

# Informatiesysteemarchitectuur AORTA



**NICTIZ**

**Nationaal ICT Instituut in de Zorg**

postadres: Postbus 262, 2260 AG Leidschendam  
bezoekadres: Overgoo 11, 2266 JZ Leidschendam  
telefoon: (070) 317 34 50; fax: (070) 320 74 37; e-mail: [info@NICTIZ.nl](mailto:info@NICTIZ.nl)  
[www.NICTIZ.nl](http://www.NICTIZ.nl)

Versie : 3.0  
Datum : 31 mei 2007



# Inhoudsopgave

1	Inleiding .....	5
1.1	Doel.....	5
1.2	Doelgroep.....	5
1.3	Versie, status en wijzigingshistorie .....	5
1.4	Achtergrond.....	7
1.5	Reikwijdte .....	8
1.6	Structuur.....	9
1.7	Samenhang met andere documenten.....	10
2	Uitgangspunten .....	11
2.1	Normatieve referenties.....	11
2.2	Informatieve referenties.....	11
2.3	Afkortingen.....	12
2.4	Begrippen.....	12
3	Applicaties .....	13
3.1	Inleiding.....	13
3.2	Zorgaanbieder-applicaties .....	14
3.3	Patiënt/cliënt-applicaties .....	16
3.4	Beheerderapplicaties.....	18
4	Gebruiksscenario's .....	19
4.1	Inleiding.....	19
4.2	In-/uitloggen gebruiker (INL) .....	22
4.3	Selecteren patiënt/cliënt (SPA).....	26
4.4	{ toekomst} Selecteren zorgaanbieder (SZA) .....	33
4.5	Bijhouden Patiëntgegevens (BIJ) .....	37
4.6	Publiceren Patiëntgegevens (PUB) .....	40
4.7	{ toekomst} Abonneren Patiëntgegevens (ABO) .....	45
4.8	Initieel koppelen Patiëntgegevens (IKO) .....	46
4.9	Opvragen Patiëntgegevens (OPV) .....	49
4.10	Versturen Patiëntgegevens (STU) .....	55
4.11	Overdragen patiëntgegevens (OVD) .....	60
4.12	Beheren autorisatieprotocol (BAT) .....	63
4.13	Bijhouden autorisatieprofiel (BAF).....	67
4.14	Raadplegen toegangslag (RLO).....	73
4.15	Bijhouden mandateringen (BMD) .....	78
4.16	Aan/afsluiten zorgaanbiederapplicatie m.b.t. schakelpunt (ASL) .....	81
4.17	Beheren zorgaanbiederapplicatie (BZA) .....	84
4.18	Beheren schakelpunt (BSC) .....	86
4.19	Beheren patiëntenregister (BPR).....	93
4.20	Beheren zorgaanbiederregister (BZR).....	93
4.21	Beheren zorgaanbiedergids (BZG) .....	94
5	Objecten.....	95
5.1	Patiëntdossier (PDO).....	96
5.2	Schakelpunt (SCH) .....	100
5.3	Verwijsindex (VWI).....	104
5.4	Gegevenssoortentabel (GGS) .....	108
5.5	Autorisatieprotocol (APT) .....	109
5.6	Autorisatieprofiel (APF) .....	111

5.7	Identificatie & authenticatie-module (I&A) .....	113
5.8	Toegangslog (LOG) .....	114
5.9	Mandateringstabel (MDT) .....	120
5.10	Patiëntenregister (PAR) .....	121
5.11	Zorgaanbiederregister (ZAR) .....	123
5.12	{toekomst} Zorgaanbiedergids (ZAG) .....	125
5.13	Zorgaanbiedertabel (ZAT) .....	127
5.14	Configuratie tabellen (CFT) .....	129
6	Interacties .....	132
6.1	Aan-/afsluiten applicatie op schakelpunt .....	132
6.2	In/uitloggen gebruiker .....	134
6.3	Selecteren patiënt/cliënt .....	135
6.4	Selecteren zorgaanbieder .....	136
6.5	Opvragen patiëntgegevens .....	137
6.6	{toekomst} Abonneren patiëntgegevens .....	138
6.7	Publiceren patiëntgegevens .....	139
6.8	Versturen patiëntbericht .....	140
Bijlage A	- Invoering burgerservicenummer .....	142
A.1	Inleiding .....	142
A.2	Eerste contact met nieuwe patiënt/cliënt .....	143
A.3	Eerste contact met ingeschreven patiënt/cliënt .....	144
A.4	Initiële koppeling patiëntgegevens .....	146
A.5	Eerste contact initieel gekoppelde patiënt/cliënt .....	147
A.6	Vervolg contact met patiënt/cliënt .....	148
A.7	Ontvangst patiëntgegevens .....	149
A.8	Consequenties .....	150
Bijlage B	- {toekomst} Ongeadresseerde opdrachten .....	152
B.1	Inleiding .....	152
B.2	Oplossing met informatiedoorgever .....	153
B.3	Oplossing met verwijnsindex .....	154
B.4	Ontwerpkeuzes .....	155
Bijlage C	- Bijhouden van de verwijnsindex .....	156
C.1	Inleiding .....	156
C.2	Sleutel .....	156
C.3	Beperkingen bij heraanmelden of afmelden .....	157
C.4	Verantwoordelijke partij .....	158
C.5	Verplichte attributen bij aanmelden .....	158
C.6	Wijzigbare attributen bij heraanmelden .....	159
C.7	Voorwaarden voor aanmelden .....	160
C.8	Conclusie .....	162

# 1 Inleiding

## 1.1 Doel

Dit document is de informatiesysteemarchitectuur van AORTA.

AORTA gaat over de basisinfrastructuur in de zorg en de wijze waarop landelijke zorgtoepassingen daarvan gebruik kunnen maken. De basisinfrastructuur omvat gemeenschappelijke ICT-voorzieningen die algemeen toegankelijk zijn voor partijen in de zorg. Deze vormt de basis voor het doelmatige en beveiligd uitwisselen van gegevens tussen die partijen.

De informatiesysteemarchitectuur definieert en analyseert het werkgebied van AORTA in termen van:

- de applicaties die de verschillende gebruikers nodig hebben,
- de gebruiksscenario's die door die applicaties ondersteund moeten worden,
- de objecten zoals die voor de gebruikers zichtbaar zijn,
- de interacties die de objecten onderling hebben.

waarbij alle benodigde ICT-techniek nog buiten beschouwing worden gelaten.

Deze informatiesysteemarchitectuur is nodig om in het document [Technische architectuur] te kunnen bepalen welke ICT-techniek op welke manier wordt ingezet is om de benodigde ICT-voorzieningen te kunnen realiseren.

## 1.2 Doelgroep

Dit document is bedoeld voor partijen die zich bezighouden met de ontwikkeling van ICT-toepassingen in de zorg, zoals ontwikkelaars, leveranciers, onderzoekers, etc. De lezer wordt verondersteld een ICT-achtergrond en enige kennis van UML en HL7v3 te hebben. Voor een goed begrip van dit document, is het raadzaam eerst het document [Bedrijfs-architectuur] te lezen, aangezien dit document daarop gebaseerd is.

## 1.3 Versie, status en wijzigingshistorie

Deze Informatiesysteemarchitectuur AORTA was voorheen hoofdstuk 4 van het document "Specificatie van de Basisinfrastructuur in de Zorg". Na de Augustus2006-release is dit een zelfstandig document geworden in het kader van de herstructurering van de AORTA-documentatie. Daarbij is ook de nummering van eisen en beslissingen gewijzigd, zie paragraaf 1.6.

Ten opzichte van de "Specificatie van de Basisinfrastructuur in de Zorg" versie 2.4 zijn hier bovendien de volgende inhoudelijke wijzigingen doorgevoerd:

- 533: overdracht van patiëntstukken niet aanbieden maar ook aanvragen, zie paragraaf 4.11.
- 916: bij overnemen van patiëntstukken van andere zorgaanbieders naar het eigen dossier, moet de datum/tijd van overnemen worden vastgelegd, zie paragraaf 4.9.
- 986: een mandatering kan nooit een autorisatieprofiel overrulen, dit is niet zozeer een wijziging maar een verduidelijking, zie paragraaf 4.13 en 4.15.

- 1007: de toegangslog moet alle gebruikersinteracties loggen, ook voor patiënten/cliënten die bezwaar hebben gemaakt tegen elektronische uitwisseling van hun patiëntgegevens, zie paragraaf 5.8.
- 1017: gebruiker moet in toegangslog kunnen selecteren op agerende resp. reagerende zorgpartij, zie paragraaf 4.14.
- 1075: welke attributen van een verwijzing in de verwijsindex kunnen worden bijgewerkt? Zie paragraaf 5.3 en Bijlage C.
- 1086: betere definitie van zorgaanbieder, dit leidde in het gehele document tot vervanging van 'zorginstelling of zorgverlener' door 'zorgaanbieder'. Voor meer achtergrond, zie document [Bedrijfsarchitectuur].
- 1094: ingangsdatum voor een autorisatieregule in het autorisatieprofiel, zie paragraaf 4.13.
- 1097: UZI-register abonnee-nr als zorgaanbieder-id, zie paragraaf 5.11.
- 1103: de toegestane tijd voor het 'vasthouden' van opgevraagde patiëntgegevens wordt gemaximeerd, afhankelijk van de zorgtoepassing, zie paragraaf 4.9.
- 1116: foutcondities voor alle gebruiksscenario's integraal inventariseren en beschrijven, zie paragraaf 4.9 en document [Technische architectuur].
- 1120: in hoeverre moet de verwijsindex worden bijgehouden voor bezwaarde patiënten? Zie paragraaf 4.6, 5.3 en Bijlage C.
- 1139: logbeheerders krijgen geen UZI-pas en mogen geen privacygevoelige gegevens van de toegangslog kunnen inzien, zie paragraaf 4.14.
- 1141: het tijdelijk onderbreken en voortzetten van een gebruikerssessie door het snel uitnemen en opnieuw insteken van een vertrouwensmiddel wordt op {toekomst} gezet, zie paragraaf 4.2.
- 1145: eis om een WID te controleren op echtheidskenmerken, is komen te vervallen, zie paragraaf 4.3 en bijlage A.
- 1146: de SBV-Z levert nieuwe dienst voor het controleren of een WID in omloop is, zie paragraaf 4.3 en bijlage A.
- 1191: bewaartermijn van de toegangslog staat nog niet vast, zie paragraaf 4.14.
- 1192: het nieuwe "Besluit gebruik burgerservicenummer in de zorg" en het nieuw verschenen "Handboek gebruik burgerservicenummer in de zorg" geven aanleiding tot diverse kleine nodige wijzigingen rond het BSN, zie paragraaf 4.3, 4.5, 4.6, 4.8, 4.9, 4.10 en bijlage A.
- 1201: op welk aggregatieniveau patiëntgegevens moeten kunnen worden afgeschermd is afhankelijk van de desbetreffende zorgtoepassing, zie paragraaf 4.6.
- 1236: in afwachting van zorgaanbiedergids, moet in berichten bij iedere zorgaanbieder-id ook de zorgaanbieder-naam, zorgaanbieder-type en zorgaanbieder-bezoeklocatie en bij iedere zorgverlener-id ook de zorgverlener-naam worden vermeld, zie paragraaf 5.3, 5.8 en 5.13.
- 1262: logbeheerders kunnen geen verzoeken tot inzage in de toegangslog aannemen van patiënten, zie paragraaf 4.14. Evenzo kunnen autorisatiebeheerders geen verzoeken tot aanpassing autorisatieprofiel aannemen van patiënten, zie paragraaf 4.13.
- 1272: logbeheerders kunnen alleen verkeersgegevens inzien en geen inhoud van de uitgewisselde patiëntstukken, zie paragraaf 4.14.
- 1286: niet alle soorten zorgpartijen kunnen momenteel worden geïmplementeerd in het autorisatieprofiel, zie paragraaf 4.13.
- 1311: alle eisen met betrekking tot de zorgaanbiedergids worden op {toekomst} gezet, zie paragraaf 4.4 en 5.12.

## 1.4 Achtergrond

NICTIZ werkt onder meer aan de ontwikkeling van een landelijke basisinfrastructuur in de zorg, AORTA genaamd, die mogelijk moet maken dat zorgaanbieders, en later ook zorgverzekeraars en patiënten, ten behoeve van verschillende zorgtoepassingen op landelijke schaal patiëntgegevens kunnen uitwisselen.

