt toegepast bij Twiin Portaal zou een centrale voorziening wellicht niet meer nodig zijn en zou de oplossing minder afhankelijkheid van mail (POP3) worden. Er zou bovendien een keuze gemaakt kunnen worden voor een DICOM standaard, zoals DICOM WEB. Hierdoor zou de oplossing meer generiek inzetbaar worden en zou er ook ondersteuning geboden kunnen worden aan bijvoorbeeld een spoed casus.
In het werkdocument worden scenario's uitgewerkt voor het gebruik van push autorisatie.

## 3.3 Toepasbaarheid van push autorisatie naast andere autorisatie mechanismes

Toepasbaarheid van push autorisatie naast andere autorisatie mechanismes, zoals:

- Twiin, Nuts en AORTA
- Decentrale en centrale oplossingen
- Compatibiliteit met andere manieren van autoriseren, en combineren van de verschillende manieren van autoriseren (in de keten)

Een grondige analyse op deze onderzoeksvraag heeft de werkgroep vanwege tijdsdruk helaas niet kunnen uitvoeren.
Push Autorisatie kan praktisch gezien toegepast worden in combinatie met andere autorisatie mechanismes. Hierbij komen er verschillende methodes en middelen voor de zorgverleners die op verschillende wijze in het werkproces van de zorgverlener worden vormgegeven. Het moet nog blijken of dit in de praktijk handig gaat werken.
De volledige decentralisatie van toestemming en autorisatie bij het gebruik van push autorisatie en het zoveel mogelijk vermijden van gemeenschappelijk beheerde voorzieningen met persoon herleidbare gegevens zijn belangrijke kenmerken en uitgangspunten van push autorisatie (in lijn met "zero trust" principes). Hiermee wordt een groep patiënten bediend die geen toestemming willen geven/ geen vertrouwen hebben in centrale voorzieningen.
Centrale voorzieningen (zoals Mitz) worden op het moment gerealiseerd. Een decentrale oplossing zoals push autorisatie kan bestaan naast een centrale oplossing. Autorisatie loopt dan via de centrale of decentrale oplossing. Wanneer welke oplossing wordt gebruikt is mogelijk afhankelijk van de use case of van de patiënt (bijv. wel/geen toestemming voor een elektronisch uitwissel systeem gegeven). Technisch gezien kunnen in verschillende scenario's oplossingen gevonden worden. Zorgen zijn er over de verscheidenheid aan combinaties van use cases en autorisatievoorkeuren.
Twiin sluit het gebruik van gemeenschappelijke voorzieningen niet uit, sterker nog dit moedigt Twiin juist aan bij de invulling van het Twiin vertrouwensmodel. Twiin beschrijft in de roadmap Twiin x Nuts echter wel een transitie naar meer decentralisatie en het gebruik van Verifiable Credentials en Dentralised Identifiers als potentiële Europese standaarden voor de (nabije) toekomst.

# 4. Conclusie

De analyse die de werkgroep heeft uitgevoerd heeft zijn beperkingen. In sessies is het concept van push autorisatie doorgrond en is de toepasbaarheid van het concept verkent. De werkgroep heeft, conform de opdracht, geen externen geconsulteerd en geen praktijk toetsing van het concept gedaan.

Er is geen praktijktoetsing van het concept gedaan en derhalve kan niets gezegd worden over de daadwerkelijke werking en integratie met (of naast) andere autorisatiemechanismen. In deze notitie wordt wel een inschatting van de schaalbaarheid en het gebruik van push autorisatie naast andere autorisatiemechanismen gegeven.

Concluderend kan over de toepasbaarheid van Push Autorisatie gesteld worden:

- Push autorisatie kan worden toegepast in situaties waarbij sprake is van een proces waarbinnen gerichte uitwisseling tussen partijen (eventueel in een keten) plaatsvindt; het proces moet duidelijk maken c.q. een aangrijpingspunt vormen om te bepalen wie bij de data moet kunnen en om welke data het gaat. Dit is het geval bij onder ander de volgende (algemene) workflows:
  - Verwijzen
  - Overdracht
  - Second opinion (evt. met doorautorisatie)
  - Collegiaal consult (evt. met doorautorisatie)

  Als we dit vergelijken met de uitwisselconcepten van Twiin zijn dit:
  - Push
  - Notified pull
- Het mechanisme van een drageronafhankelijke autorisatiecode geeft flexibiliteit in het proces waarbij een zorgverlener in het proces (die zelf geautoriseerd is en die hiertoe rechten heeft) of de patiënt zelf kan bepalen aan welke zorgverlener de toestemming wordt gegeven om geautoriseerd de gegevens op te halen.
- Er zijn veel overeenkomsten tussen push autorisatie en notified pull. Verschillend zijn:
  - Patiënt kan bij push autorisatie zelf bepalen met wie gegevens worden gedeeld;
  - Autorisatie en lokalisatie zijn bij push autorisatie gecombineerd in een URL;
  - Doorautorisatie is onderdeel van de Push Autorisatie standaard. Notified Pull gaat (net als Nuts) primair uit van 1-op-1 autorisaties/transacties.
- Push Autorisatie geeft de mogelijkheid om te zorgen dat mensen die geen toestemming willen geven voor c.q. geen vertrouwen hebben in centrale voorzieningen waarvoor zij toestemming voor moeten geven, ook bediend kunnen worden.
- Aandachtspunt en zorg bij het bestaan van verschillende autorisatiemechanismen (centraal en decentraal) bij verschillende use cases:
  - Onoverzichtelijkheid voor de zorgverleners en burgers
  - Mogelijk extra registratielast
  - Verscheidenheid aan combinaties van use cases en autorisatievoorkeuren.

Conclusie ten slotte aan de hand van de onderzoeksvragen:

### 4.1 Toepasbaarheid van push autorisatie naast andere autorisatie mechanismes

Technisch gezien kunnen verschillende autorisatie mechanismes naast elkaar bestaan. Dit kan recht doen aan patiënten die geen toestemming willen geven voor het gebruik een elektronisch uitwisselingssysteem, of die geen toestemming willen vastleggen in een centrale voorziening. Niet onderzocht maar aandachtspunt bij verder onderzoek is de overzichtelijkheid voor zorgverleners en burgers bij gebruik van verschillende autorisatiemechanismen. Een ander aandachtspunt is de mogelijk bijkomende registratielast. Hierbij is relevant dat push autorisatie kan worden toegepast onder veronderstelde toestemming.

### 4.2 Mogelijkheden voor andere startpunten dan de huisarts

Niet alleen de huisarts kan het startpunt zijn van autorisatie ook andere bronnen kunnen het startpunt zijn.

### 4.3 Impact van push autorisatie voor zorgveld (zorgaanbieders en leveranciers)

Deze vraag hebben we door de onderzoeksopzet niet uitvoerig kunnen beantwoorden.