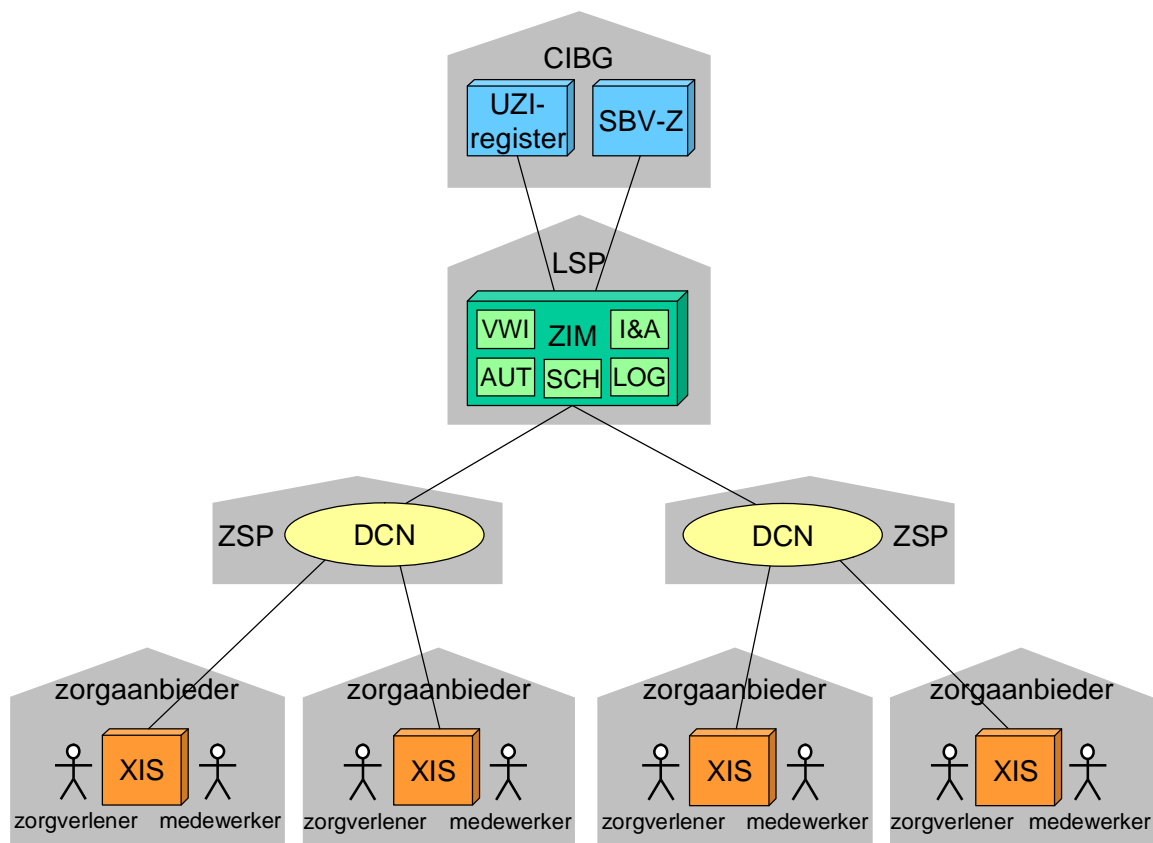
De volgende landelijke zorgtoepassingen zijn onder meer gepland voor AORTA:

- elektronisch medicatiedossier (EMD)
- waarneemdossier huisartsen (WDH)
- spoedeisende-hulpdossier (SEH)
- elektronisch pathologiedossier (PAD)

Centraal in AORTA staat de zorginformatiemakelaar (ZIM), die wordt geëxploiteerd door het landelijke schakelpunt (LSP). Daarop kunnen zorgaanbieders hun bestaande zorginformatiesystemen (ook wel XIS'en genoemd) aansluiten, mits zij voldoen aan de eisen van een goed beheerd zorgsysteem (GBZ). Die aansluiting vindt plaats via data-communicatienetwerken (DCN), die worden geëxploiteerd door zorgserviceproviders (ZSP).

Voor het uniek identificeren van patiënten, zorgaanbieders en zorgsystemen wordt gebruik gemaakt van landelijke registers: het UZI-register (Unieke Zorgverleners Identificatie) en de SBV-Z (Sectorale BerichtenVoorziening in de Zorg van het BSN-stelsel).

De onderstaande figuur toont op vereenvoudigde wijze hoe zorgaanbieders met hun XIS via het DCN van een ZSP worden aangesloten op de ZIM van het LSP, opdat zorgverleners en hun medewerkers vanuit hun eigen XIS op landelijke schaal patiëntgegevens kunnen uitwisselen met andere zorgaanbieders.



Het LSP, de SBV-Z en het UZI-register zijn reeds operationeel. Binnenkort zullen de eerste zorgaanbieders aansluiten op het LSP in het kader van een pilot met de zorgtoepassingen EMD en WDH.

## 1.5 Reikwijdte

Omdat het toepassingsgebied van ICT in de zorg zeer groot is, beperkt AORTA zich voorlopig tot het landelijke elektronische patiëntdossier (EPD), m.a.w. de uitwisseling van patiëntgegevens tussen zorgaanbieders en hun patiënten/cliënten. Later zal de uitwisseling van informatie met zorgverzekeraars en andere zorgpartijen worden uitgewerkt. Naar verwachting zijn de meeste architectuurprincipes in dit document ook toepasbaar voor de zorgverzekeraars.

AORTA richt zich voornamelijk op de eisen voor de basisinfrastructuur, dus de gemeenschappelijke ICT-voorzieningen en het beheer daarvan, en bemoeit zich niet onnodig met de gang van zaken binnen zorgaanbieders of de functionaliteit van hun ICT-voorzieningen. Toch is het onvermijdelijk ook eisen te stellen aan de individuele ICT-voorzieningen binnen zorgaanbieders en het beheer daarvan. Daarbij gaat het zowel om technische eisen, inzake de wijze waarop zorgsystemen dienen te communiceren met de basisinfrastructuur, als om organisatorische eisen, inzake het daadwerkelijke gebruik en beheer van die zorgsystemen. Als aan die eisen wordt voldaan, krijgt de individuele ICT-voorziening binnen de zorgaanbieder het predikaat Goed Beheerd Zorgsysteem (GBZ).

Daarnaast concentreert dit document zich op de generieke functionaliteit die de basisinfrastructuur biedt aan de vele verschillende zorgtoepassingen: faciliteiten voor het



uitwisselen van patiëntgegevens tussen zorginformatiesystemen. Binnen AORTA worden generieke berichten gedefinieerd, ter ondersteuning van de specifieke berichten voor de verschillende, bestaande en toekomstige zorgtoepassingen. De invulling van deze specifieke berichten is het werkterrein van het programma Zorgtoepassingen. Toch worden deze specifieke berichten in dit document in generieke zin meegenomen, om duidelijk te maken hoe de basisinfrastructuur deze afhandelt. De generieke functionaliteit omvat verder de verwijs-, de identificatie-, authenticatie-, autorisatie- en loggingfuncties, en wordt ondergebracht bij de Zorg Informatie Makelaar (ZIM).

Tenslotte richt de AORTA-architectuur zich vooral op de gewenste, toekomstige situatie van ICT in de zorg. Voorlopig heeft de zorgsector te maken met zeer verschillende, gesloten zorginformatiesystemen, die op één of andere manier moeten kunnen worden aangesloten op de basisinfrastructuur. Derhalve dient de basisinfrastructuur flexibel genoeg te zijn om bestaande zorginformatiesystemen te accommoderen én mee te buigen met toekomstige ontwikkelingen.

## 1.6 Structuur

Hoofdstuk 3 geeft een kort overzicht van de verschillende soorten *gebruikersapplicaties* en beschrijft globaal hoe die applicaties gebruik kunnen maken van de verschillende objecten zoals geïdentificeerd in de Bedrijfsarchitectuur van AORTA.

Hoofdstuk 4 analyseert in een aantal *gebruiksscenario's* de mogelijke informatiebehoefte van gebruikers en beschrijft de wijze waarop de benodigde gegevens kunnen of moeten worden ingevoerd door de gebruiker resp. gepresenteerd aan de gebruiker.

Hoofdstuk 5 geeft een nadere analyse van de verschillende *objecten* zoals geïdentificeerd in de Bedrijfsarchitectuur van AORTA.

Hoofdstuk 6 beschrijft tenslotte de *interacties* tussen de applicaties uit hoofdstuk 3 en de objecten uit hoofdstuk 5 als gevolg van de gebruiksscenario's uit hoofdstuk 4.

Een rode draad door de architectuur van AORTA wordt gevormd door een stelsel van:

- *gebruiks-scenario's*, binnen dit document gemarkeerd met `[ccc.Snn]` waarbij ccc een categorie aanduidt en nn een nummer is. Buiten dit document kan hiernaar worden verwezen met [AORTA·IA·ccc·Snn].
- *architectuur-eisen*, binnen dit document gemarkeerd met `[ccc.Enn]` waarbij ccc een categorie aanduidt en nn een nummer is. Buiten dit document kan hiernaar worden verwezen met [AORTA·IA·ccc·Enn].
- *architectuur-beslissingen*, binnen dit document gemarkeerd met `[ccc.Bnn]` waarbij ccc een categorie aanduidt en nn een volgnummer is. Buiten dit document kan hiernaar worden verwezen met [AORTA·IA·ccc·Bnn].

De verschillende categorieën ccc komen terug in de desbetreffende paragraaftitels en zijn derhalve gemakkelijk terug te vinden in de inhoudsopgave.

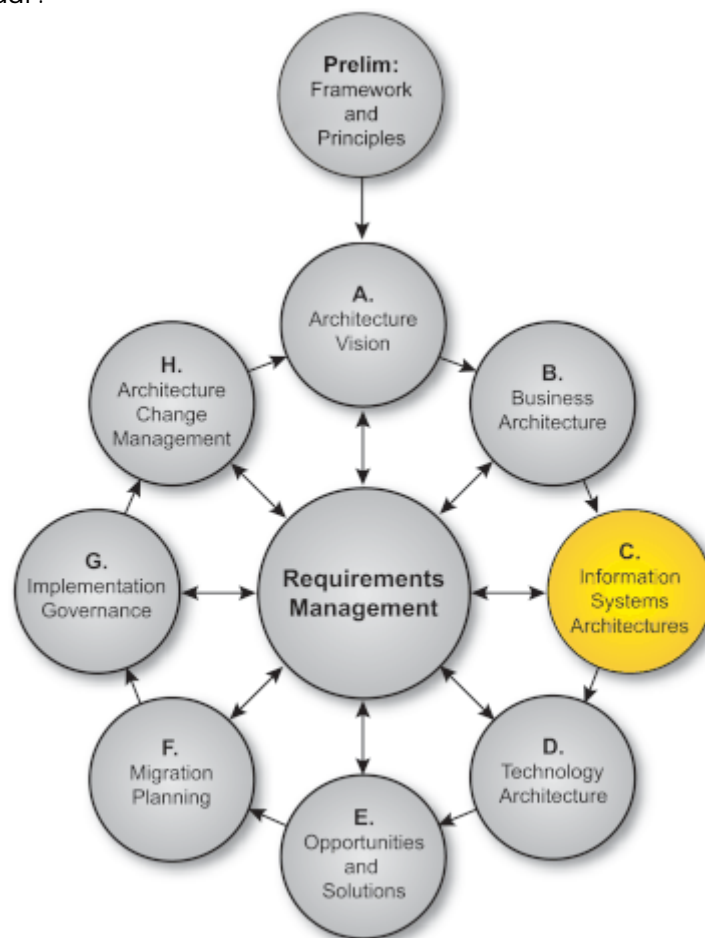
Scenario's, eisen en beslissingen die niet op korte termijn kunnen worden gerealiseerd, hebben het predikaat {toekomst} gekregen.

## 1.7 Samenhang met andere documenten

Voor AORTA is een architectuur ontwikkeld en ondergebracht in de volgende documenten:

- Architectuurvisie
- Bedrijfsarchitectuur
- Informatiesysteemarchitectuur
- Technische architectuur

Deze indeling is gebaseerd op de *Architecture Development Cycle* van TOGAF, zie de onderstaande figuur.



Tenslotte is dit document onderdeel van de AORTA-baseline zoals gedefinieerd in het document [Documentatieoverzicht].

## 2 Uitgangspunten

### 2.1 Normatieve referenties

De onderstaande documenten zijn beschouwd als leidend voor dit document:

Referentie	Document(en)	Bron
[Architectuurvisie]	"Architectuurvisie AORTA"	NICTIZ
[Bedrijfsarchitectuur]	"Bedrijfsarchitectuur AORTA"	NICTIZ
[HL7v3]	"HL7 Version 3 Standard".	Health Level Seven, Inc
[BSN]	een verzameling documenten m.b.t. het BSN-stelsel	www.programmabsn.nl
[SBV-Z]	een verzameling documenten m.b.t. de SBV-Z	www.sbv-z.nl onder "Technische specificaties"
[UZI]	een verzameling documenten m.b.t. het UZI-register	www.uzi-register.nl
[WBP]	"Wet Bescherming Persoonsgegevens"	
[WGBO]	"Wet op de geneeskundige behandelingsovereenkomst"	
[Wbsn-z]	voorstel tot "Wet gebruik burgerservicenummer in de zorg"	VWS
[Bbsn-z]	voorstel tot "Besluit gebruik burgerservicenummer in de zorg"	VWS
[Hbsn-z]	"Handboek invoering en gebruik burgerservicenummer in de zorg"	VWS
[NEN7510]	"Nederlandse norm NEN7510 (nl), Medische Informatica – Informatiebeveiliging in de zorg - Algemeen"	NEN

### 2.2 Informatieve referenties

De onderstaande documenten hebben gediend als bron voor dit document:

Referentie	Document(en)	Bron
[Documentatie-overzicht]	"Documentatieoverzicht AORTA-basisinfrastructuur"	NICTIZ
[Verklarende woordenlijst]	"Verklarende woordenlijst AORTA"	NICTIZ
[Technische architectuur]	"Technische architectuur AORTA"	NICTIZ
[IH Generieke berichten]	"Implementatiehandleiding Generieke berichten"	NICTIZ

Referentie	Document(en)	Bron
[prENV13606:2003]	"Health Informatics – Electronic Health Care Record communication", revised final draft, May 1999	CEN/TC251
[Tijdmachine]	"Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences"	artikel van Ab Bakker voor IMIA Working Conference "Realizing Security of the Electronic Health Record", 31 mei - 3 juni 2003, Varenna, Italië
[EMD-autorisatie]	"Modelrichtlijn en modelvoorlichtingsmateriaal autorisatie voor koplopers Electronisch Medicatie Dossier", versie 1.0, november 2005, Leidschendam	NICTIZ
[WDH-autorisatie]	"Modelrichtlijn en modelvoorlichtingsmateriaal autorisatie voor koplopers Waarneem Dossier Huisartsen", versie 1.0, november 2005, Leidschendam	NICTIZ
[UML]	"UML in a Nutshell, a desktop quick reference" 1 <sup>st</sup> edition 1998, Sinan Si Alhir, O'Reilly and Associates Inc. USA	

## 2.3 Afkortingen

Zie het document [Verklarende woordenlijst].

## 2.4 Begrippen

Zie het document [Verklarende woordenlijst].

## 3 Applicaties

### 3.1 Inleiding

Voor de verschillende zorgpartijen zullen gebruikersapplicaties nodig zijn om deze zorgpartijen te ondersteunen bij hun taken, bijv. door het vastleggen en uitwisselen van patiëntgegevens. Op welke technische ICT-voorzieningen deze applicaties draaien, wordt besproken in de [Technische architectuur]. Hier wordt verondersteld dat:

- zorgaanbiederapplicaties toegankelijk moeten zijn op een willekeurige werkplek van de desbetreffende zorgverlener,
- patiënt/cliëntapplicatie toegankelijk moeten zijn op een willekeurige woonplek, werkplek, of publieke locatie,
- diverse beheerapplicaties toegankelijk moeten zijn op een willekeurige werkplek van de desbetreffende beheerders.

In principe vormen de verschillende gebruikersapplicaties geen onderdeel van de basisinfrastructuur. Deze applicaties kunnen worden ontwikkeld in vele soorten en smaken. De benodigde standaardisatie rond applicaties valt onder het programma Zorgtoepassingen. Toch is het hier nodig een beeld te vormen van deze applicaties om te bepalen op welke wijze de basisinfrastructuur deze applicaties kan en moet ondersteunen met generieke functies.

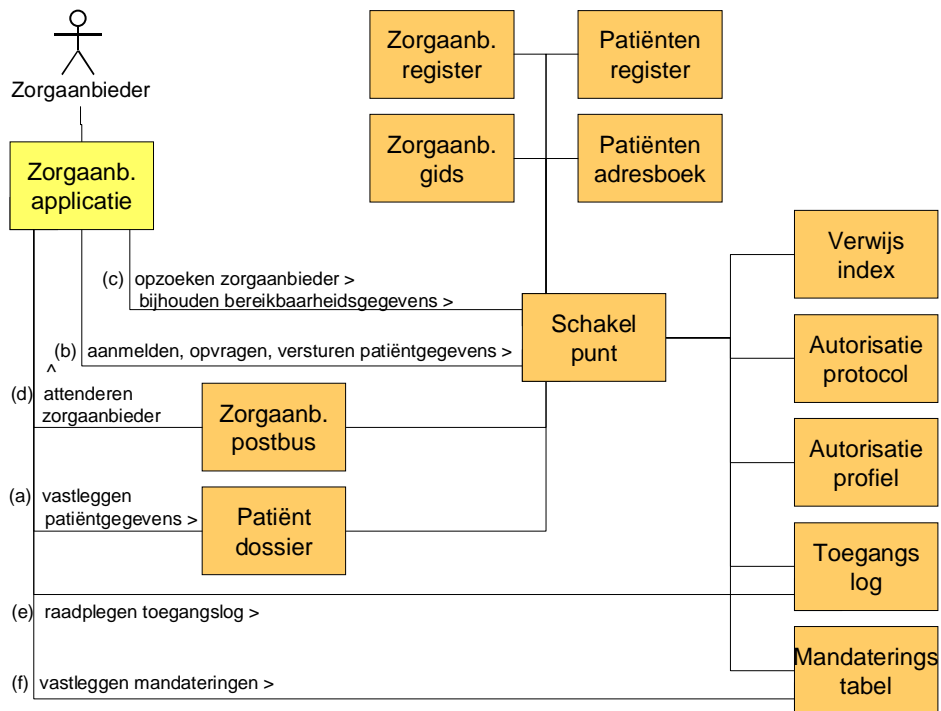
De basisinfrastructuur moet in principe mogelijk maken dat applicaties onderling alle soorten patiëntgegevens landelijk kunnen uitwisselen. Maar dat betekent nog niet dat één bepaalde applicatie daadwerkelijk alle soorten patiëntgegevens moet kunnen uitwisselen. Zoals zal blijken uit de volgende paragrafen, krijgen we te maken met gespecialiseerde applicaties die zich beperken tot specifieke zorgtoepassingen en daarbinnen een specifieke toepassingsrol hebben.

Bij landelijke uitwisseling van patiëntgegevens moet aldus van iedere applicatie kunnen worden vastgesteld:

- welke zorgtoepassingen de applicatie ondersteunt:
  - EMD,
  - WDH,
  - etc.
- welke toepassingsrol de applicatie daarbinnen ondersteunt:
  - EMD: voorschrijver, verstrekker, etc.
  - WDH: dossierhouder, waarnemer.

## 3.2 Zorgaanbieder-applicaties

Om zorgaanbieders zoveel mogelijk te ondersteunen bij het uitwisselen van patiëntgegevens, zijn specifieke zorgaanbiederapplicaties nodig voor de verschillende doeleinden. De onderstaande figuur toont dit in een UML collaboration diagram:



Hoewel bijv. een apotheker heel andere applicaties nodig heeft dan een radioloog, hebben beide toch behoefte aan dezelfde generieke functies. Aldus zijn zorgaanbiederapplicaties wenselijk die een zorgaanbieder in staat stellen tot:

- (a) het vastleggen van patiëntgegevens in het eigen patiëntdossier,
- (b) het aanmelden, opvragen en versturen van patiëntgegevens via het schakelpunt,
- (c) het bijhouden van de eigen bereikbaarheidsgegevens en het opzoeken van andere zorgaanbieders in de zorgaanbiedergids,
- (d) het geattendeerd worden wanneer patiëntgegevens door een andere zorgaanbieder of een patiënt/cliënt toegestuurd zijn,
- (e) het raadplegen van de toegangslog inzake bevestigingen van het eigen dossier door andere zorgaanbieders,
- (f) het mandateren van medebehandelaren en medewerkers.

Specifieke applicaties voor specifieke doeleinden zullen, ieder op een eigen wijze, de twee manieren van gegevensuitwisseling (haal- en breng-mechanisme, dus opvragen en versturen van patiëntgegevens) combineren. Voorbeelden zijn:

- *elektronisch voorschrijfsysteem*: deze applicatie kan een zorgaanbieder in staat stellen:
  - een overzicht van de actuele medicatie van een patiënt/cliënt te krijgen (opvragen patiëntgegevens: medicatievoorschriften en -verstrekkingen)
  - een recept uit te schrijven (vastleggen patiëntgegevens + aanmelden patiëntgegevens)
  - een apotheek in een bepaalde regio te selecteren (opzoeken zorgaanbieder)
  - een receptaanvraag te sturen naar een apotheek (versturen patiëntgegevens: opdracht)
  - de receptverstrekking bevestigd te krijgen door de apotheek (versturen patiëntgegevens: antwoord)
- *elektronische agenda*: deze applicatie kan een zorgaanbieder in staat stellen:
  - een overzicht van alle zorgaanbieders met een bepaalde functie in een bepaalde regio te krijgen (opzoeken zorgaanbieder)
  - van iedere zorgaanbieder inzicht in de wachtlijst te krijgen (opvragen patiëntgegevens: afspraken)
  - een afspraak aan te vragen binnen een gewenste tijdsruimte (versturen patiëntgegevens: opdracht)
  - de afspraak bevestigd te krijgen door de zorgaanbieder (versturen patiëntgegevens: antwoord)

Tenslotte zullen ook generieke applicaties nodig zijn voor:

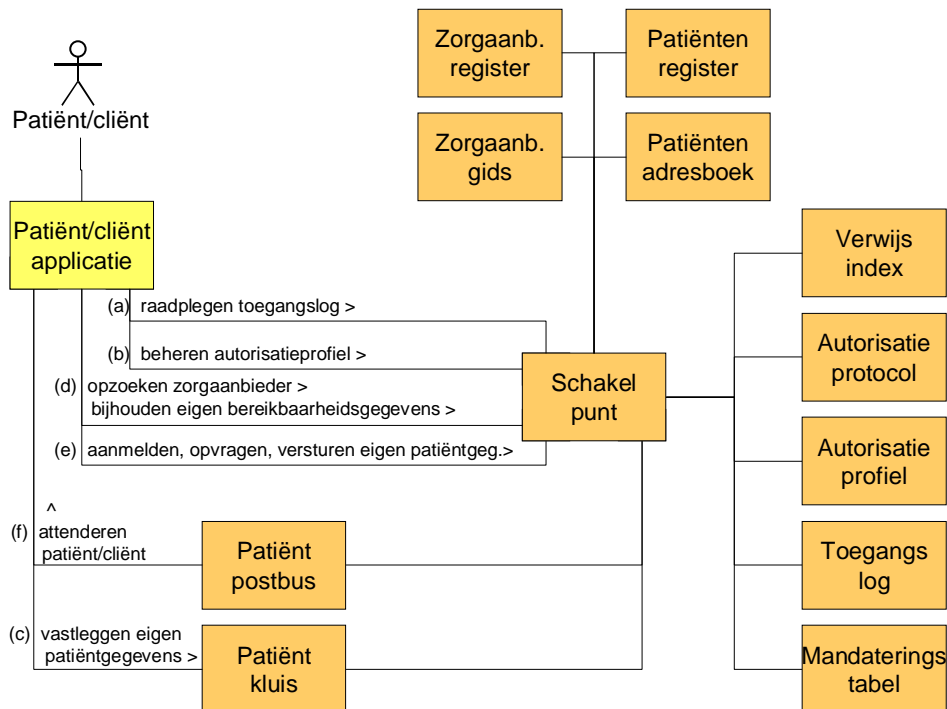
- *elektronisch dossier inkijken*: deze applicatie kan een zorgaanbieder in staat stellen:
  - een index van alle beschikbare patiëntgegevens van een patiënt/cliënt te krijgen (opvragen patiëntgegevens: index)
  - de beschikbare patiëntgegevens van een bepaalde gegevenssoort bij een specifieke zorgaanbieder nader in te kijken (opvragen patiëntgegevens: specifieke gegevenssoort)
- *elektronische post*: deze applicatie kan zorgaanbieders in staat stellen willekeurige berichten met patiëntgegevens te versturen (gestructureerd of niet).

Opmerkingen:

- de verschillende zorgaanbiederapplicaties met bijbehorende dossiers, postbussen en systeemvertrouwenmiddel vormen tezamen een zorginformatiesysteem, zoals een huisartsinformatiesysteem (HIS), apotheekinformatiesysteem (AIS), ziekenhuisinformatiesysteem ZIS, etc. In generieke zin worden deze vaak als XIS aangeduid.
- idealiter worden de verschillende gebruikersapplicaties zodanig geïntegreerd dat de zorgaanbieder naadloos kan overstappen van de ene naar de andere applicatie.
- in de praktijk zijn zorgapplicaties vaak veel complexer gestructureerd: vooral in grote zorginstellingen zijn er veel applicaties van verschillend fabrikaat, die onderling op zeer ingewikkelde wijze zijn geïntegreerd.

### 3.3 Patiënt/cliënt-applicaties

Ook patiënten/cliënten zullen in de toekomst op elektronische wijze hun rechten ten aanzien van hun patiëntgegevens willen uitoefenen. Om hen daarbij te ondersteunen, zijn patiënt/cliënt-applicaties wenselijk. De onderstaande figuur toont dit in een UML collaboration diagram:



Aldus zijn applicaties wenselijk die patiënten/cliënten in staat stellen tot:

- (a) het raadplegen van de toegangslog m.b.t. de eigen patiëntgegevens,
- (b) het beheren van het eigen autorisatieprofiel,
- (c) het vastleggen van eigen patiëntgegevens in hun eigen patiëntenkluis, opdat deze beschikbaar zijn voor opvraag door zorgaanbieders,
- (d) het bijhouden van eigen bereikbaarheidsgegevens in het patiëntenadresboek en het opzoeken van zorgaanbieders in de zorgaanbiedergids,
- (e) het aanmelden, opvragen en versturen van eigen patiëntgegevens,
- (f) het er op geattendeerd worden wanneer patiëntgegevens door een zorgaanbieder toegestuurd zijn.



Voor patiënt-/cliëntapplicaties geldt veelal hetzelfde als voor zorgaanbiederapplicaties. Immers, ook patiënten/cliënten kunnen behoefte hebben aan:

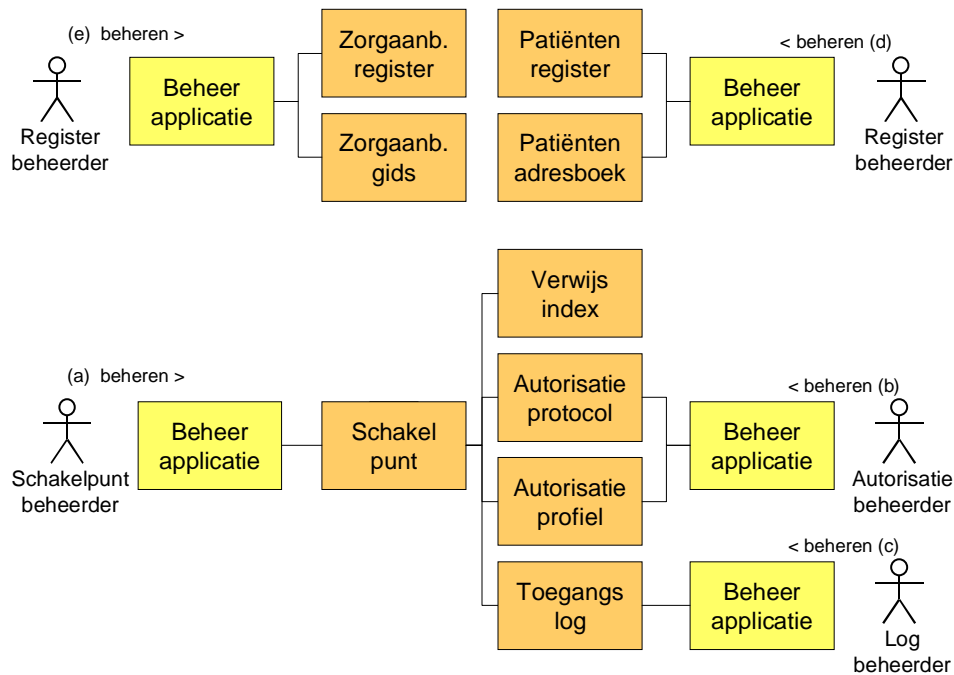
- *een elektronische agenda*: om zelfstandig een afspraak met een zorgaanbieder te kunnen maken,
- *een elektronisch dossier inkijken*: om hun recht uit te oefenen tot inzage in hun dossier bij de zorgaanbieder,
- *elektronische post*: om vragen te kunnen stellen aan een zorgaanbieder.

Opmerkingen:

- ad (c) Hier kan het bijv. gaan om telemedicine, het bijhouden van een logboek met eigen metingen of medicatiegebruik, het vastleggen van wensen met betrekking tot euthanasie, reanimatie, etc.
- ad (e) Langs deze weg krijgen patiënten/cliënten de mogelijkheid om zelfstandig inzage te krijgen in de eigen patiëntdossiers bij de verschillende zorgaanbieders. Het recht op aanvulling en vernietiging kan echter niet zelfstandig worden uitgeoefend, dat moet in overleg met de verantwoordelijke zorgaanbieder geschieden.

## 3.4 Beheerderapplicaties

Tenslotte hebben de verschillende beheerders behoefte aan ondersteuning in de vorm van beheerderapplicaties. De onderstaande figuur toont dit in een UML collaboration diagram:



Aldus zijn applicaties wenselijk die beheerders in staat stellen tot:

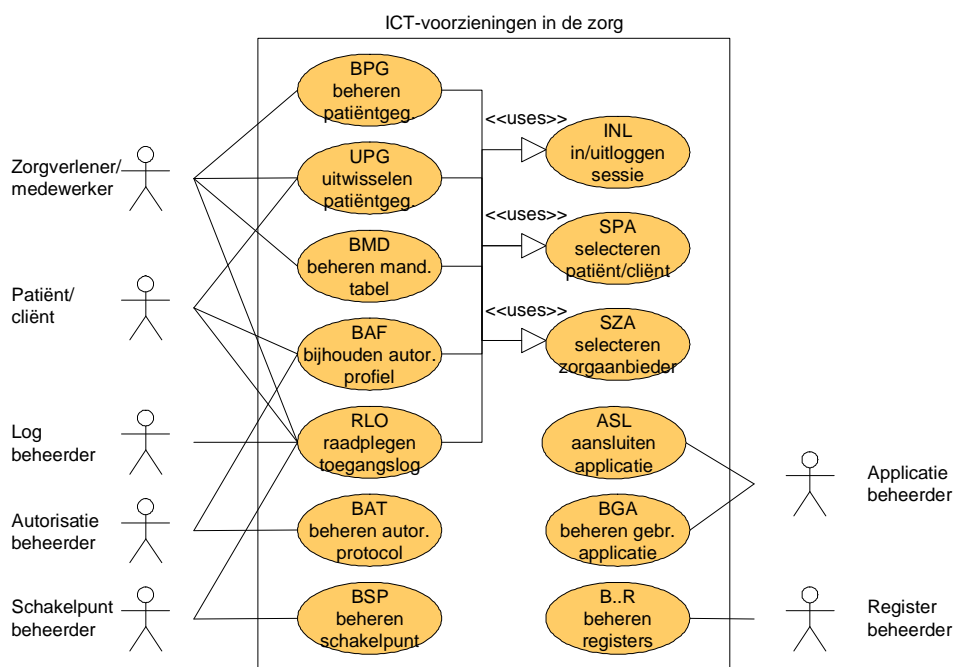
- (a) het beheren van het schakelpunt en de verwijzindex,
- (b) het bijhouden van het autorisatieprotocol en de autorisatieprofielen,
- (c) het raadplegen van de toegangsllog,
- (d) het beheren van het patiëntenregister,
- (e) het beheren van het zorgaanbiederregister.

Anders dan zorgaanbieders en patiënten/cliënten, zullen beheerders geen patiëntgegevens beheren of uitwisselen.

## 4 Gebruiksscenario's

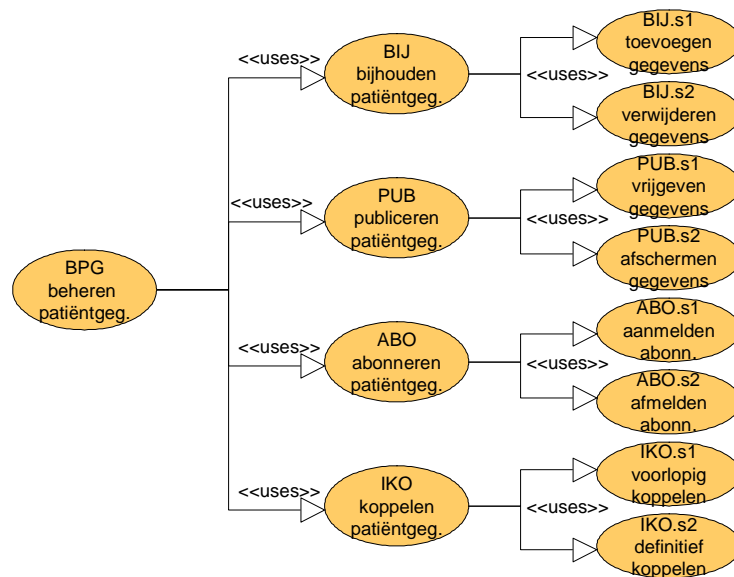
### 4.1 Inleiding

De onderstaande figuur toont *welke* gebruikers *welke* functionaliteit nodig hebben van de ICT-voorzieningen in de zorg, in een UML use case diagram:

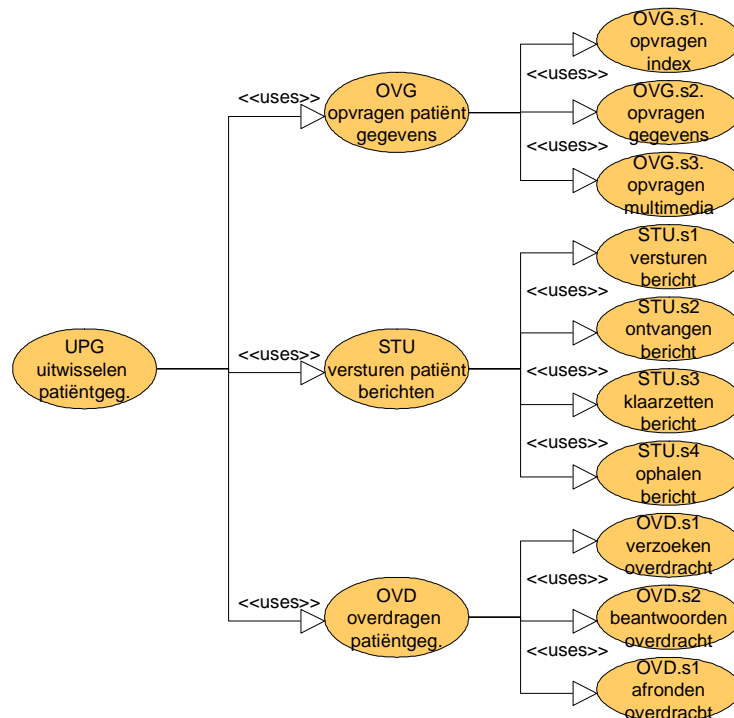


De gebruiksscenario's komen overeen met de benodigde functionaliteit beschreven in de hoofdstukken 7 tot en met 10 van de [Bedrijfsarchitectuur]. Merk op dat de gebruiksscenario's INL, SPA en SZA geen zelfstandige gebruiksscenario's zijn, maar een onderdeel van de andere gebruiksscenario's vormen.

De onderstaande figuur geeft een nadere uitwerking van gebruiksscenario BPG, *beheren patiëntgegevens*, in een UML use case diagram:

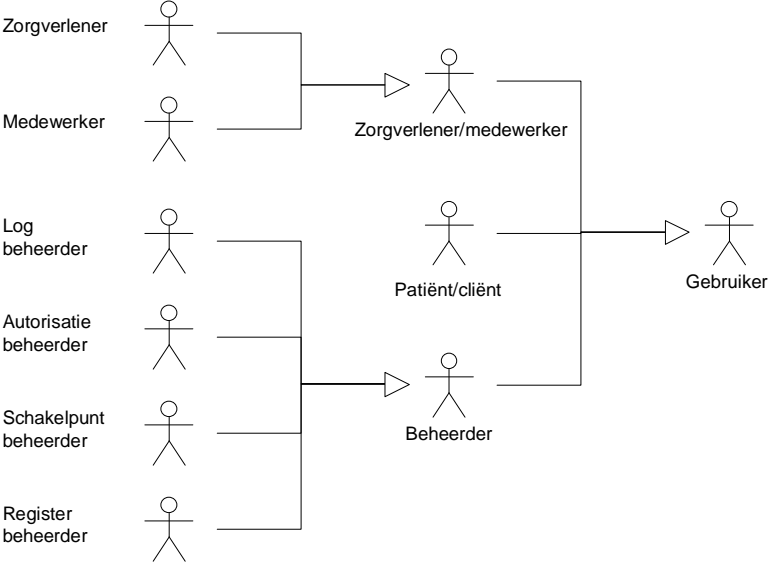


De onderstaande figuur geeft een nadere uitwerking van gebruiksscenario UPG, *uitwisselen patiëntgegevens*, in een UML use case diagram:



In de navolgende paragrafen worden deze gebruiksscenario's nader uitgewerkt naar eisen en wensen van de gebruiker. Deze gebruiksscenario's komen later terug in hoofdstuk 6, alwaar de interacties tussen de objecten voor elk van de gebruiksscenario's worden uitgewerkt. Gebruiksscenario [ABO] *abonneren patiëntgegevens* is nog niet uitgewerkt. Dit wordt in een latere versie voorzien.

Bij de uitwerking van de bovenstaande gebruiksscenario's in de navolgende paragrafen, zal blijken dat er behoefte is aan generalisaties van de bovengenoemde gebruikers. Deze worden samengevat in de onderstaande figuur:



## 4.2 In-/uitloggen gebruiker (INL)

Wanneer een zorgverlener/medewerker via een applicatie op een werkplek gebruik wil maken van zijn bevoegdheden tot het landelijk uitwisselen van patiëntgegevens, dient hij zich eerst te identificeren en authenticeren. Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 11.6 kan dat op verschillende vertrouwensniveaus.

Voor het vertrouwensniveau *laag* is zwakke authenticatie aan het begin van een sessie voldoende, dan wel normale of sterke authenticatie aan het begin van een werkdag. Dit kan als volgt worden geïmplementeerd:

- Inloggen aan het begin van iedere sessie, met een wachtwoord. Uitloggen aan het einde van de sessie.
- Inloggen aan het begin van een werkdag, door het invoeren van een vertrouwensmiddel in een leesapparaat op zijn werkplek. Uitloggen aan het einde van de werkdag.

Voor het vertrouwensniveau *midden* is het nodig dat voor iedere sessie sterke authenticatie plaatsvindt en vervolgens voor iedere landelijke uitwisseling van patiëntgegevens normale authenticatie plaatsvindt. Dit kan als volgt worden geïmplementeerd:

- Inloggen aan het begin van iedere sessie, door het invoeren van zijn vertrouwensmiddel in een leesapparaat op zijn werkplek en het intoetsen van een toegangscode. Uitloggen aan het einde van de sessie.
- Daarnaast moet voor iedere gebruikersinteractie (aanmelden, opvragen, versturen, etc.) met patiëntgegevens gecontroleerd worden dat het vertrouwensmiddel in het leesapparaat ingevoerd is.

Voor het vertrouwensniveau *hoog* is het nodig dat voor iedere landelijke uitwisseling van patiëntgegevens sterke authenticatie plaatsvindt. Dit kan als volgt worden geïmplementeerd:

- Voor iedere gebruikersinteractie (aanmelden, opvragen, versturen, etc.) met patiëntgegevens moet het vertrouwensmiddel in het leesapparaat ingevoerd zijn of opnieuw ingevoerd worden en moet een toegangscode worden ingetoetst. Na uitnemen van het vertrouwensmiddel verdwijnen de vertrouwelijke patiëntgegevens automatisch van het scherm.

Voor het uitloggen is geen vertrouwensmiddel vereist, zoals dat voor inloggen wel vereist is. Het uitloggen aan het einde van een sessie of een werkdag, kan op verschillende manieren:

- *Uitloggen op commando*: dit als enige manier is niet veilig omdat de zorgverlener/medewerker dit gemakkelijk kan vergeten of nalaten bij het verlaten van zijn werkplek, en de sessie dan blijft doorlopen;
- *Automatisch uitloggen door uitnemen vertrouwensmiddel*: dit als enige manier is niet veilig want het brengt de zorgverlener/medewerker in de verleiding zijn

vertrouwsmiddel in het leesapparaat achter te laten om niet te worden uitgelogd bij het tijdelijk verlaten van de werkplek,

- *Automatisch uitloggen na een tijdsinterval*: dit als enige manier is redelijk veilig, maar is onwerkbaar voor de zorgverlener/medewerker die onregelmatig op zijn werkplek zit,
- *Automatisch uitloggen na een tijdsinterval na verwijderen van het vertrouwsmiddel*: dit is het meest veilig en werkbaar.

Architectuurbeslissingen:

**INL·b01** Een zorgverlener/medewerker moet voor vertrouwensniveau *midden* aan het begin van een sessie inloggen door het invoeren van een persoonlijk vertrouwsmiddel én het intoetsen van een persoonlijke toegangscode. Daarna kan hij patiëntgegevens landelijk uitwisselen, gedurende een sessie die wordt onderbroken na verwijderen van het vertrouwsmiddel. Als het vertrouwsmiddel binnen een bepaald tijdsinterval opnieuw wordt ingevoerd, mag de sessie worden voortgezet zonder het hoeven invoeren van de toegangscode. Anders eindigt de sessie definitief na verstrijken van dit tijdsinterval.

**INL·b02** {toekomst} Een zorgverlener/medewerker moet voor vertrouwensniveau *hoog* voor iedere toegang tot patiëntgegevens inloggen door het invoeren van een persoonlijk vertrouwsmiddel én een persoonlijke toegangscode.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**INL·s01** inloggen van een gebruikerssessie.

**INL·s02** tijdelijk onderbreken van een gebruikerssessie.

**INL·s03** voortzetten van een onderbroken gebruikerssessie.

**INL·s04** uitloggen van de gebruikerssessie.

Bij gebruiksscenario [INL·s01] *inloggen sessie* gelden de volgende eisen en wensen:

**INL·e01** Een zorgverlener/medewerker moet een sessie voor het landelijk uitwisselen van patiëntgegevens op vertrouwensniveau *laag* kunnen starten door: het invoeren van zijn gebruikersnaam en wachtwoord.

**INL·e02** Een zorgverlener/medewerker moet een sessie voor het landelijk uitwisselen van patiëntgegevens op vertrouwensniveau *midden* kunnen starten door: het invoeren van zijn vertrouwsmiddel op de werkplek, en het invoeren van de bijbehorende toegangscode.

Bij gebruiksscenario [INL·s02] *onderbreken sessie* gelden de volgende eisen en wensen:

**INL·e03** {toekomst} Een zorgverlener/medewerker moet een sessie voor het landelijk uitwisselen van patiëntgegevens op vertrouwensniveau *midden* tijdelijk kunnen onderbreken door: het uitnemen van zijn vertrouwsmiddel op de werkplek.

Bij gebruiksscenario [INL.s03] *voortzetten sessie* gelden de volgende eisen en wensen:

**INL.e04** {toekomst} Een zorgverlener/medewerker moet die sessie voor het landelijk uitwisselen van patiëntgegevens op vertrouwensniveau *midden* binnen het tijdsinterval *gebruiker-max-kaart-uit* na onderbreking kunnen voortzetten door: het opnieuw invoeren van zijn vertrouwensmiddel op de werkplek, zonder het invoeren van de toegangscode.

Bij gebruiksscenario [INL.s04] *uitloggen sessie* gelden de volgende eisen en wensen:

**INL.e05** Een zorgverlener/medewerker moet een sessie voor het landelijk uitwisselen van patiëntgegevens op vertrouwensniveau *laag* of *midden* op de volgende manieren kunnen afsluiten:

- op commando (toetsaanslagen, muisklik, etc.),
- door het uitnemen van het vertrouwensmiddel,

**INL.e06** Een sessie voor het landelijk uitwisselen van patiëntgegevens op vertrouwensniveau *midden* moet in de volgende gevallen automatisch worden afgesloten:

- {toekomst} wanneer het vertrouwensmiddel meer dan het tijdsinterval *gebruiker-max-kaart-uit* uit de kaartlezer is verwijderd,
- wanneer deze sessie reeds gedurende het tijdsinterval *gebruiker-max-sessie-duur* open staat,
- wanneer de gebruiker via deze sessie gedurende het tijdsinterval *gebruiker-max-sessie-onbruik* geen gegevens meer landelijk heeft uitgewisseld,
- wanneer de gebruiker zijn gebruikersapplicatie gedurende het tijdsinterval *gebruiker-max-applicatie-onbruik* niet meer heeft gebruikt.

{toekomst} Voor deze gebruiksscenario's is het nodig dat de zorgaanbiederapplicatie zich als actief heeft gemeld bij het schakelpunt, zie gebruiksscenario [ASL.s01].

Opmerkingen:

- Het inloggen met een fysiek vertrouwensmiddel (bijv. chipkaart) kan door zorgverleners/medewerkers als gebruiksongemak worden ervaren, maar biedt ook nieuwe mogelijkheden. {toekomst} Zo wordt het in principe mogelijk in een apotheek te wisselen van werkplek, waarbij de gebruikerssessie met het vertrouwensmiddel wordt meegenomen, dat wil zeggen de sessie wordt op de oude werkplek afgebroken en op de nieuwe werkplek voortgezet.
- Het moeten inloggen om landelijk patiëntgegevens te kunnen uitwisselen, staat in principe los van het moeten inloggen voor de toegang tot de patiëntgegevens in het eigen patiëntdossier. Het eerste valt onder landelijk beleid, het tweede is een zaak voor de zorgaanbieder zelf. Toch kan een applicatie deze twee op slimme wijze combineren, door gebruik van hetzelfde vertrouwensmiddel.
- Het scenario van inloggen kan vervlochten met een ander gebruiksscenario plaatsvinden. Bijv. als een zorgverlener/medewerker ongemerkt was uitgelogd en vervolgens patiëntgegevens opvraagt, dan kan de applicatie na het opvraagcommando de gebruiker vragen opnieuw in te loggen.



- Ad [INL.b01] en [INL.e04] Voorzover NICTIZ bekend is, is er (nog) geen hardware/software verkrijgbaar die het mogelijk maakt dat geen toegangscode hoeft te worden ingetoetst wanneer het vertrouwensmiddel binnen een bepaald tijdsinterval opnieuw wordt ingevoerd. Dit betekent dat bij wisseling van werkplek altijd opnieuw een toegangscode moet worden ingetoetst.

### 4.3 Selecteren patiënt/cliënt (SPA)

Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 10.2 zal een zorgaanbieder die contact heeft met een patiënt/cliënt, die patiënt/cliënt moeten identificeren door het bepalen van diens landelijke patiëntnummer (BSN) en zonodig authenticeren door het controleren van diens Wettelijk Identificatie Document (WID).

Bovendien zal de zorgaanbieder bij het eerste contact na de invoering van het BSN extra controles moeten of willen uitvoeren, zoals uitgewerkt in bijlage A:

- het BSN opvragen of verifiëren bij het landelijke patiëntenregister,
- het WID controleren op gelijkheid met de patiënt/cliënt,
- het WID controleren op geldigheidsdatum,
- het WID controleren op echtheid,
- het WID controleren op het in omloop mogen zijn,
- het patiëntdossier inhoudelijk controleren met de patiënt/cliënt,
- de identificerende gegevens zonodig bijwerken.

Nadat het BSN is opgevraagd of geverifieerd in het landelijke patiëntenregister (BVBSN via SBV-Z), mag het BSN tezamen met de identificerende gegevens worden opgenomen in de lokale patiëntenindex of patiëntdossiers bij de zorgaanbieder, zodat de zorgaanbieder bij volgende contacten niet steeds het landelijke patiëntenregister hoeft te raadplegen. Omdat een zorgaanbieder voor een verschijnende patiënt/cliënt niet bij voorbaat weet of dit zijn eerste contact na de invoering van het BSN is, zal hij eerst in zijn patiëntenindex gaan zoeken.

Omdat de extra controles in de praktijk niet altijd bij het eerste contact kunnen worden uitgevoerd, zal voor iedere patiënt/cliënt moeten worden bijhouden welke controles wel/niet zijn uitgevoerd, opdat de zorgaanbieder bij een volgend contact kan worden geattendeerd op achterstallige controles. Dit is belangrijk want met achterstallige controles mogen patiëntgegevens niet landelijk worden uitgewisseld, we spreken dan van *voorlopig* gekoppelde patiëntgegevens. Als alle onzekerheden zijn opgelost, spreken we van *definitief* gekoppelde patiëntgegevens, zie ook paragraaf 5.1.

Architectuurbeslissingen:

**SPA·b01** Een zorgaanbieder moet een patiënt/cliënt eerst in zijn lokale patiëntenindex kunnen zoeken en daarna zonodig in het landelijke patiëntenregister.

**SPA·b02** Een zorgaanbieder moet voor iedere patiënt/cliënt kunnen bijhouden welke controles wel/niet zijn uitgevoerd.

Tenslotte zal de zorgaanbieder de bereikbaarheidsgegevens van de patiënt/cliënt in zijn patiëntenindex actueel willen houden. Sommige bereikbaarheidsgegevens, zoals het woonadres, zijn als identificerende gegevens op te vragen uit het landelijke patiëntregister.

Wanneer de originele identificerende gegevens en/of bereikbaarheidsgegevens ooit wijzigen, wil de zorgverlener/medewerker daarover worden ingelicht, bij voorkeur door het landelijke patiëntenregister of anders door middel van een gezamenlijk patiëntenadresboek, dat eventueel door patiënten/cliënten zelf kan worden bijgewerkt.

Zoals onderbouwd in paragraaf A.6, zijn hier aldus de volgende gebruiksscenario's te onderkennen:

**SPA·s01** identificeren patiënt/cliënt.

**SPA·s02** authenticeren patiënt/cliënt.

**SPA·s03** controleren patiëntdossier.

**SPA·s04** bijwerken patiëntenindex.

Bij gebruiksscenario [SPA·s01] *identificeren patiënt/cliënt* gelden de volgende eisen en wensen:

**SPA·e01** De gebruiker moet een patiënt/cliënt kunnen opzoeken in de lokale patiëntenindex dan wel de patiëntdossiers bij de zorgaanbieder door het invoeren van identificerende gegevens, waarna wordt getoond:

- of de patiënt/cliënt is gevonden, en zo ja
- of het BSN wel/niet is opgevraagd of geverifieerd in het landelijke patiëntenregister.

**SPA·e02** Indien bij [SPA·e01] de patiënt/cliënt niet is gevonden of blijkt dat nog geen BSN succesvol is opgevraagd of geverifieerd bij het landelijke patiëntenregister, moet de gebruiker na invoeren van (een deel van) de identificerende gegevens beschreven in [SBV-Z], het BSN van die patiënt/cliënt uit het landelijke patiëntenregister gepresenteerd of bevestigd kunnen krijgen.

**SPA·e03** Indien bij [SPA·e02] de patiënt/cliënt is gevonden, moet de gebruiker het BSN kunnen koppelen aan diens identificerende gegevens in de patiëntenindex of het patiëntdossier waarbij automatisch wordt vastgelegd bij het overgenomen BSN:

- de bron van het BSN,
- datum en tijd van koppelen,
- zorgverlener-id of andere identificatie van de gebruiker,

en waarbij de patiëntstukken die op dat moment in het patiëntdossier staan, worden bestempeld als *voorlopig* gekoppeld aan het BSN.

Bij gebruiksscenario [SPA·s02] *authenticeren patiënt/cliënt* gelden de volgende eisen en wensen:

**SPA·e04** De gebruiker moet na identificatie van een patiënt/cliënt:

- worden gewaarschuwd indien de zorgaanbieder zich er nog niet van heeft vergewist dat het BSN hoort bij de patiënt/cliënt,
- kunnen vastleggen in de patiëntenindex of het patiëntdossier dat hij zich ervan heeft vergewist dat het BSN hoort bij de patiënt/cliënt, onder vermelding van:
  - manier van vergewissen:
    - § WID-controle op echtheid, gelijkenis en geldigheidsdatum (verplicht voor nieuwe patiënten)
    - § anders (alleen voor ingeschreven patiënten)
  - datum en tijd
  - zorgverlener-id of andere identificatie van de gebruiker
  - in geval van WID-controle:

- § aard van het WID
- § nummer van het WID.

- de vastgelegde controlegegevens naderhand kunnen raadplegen.

**SPA·e05** Deze eis is vervallen.

**SPA·e06** De gebruiker moet na identificatie van een patiënt/cliënt:

- het in omloop mogen zijn van een WID kunnen controleren door raadplegen van het relevante WID-register na invoeren van de volgende WID-kenmerken:
  - aard van het WID
  - nummer van het WID
- kunnen vastleggen in de patiëntenindex of het patiëntdossier dat hij het in omloop mogen zijn van diens WID heeft gecontroleerd, onder vermelding van:
  - resultaat van de controle
  - datum en tijd
  - zorgverlener-id of andere identificatie van de gebruiker
  - aard en nummer van het WID
- de vastgelegde controlegegevens naderhand kunnen raadplegen.

Bij gebruiksscenario [SPA·s03] *controleren patiëntdossier* gelden de volgende eisen en wensen:

**SPA·e07** De gebruiker moet na identificatie van een patiënt/cliënt:

- worden gewaarschuwd indien diens patiëntdossier nog patiëntstukken bevat, die niet inhoudelijk zijn gecontroleerd met de patiënt/cliënt, en dus *voorlopig* zijn gekoppeld aan het BSN,
- deze patiëntstukken *definitief* kunnen koppelen aan het BSN door vast te leggen in het patiëntdossier dat hij heeft gecontroleerd dat ze inhoudelijk horen bij de patiënt/cliënt, onder vermelding van:
  - resultaat van de controle
  - datum en tijd
  - zorgverlener-id of andere identificatie van de gebruiker,
  - zorgverlener-id van de mandaterende zorgverlener, indien van toepassing
- deze patiëntstukken anders kunnen ontkoppelen van het BSN,
- de vastgelegde controlegegevens naderhand kunnen raadplegen.

**SPA·e08** De gebruiker moet de eerste keer nadat alle controles positief zijn, worden doorgeleid naar gebruiksscenario [PUB·s01] *vrijgeven patiëntgegevens*.

Bij gebruiksscenario [SPA·s04] *bijwerken patiëntenindex* gelden de volgende eisen en wensen:

**SPA·e09** De gebruiker moet na identificatie van een patiënt/cliënt op basis van diens BSN uit het landelijke patiëntenregister diens persoonsgegevens kunnen opvragen.

**SPA·e10** De gebruiker moet na raadplegen van het landelijke patiëntenregister voor een patiënt/cliënt, zoals bedoeld in [SPA·e02] of [SPA·e09]:

- worden gewaarschuwd indien blijkt dat:

- diens identificerende gegevens in de patiëntenindex of diens patiëntdossier afwijken van de persoonsgegevens in het landelijke patiëntenregister,
- er aanvullende persoonsgegevens zijn,
- er uitzonderingen zijn zoals gedefinieerd in document [Hbsn-z] bijlage 1,
- desgewenst deze afwijkingen, aanvullingen en uitzonderingen kunnen overnemen naar de patiëntenindex of diens patiëntdossier, onder automatische vermelding van:
  - datum en tijd van overnemen,
  - zorgverlener-id of andere identificatie van de gebruiker.

**SPA·e11** {toekomst} De gebruiker moet kunnen aangeven dat hij voor een bepaalde patiënt/cliënt wil worden ingelicht door een patiëntenadresboek over eventuele wijzigingen van diens identificerende gegevens en bereikbaarheidsgegevens.

**SPA·e12** {toekomst} De gebruiker moet, na een signaal dat de identificerende gegevens en bereikbaarheidsgegevens van een patiënt zijn gewijzigd, de nieuwe gegevens kunnen overnemen in de patiëntenindex of diens patiëntdossier, waarbij automatisch wordt vastgelegd:

- datum en tijd van overnemen,
- zorgverlener-id of andere identificatie van de gebruiker.

Voor al deze gebruiksscenario's is het nodig dat de gebruiker heeft ingelogd als zorgverlener of medewerker op vertrouwensniveau *laag* of *midden*, zie gebruiksscenario [INL·s01]. In geval van gebruiksscenario [SPA·s03] moet de medewerker gemandateerd zijn door een zorgverlener.

Opmerkingen:

- Binnen een zorgaanbieder kan men volstaan met eenmalige identificatie en authenticatie van een patiënt/cliënt, indien de verschillende afdelingen of zorgverleners het BSN of een daaraan gekoppeld lokaal patiëntnummer gebruiken. De controle van de dossiers zal iedere afdeling of zorgverlener afzonderlijk moeten doen, indien zij afzonderlijke dossiers hebben, zie ook ad [SPA·e07].
- Volgens Bbsn-z artikel 25 hoeven apothekers geen BSN te bepalen en geen WID te controleren, omdat medicatie vaak door derden wordt afgehaald. Derhalve zouden de meeste eisen in deze paragraaf niet gelden. Maar een apotheker verstrekt ook medicijnen zonder recept. Die wil hij vervolgens toevoegen aan het juiste patiëntdossier ten behoeve van de medicatiebewaking. Daarvoor zal de apotheker toch tenminste het BSN moeten opvragen bij de SBV-Z. En in twijfelgevallen moet hij alsnog het WID raadplegen en controleren. Als er dan geen WID is, mag hij het BSN niet gebruiken. Dit betekent dat alle eisen in deze paragraaf toch gelden, alleen de waarschuwing van eis [SPA·e04] geldt niet voor apothekers.
- Ad eis [SPA·e01] Dit is de enige stap die altijd plaatsvindt voor ieder contact tussen een zorgaanbieder en een patiënt/cliënt. De overige stappen vinden alleen plaats als na de invoering van het BSN nog achterstallige controles moeten worden uitgevoerd.
- Ad eis [SPA·e01] en [SPA·e02] Voor het zoeken in de patiëntdossiers bij de zorgaanbieder hoeven niet dezelfde zoekpaden te worden gebruikt als voor het opvragen en verifiëren in het landelijke patiëntenregister. Lokaal zoeken kan immers

verscheidene hits opleveren waaruit kan worden gekozen, echter met het risico van fout kiezen. Het landelijk patiëntregister biedt geen zoekfunctionaliteit maar alleen functies voor het opvragen en verifiëren van het BSN. Daarmee wordt de kans op fout kiezen geminimaliseerd, maar het betekent wel dat de zorgverlener eerst zelf (al dan niet met behulp van een lokale zoekfunctie) de patiënt moet identificeren.

- Ad eis [SPA-e02] De identificerende gegevens kunnen worden afgelezen van het WID, indien aanwezig, anders kan de patiënt/cliënt zelf worden bevroegd. Een BSN kan in de toekomst eventueel automatisch ingelezen worden, indien de patiënt/cliënt een geschikt vertrouwensmiddel (bijv. e-NIK) heeft en de zorgverlener/medewerker een geschikt leesapparaat.
- Ad eis [SPA-e02] In geval van een landelijk patiëntenregister, zoals de BVBSN, moet er voor een Nederlands ingezetene altijd één match zijn. Als er toch geen match is, zal vermoedelijk ergens een fout zijn opgetreden. De patiënt/cliënt of diens zorgaanbieder moet dan ergens deze fout kunnen melden. Zo heeft de SBV-Z een Servicedesk en een Foutenmeldpunt.
- Ad eis [SPA-e02] Er zijn slechts beperkte mogelijkheden om foutief gespelde namen te corrigeren. Zo kunnen bijv. ontbrekende diakrieten worden aangevuld en dubbele karakters worden verwijderd. Echter, het is niet mogelijk om na een mislukte match, met behulp van fonetische matching, een lijst met alternatieven te presenteren. Dit zou gemakzucht en onzorgvuldigheid in de hand kunnen werken.
- Ad eis [SPA-e03] De bron van het BSN kan zijn: de SBV-Z, de GBA, maar ook de CoV-functie van VeCoZo. Zorgaanbieders mogen de laatste bron raadplegen ten behoeve van hun declaratieverkeer. Voor het landelijk uitwisselen van medische patiëntgegevens moet tenminste de SBV-Z of de GBA zijn geraadpleegd.
- Ad eis [SPA-e04] Deze eis combineert de algemene vergewisplicht (zie Wabb artikel 12) met de eventueel verplichte WID-controles. Volgens Wbsn-z artikel 6 moet een zorgaanbieder de identiteit van een patiënt/cliënt vaststellen door controle van diens WID. Volgens Bbsn-z artikel 26 is dit niet verplicht voor een patiënt/cliënt die reeds was ingeschreven op het moment van inwerkingtreding van de Wbsn-z, maar de toelichting op dat artikel benadrukt dat de vergewisplicht onverkort geldt en dat WID-controle nodig kan zijn, tenzij de zorgaanbieder de patiënt/cliënt zeer goed kent. Voor de afweging wel/niet WID controleren wordt dus een grote verantwoordelijkheid bij de zorgaanbieder gelegd, daarom is het belangrijk dat een zorgaanbieder het resultaat van zijn controles voor alle patiënten/cliënten kan vastleggen.
- Ad eis [SPA-e06] Volgens de Wbsn-z toelichting op artikelen 5,6 en 7 moet een zorgaanbieder kunnen nagaan of een WID als ongeldig te boek staat. Daartoe biedt de SBV-Z een dienst om te kunnen controleren of een bepaald WID in omloop is, zie verder [Hbsn-z]. Een zorgaanbieder moet die dienst kunnen gebruiken. Merk op dat de beschreven controle geheel automatisch kan worden afgehandeld in combinatie met eis [SPA-e04].
- Ad eis [SPA-e01] Hoewel huisartsen hun patiënten/cliënten veelal kennen en dus minder behoefte hebben aan een compleet zoekpad conform [SBV-Z], kan het optimale zoekpad cruciaal blijken, bijv. om meerlingen uit elkaar te houden.
- Ad eis [SPA-e07] De waarschuwing moet duidelijk maken aan de zorgverlener dat vrijgave en aanmelding bij de verwijzindex niet kan plaatsvinden voor patiëntstukken

die nog niet inhoudelijk zijn gecontroleerd. Overigens is het aan de zorgverlener om te bepalen of hij alle detailgegevens samen met de patiënt moet langslopen, dan wel op basis van een snelle blik kan zien dat het klopt. Essentie van de waarschuwing is dat een systeem niet buiten de verantwoordelijke zorgverlener om, automatisch patiëntstukken gaat vrijgeven en aanmelden.

- Ad eis [SPA-e07] Grote zorgaanbieders, zoals ziekenhuizen, zullen per afdeling een afzonderlijk medisch dossier hebben, zie ook paragraaf 5.1. In dergelijke gevallen zal iedere afdeling deze controle afzonderlijk moeten uitvoeren en het resultaat daarvan per dossier moeten vastleggen. Deze controle is overigens niet noodzakelijk voor dossiers waarvan de inhoud nooit zal worden uitgewisseld met andere zorgaanbieders.
- Ad eis [SPA-e07] Een patiëntstuk kan een heel patiëntdossier of een apart document zijn, zie [Bedrijfsarchitectuur] paragraaf 6.3. Veelal zal een zorgaanbieder een geheel patiëntdossier in één keer inhoudelijk controleren en gekoppelen/ontkoppeld, maar de formulering laat de mogelijkheid open dat verschillende patiëntstukken afzonderlijk worden gecontroleerd en gekoppeld/ontkoppeld. Zie ook een van de opmerkingen bij eis [BIJ-e02].
- Ad eis [SPA-e09] De beschreven controle kan geheel automatisch worden afgehandeld in combinatie met eis [SPA-e01].
- Ad eis [SPA-e11] Wanneer de GBA deze faciliteit gaat bieden, zal er vermoedelijk een limiet komen aan de termijn waarop de zorgverlener wordt ingelicht. Voor een ziekenhuis heeft het geen zin om van alle patiënten/cliënten de adreswijzigingen bij te houden, voor een huisarts echter wel.
- Inloggen op vertrouwensniveau *laag* heeft niet alleen het voordeel dat de gebruiker geen UZI-pas nodig heeft, het biedt de applicatie tevens de mogelijkheid om 's nachts op basis van een behandelagenda het BSN van alle patiënten voor de volgende dag te verifiëren.

Voorbeeld van [SPA-e02] waarbij een zorginstellingmedewerker voor een patiënt/cliënt aan de balie een foutieve geboorteplaats intoetst:

Actie		
<opvragen>	<i>Patiëntnr (BSN)</i>	<i>Geslacht</i> [Vrouw]
	<i>Voornamen</i>	<i>Gemeente</i>
	<i>Voorletter</i> J	<i>Straatnaam</i>
	<i>Voorvoegsels</i>	<i>Huisnummer</i>
	<i>Geboortenaam</i> Jong	<i>Huisletter</i>
	<i>Geboortedatum</i> 11-11-1911	<i>Huisnr.toev.</i>
	<i>Geboorteplaats</i> Amsterdam	<i>Aanduid.huisnr.</i>
	<i>Geboorteland</i>	<i>Postcode</i>

Het resultaat na het aanklikken van <opvragen> zou er als volgt kunnen uitzien:

Actie				
<kiezen>	<i>Patiëntnr (BSN)</i>	1234567890	<i>Geslacht</i>	[Vrouw]
<overnemen>	<i>Voornamen</i>	Johanna	<i>Gemeente</i>	Rotterdam
<afsluiten>	<i>Voorletter</i>	J	<i>Straatnaam</i>	Amstelweg
	<i>Voorvoegsels</i>	de	<i>Huisnummer</i>	11
	<i>Geboortenaam</i>	Jong	<i>Huisletter</i>	A
	<i>Geboortedatum</i>	11-11-1911	<i>Huisnr.toev.</i>	
	<i>Geboorteplaats</i>	Amsterdam !	<i>Aanduid.huisnr.</i>	
	<i>Geboorteland</i>	Nederland	<i>Postcode</i>	1111 ZZ
<kiezen>	<i>BSN opgevraagd uit SBV-Z</i>			
<kiezen>	<i>WID nog NIET gecontroleerd met patiënt/cliënt !</i>			
<kiezen>	<i>WID nog NIET gecontroleerd op in omloop zijn !</i>			
<kiezen>	<i>Dossier nog NIET gecontroleerd met patiënt/cliënt</i>			
<kiezen>	<i>Dossier nog NIET geactualiseerd !</i>			

Bovenstaande tabellen zijn een bescheiden poging tot weergave van een dialoogschermbaarbij:

- <xxx> een knop voorstelt die geselecteerd kan worden (al dan niet door het aanklikken met de muis)
- [xxx] een veld voorstelt dat ingevuld kan worden (al dan niet door het aanklikken van de gewenste optie binnen een lijst van opties)



## 4.4 {toekomst} Selecteren zorgaanbieder (SZA)

Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 10.3 moeten zorgaanbieders elkaar elektronisch kunnen opzoeken, identificeren en bereiken.

Wanneer een zorgverlener zijn patiënt/cliënt wil doorverwijzen naar een zorgaanbieder van een bepaald type, met bepaalde zorgdiensten, in een bepaald specialisme, in een bepaalde regio, etc. moet hij vrij kunnen zoeken in een landelijke zorgaanbiedergids, op basis van verschillende zoekcriteria. Sommige patiënten/cliënten willen dit ook zelfstandig kunnen doen.

Wanneer een zorgverlener of zijn patiënt/cliënt eenmaal een zorgaanbieder heeft gekozen, moet hij diens actuele bereikbaarheidsgegevens kunnen opvragen uit deze zorgaanbiedergids. Belangrijk onderdeel daarvan is het adres van de zorgaanbiederpostbus, opdat aan deze zorgaanbieder een patiëntbericht kan worden toegestuurd. Ook belangrijk is te weten welke zorgtoepassingen en toepassingsrollen worden ondersteund, zie ook paragraaf 3.1. Omdat telefoonnummers, openingstijden, spreekuren, etc. veranderlijk zijn, moeten deze door de zorgaanbieders vrij kunnen worden bijgewerkt.

Architectuurbeslissingen:

**SZA·b01** Voor zorgaanbieders moeten de aangeboden zorgdiensten en de bereikbaarheidsgegevens door de zorgaanbieder zelf kunnen worden bijgewerkt en door andere zorgaanbieders worden opgevraagd.

Wanneer die andere zorgaanbieder een opdracht, bijv. een medicatievoorschrift of een verwijsbrief, krijgt van een onbekende zorgverlener, wil de ontvangende zorgverlener kunnen controleren wie de versturende zorgverlener is, welke functie hij heeft, voor wie hij werkt, etc. Hiervoor moet hij een zorgaanbiederregister kunnen raadplegen, waarvan de juistheid wordt gewaarborgd door een autoriteit.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**SZA·s01** opzoeken zorgaanbieder in de zorgaanbiedergids.

**SZA·s02** opvragen bereikbaarheidsgegevens uit de zorgaanbiedergids.

**SZA·s03** bijwerken bereikbaarheidsgegevens in de zorgaanbiedergids.

**SZA·s04** controleren zorgverlener in het zorgaanbiederregister.

Bij gebruiksscenario [SZA·s01] *opzoeken zorgaanbieder* gelden de volgende eisen en wensen:

**SZA·e01** De gebruiker moet vrij kunnen zoeken in de zorgaanbiedergids en daarbij per zorgaanbieder de onderstaande gegevens gepresenteerd krijgen:

- naam
- vestigingsplaats
- type zorgaanbieder
- eventueel lijst van afdelingen binnen deze zorgaanbieder

- eventueel lijst van zorgverleners binnen deze zorgaanbieder of afdeling
- per zorgverlener bovendien:
  - beroepstitel
  - specialisme(n)

**SZA·e02** De gebruiker moet na invoeren van één of meer van de onderstaande selectiecriteria, een lijst met alle matchende zorgaanbieders resp. zorgverleners gepresenteerd krijgen, waaruit de zorgverlener kan selecteren om alsnog (a) gepresenteerd te krijgen:

- {toekomst} zorgaanbieder-type
- {toekomst} beroepstitel (alleen voor zorgverleners)
- {toekomst} specialisme (alleen voor zorgverleners)
- naam
- vestigingsplaats of regio

Bij gebruiksscenario [SZA·s02] *opvragen bereikbaarheidsgegevens* gelden de volgende eisen en wensen:

**SZA·e03** De gebruiker moet voor een geselecteerde zorgaanbieder de volgende bereikbaarheidsgegevens gepresenteerd kunnen krijgen:

- bezoekadres
- fysiek postadres
- elektronisch postadres (Internet)
- elektronisch postadres (HL7v3)
- ondersteunde zorgtoepassingen en toepassingsrollen
- telefoonnummers
- {toekomst} beschikbare diensten per adres
- {toekomst} openingstijden per dienst per adres
- {toekomst} verwijzing naar een waarnemer

**SZA·e04** De gebruiker moet een elektronisch postadres door eenvoudig aanklikken kunnen overnemen als bestemming voor een te versturen patiëntbericht.

Bij gebruiksscenario [SZA·s03] *bijwerken bereikbaarheidsgegevens* gelden de volgende eisen:

**SZA·e05** {toekomst} De gebruiker moet na gebruiksscenario [SZA·s01] of [SZA·s02], de onder gebruiksscenario [SZA·s02] genoemde bereikbaarheidsgegevens kunnen bijwerken.

Bij gebruiksscenario [SZA·s04] *controleren zorgaanbieder* gelden de volgende eisen:

**SZA·e06** {toekomst} De gebruiker moet na gebruiksscenario [SZA·s01] of [SZA·s02], een zorgaanbieder kunnen selecteren en diens gegevens opvragen uit het zorgaanbiederregister.

Voor al deze gebruiksscenario's is het nodig dat de gebruiker heeft ingelogd als zorgverlener of medewerker op vertrouwensniveau *laag* of *midden*, zie gebruiksscenario [INL·s01].

Opmerkingen:

















- Ad eis [SZA-e01] Medewerkers staan niet in de zorgaanbiedergids, omdat zij geen formeel aanspreekpunt zijn van een zorgaanbieder.
- Ad eis [SZA-e03] Zorgverleners binnen een zorginstelling hebben vaak geen individuele bereikbaarheidsgegevens; zij kunnen daarom volstaan met de gezamenlijke bereikbaarheidsgegevens van hun afdeling gepubliceerd in de zorgaanbiedergids, zie ook [Bedrijfsarchitectuur] paragraaf 10.4.
- Ad eis [SZA-e03] Merk op dat een zorgaanbieder verschillende elektronische postbussen kan hebben, zie ook [Bedrijfsarchitectuur] paragraaf 8.3:
  - openbare internet: dit kan nuttig zijn voor ongestructureerde berichten van vrijblijvende afzenders (bijv. patiënten)
  - gesloten HL7v3: dit is noodzakelijk voor HL7v3-gestructureerde, dus elektronisch verwerkbare, berichten van authenticeerbare afzenders.
- Ad eis [SZA-e04] Ter voorkoming van fouten is het belangrijk dat een zorgverlener of medewerker geen ingewikkelde nummers en adressen hoeft over te tikken. Een gebruikersvriendelijke applicatie moet ervoor zorgen dat met name het UZI-nummer en het HL7v3-postadres "onder water" kunnen blijven. In dat geval hoeven deze attributen ook niet te worden getoond onder [SZA-e01] resp. [SZA-e03]. Wel is belangrijk om te tonen DAT de zorgaanbieder een HL7-adres heeft.
- Ad eis [SZA-e05] In principe kunnen alleen zorgverleners hun eigen bereikbaarheidsgegevens invullen en bijhouden, echter:
  - in geval van een zorginstelling kan dit worden voorbehouden aan een specifieke verantwoordelijke,
  - een HL7-postadres is een lange cijferreeks, die tijdens het invullen bij voorkeur wordt getoetst met een lijst van uitgegeven HL7-postadressen.
- Ad eis [SZA-e06] Het CIBG garandeert de juistheid van de gegevens in het UZI-register en is daarom geschikt als toetsingsregister. Verificaties van zorgaanbieders moeten handmatig op de website uitgevoerd worden, er is geen op HL7-berichten gebaseerde koppeling geïmplementeerd.
- Sommige gebruiksscenario's kunnen door een zorgaanbiederapplicatie ook gecombineerd worden. Het is aan de leveranciers van zorgtoepassingen om gebruikersvriendelijke dialoogschermen te ontwikkelen.
- Naast een gezamenlijke zorgaanbiedergids, kan een zorgverlener ook een eigen zorgaanbiederadresboek beheren, met daarin de zorgaanbieders waarmee deze zorgverlener bij voorkeur samenwerkt. De gebruiksscenario's voor het overnemen van bereikbaarheidsgegevens uit de zorgaanbiedergids, naar het eigen zorgaanbiederadresboek zijn hier niet uitgewerkt. Een dergelijk adresboek is een zaak voor de zorgaanbieder zelf. Het is aan de leveranciers van zorgtoepassingen om op een eventuele behoefte daaraan in te spelen.

#### Openstaande punten:

- Het CIBG zal een zorgaanbiedergids gaan leveren. Welke gegevens de eerste versie van deze zorgaanbiedergids precies gaat bevatten, hoe de autorisatie wordt geregeld, etc. is nog in onderzoek.

- Wanneer zorgverzekeraars straks zorgdiensten gaan inkopen bij bepaalde zorgaanbieders, zou het wenselijk zijn als het zoeken naar een zorgaanbieder in de regio kon worden gecombineerd met het toetsen of de zorgaanbieder wel vergoed kan worden door de zorgverzekeraar van de onderhavige patiënt/cliënt. De mogelijkheden hiertoe moeten worden onderzocht.

De onderstaande figuur geeft een voorbeeld van [SZA-e02] voor de plaats Amsterdam en [SZA-e03] voor een huisarts. De getoonde boomstructuur met in-/uitklapbare takken is slechts een mogelijke manier van presenteren. Overigens is een dergelijke hiërarchie met de huidige HL7-berichten nog niet op te vragen.

Zorgaanbieder (type)	Dienst	Adres	Openingstijd
 Amsterdam	Inloopspreekuur	Amstelweg 11	wrkdg 08:00-09:00
 Amstel, van (arts, huisartsgeneeskunde)	Spreekuur op afspraak	Amstelweg 11	wrkdg 10:00-13:00
 Amstelapotheek (apotheek)	Telefonisch spreekuur	020-1234567	wrkdg 10:00-13:00
 Gerritsen (apotheker)	Afspraken maken	020-1234568	wrkdg 08:00-09:00
 Amstelberg (arts, huisartsgeneeskunde)	Herhalingsrecepten	020-1234568	wrkdg 00:00-24:00
 Amstelpraktijk (huisartsenpraktijk)	Noodgevallen	0612-345678	wrkdg 00:00-24:00
 Amstelthuis (thuiszorginstelling)	Waarneming	AmstelPost	weekend
 Amstelkliniek (specialistisch ziekenhuis)	EMD-voorschrijver	HL7-adres	
 Oogheelkunde (afdeling)	WDH-dossierhouder	HL7-adres	
 Orthopedie (afdeling)	Vragen beantwoorden	H.Arts@Net.nl	
 Jansen (arts, orthopedie)			
 Pietersen (arts, orthopedie)			
 Willemsen (arts, orthopedie)			
 Plastische chirurgie (afdeling)			
 Amstelziekenhuis (algemeen ziekenhuis)			
 Amstelzorg (verzorgingstehuis)			

## 4.5 Bijhouden Patiëntgegevens (BIJ)

Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 7.3, moet een zorgverlener voor iedere patiënt/cliënt allerlei patiëntgegevens kunnen bijhouden in zijn dossier. Typische bewerkingen op patiëntgegevens zijn: aanmaken, inzien, wijzigen en verwijderen. Omdat medische patiëntstukken nooit mogen worden gewijzigd, komt het erop neer dat een zorgverlener een nieuwe versie van het achterhaalde patiëntstuk moet aanmaken en toevoegen aan het dossier.

Ook mogen medische patiëntstukken niet worden verwijderd, behalve na verstrijken van de bewaartermijn of op nadrukkelijk verzoek van een patiënt/cliënt. In het laatste geval is het wenselijk dat de verwijdering ongedaan gemaakt kan worden, als de patiënt/cliënt dat wenst. Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 11.3, zijn hiervoor vertrouwenswaarborgen nodig.

Wanneer een zorgverlener een patiëntstuk heeft vastgelegd in zijn dossier, maar later ontdekt dat het foutief is, kan hij dit patiëntstuk niet verwijderen, maar wel *herroepen* door het ongeldig te maken.

Tenslotte heeft een patiënt/cliënt recht op inzage, afschrift en aanvulling op zijn patiëntdossier, zie [Bedrijfsarchitectuur] paragraaf 9.1. Een patiënt/cliënt kan dat recht eventueel ook zonder de hulp van de zorgverlener uitoefenen. Deze functies worden in een latere versie van dit document uitgewerkt.

Architectuurbeslissingen:

**BIJ·b01** Zorgverleners moeten in staat gesteld worden patiëntgegevens vast te leggen, zowel *niet* gekoppeld, *voorlopig* gekoppeld als *definitief* gekoppeld aan een BSN, zie bijlage A.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**BIJ·s01** toevoegen patiëntgegevens aan het dossier,

**BIJ·s02** verwijderen patiëntgegevens uit het dossier.

Bij gebruiksscenario [BIJ·s01] *toevoegen patiëntgegevens* gelden de volgende eisen en wensen:

**BIJ·e01** De gebruiker moet patiëntstukken kunnen aanmaken, vastleggen, fiatteren, herroepen, waarbij voor een gemandateerde gebruiker wordt vastgelegd in een patiëntdossier namens welke inhoudsverantwoordelijke zorgverlener dit wordt gedaan.

**BIJ·e02** De gebruiker moet patiëntstukken kunnen aanmaken en toevoegen aan het patiëntdossier van een bepaalde patiënt/cliënt, waarbij:

- een patiëntstuk *voorlopig* wordt gekoppeld aan het BSN indien vooraf alleen gebruiksscenario [SPA·s01] *identificeren patiënt/cliënt* was doorlopen,
- een patiëntstuk *definitief* wordt gekoppeld aan het BSN indien vooraf ook gebruiksscenario [SPA·s02] *authenticeren patiënt/cliënt* was doorlopen,

- een patiëntstuk *definitief* wordt gekoppeld aan het BSN vermeld in een patiëntstuk ontvangen van een andere zorgaanbieder indien de inhoud van het aangemaakte patiëntstuk uitsluitend is gebaseerd op de inhoud van het patiëntstuk ontvangen van de andere zorgaanbieder,
- een patiëntstuk anders *niet* wordt gekoppeld aan het BSN.

**BIJ·e03** De gebruiker moet de zekerheid hebben dat patiëntstukken, na het vastleggen daarvan in een patiëntdossier, niet ongemerkt kunnen worden gewijzigd.

**BIJ·e04** {toekomst} De gebruiker moet onder zijn verantwoordelijkheid aangemaakte, vastgelegde en gefiatteerde patiëntstukken kunnen bekrachtigen door het zetten van een elektronische handtekening met behulp van zijn vertrouwensmiddel en deze toevoegen aan het patiëntdossier.

Bij gebruiksscenario [BIJ·s02] *verwijderen patiëntgegevens* gelden de volgende eisen en wensen:

**BIJ·e05** De gebruiker moet op verzoek van een patiënt/cliënt bepaalde patiëntstukken kunnen verwijderen, waarbij na keuze:

- {toekomst} de patiëntstukken worden versleuteld met behulp van het vertrouwensmiddel van de patiënt/cliënt,
- de patiëntstukken definitief en onherstelbaar worden uitgewist, inclusief de eventuele verwijzingen vanuit een toegangsllog voor zover die nog niet gearchiveerd zijn.

Voor al deze gebruiksscenario's is het nodig dat de gebruiker heeft ingelogd als zorgverlener of gemandateerde medewerker op vertrouwensniveau *midden*, zie gebruiksscenario [INL·s01].

Opmerkingen:

- Ogenschijnlijk is het bijhouden van patiëntgegevens in een dossier slechts een interne aangelegenheid voor de verantwoordelijke zorgverlener. Maar wanneer deze patiëntgegevens vervolgens voor landelijke uitwisseling in aanmerking komen, is het noodzakelijk eisen te stellen aan de manier waarop zorgverleners hun dossier bijhouden. De bovenstaande eisen gelden dus voor de patiëntgegevens die in het kader van een bepaalde landelijke zorgtoepassing kunnen worden uitgewisseld.
- Ad eis [BIJ·e02] Als gevolg van architectuurbeslissing [BIJ·b01] zijn verschillende mates van koppeling aan het BSN mogelijk, afhankelijk van de uitgevoerde BSN-verificatie en WID-controle. Ook voor patiënten/cliënten zonder BSN (nieuw-ingezetenen, pasgeborenen, etc.) moeten patiëntgegevens kunnen worden vastgelegd, zonder enige koppeling aan een BSN. Nadat de patiënt alsnog een BSN is toegekend, moeten die gegevens alsnog *voorlopig* respectievelijk *definitief* worden gekoppeld, zie paragraaf 4.3.
- Ad eis [BIJ·e02] Als een zorgverlener een nieuw patiëntstuk aanmaakt uitsluitend op basis van de inhoud van een ander patiëntstuk ontvangen van een andere zorgaanbieder, mag die zorgverlener het nieuwe patiëntstuk *definitief* koppelen aan het BSN uit dat andere patiëntstuk. Zo mag een apotheker een medicatieverstrekking *definitief* koppelen aan een BSN zoals vermeld in een medicatievoorschrift ontvangen van een arts, zonder nadere BSN-verificatie of WID-controle. Dit is in overeenstemming met Bbsn-z artikel 25.

- Ad eis [BIJ-e02] Een patiëntstuk kan verschillende aggregatieniveaus hebben, zie [Bedrijfsarchitectuur] paragraaf 6.3. In geval van een eerstelijnsdossier is het wellicht niet mogelijk om daarbinnen verschillende patiëntstukken afzonderlijk te koppelen aan een BSN. In dat geval geldt het gehele dossier als patiëntstuk en wordt het gehele dossier *niet* gekoppeld, *voorlopig* gekoppeld of *definitief* gekoppeld. Dit betekent dat bijv. een huisarts bij het eerste bezoek van een reeds ingeschreven patiënt na de inwerkingtreding van de Wbsn-z, bijv. en nieuw medicatievoorschrift kan toevoegen aan dat dossier, maar eerst alle oude patiëntgegevens inhoudelijk moet controleren met de patiënt, alvorens het medicatievoorschrift beschikbaar kan worden gemaakt voor landelijke opvraag.
- Ad eis [BIJ-e04] NICTIZ zal nader uitzoeken welke patiëntstukken en welke onderdelen daarvan precies in aanmerking komen voor ondertekening.
- Ad eis [BIJ-e05] Het verwijderen van verwijzingen naar patiëntstukken uit een toegangslog is moeilijk realiseerbaar wanneer deze is gearhiveerd op een off-line medium.

## 4.6 Publiceren Patiëntgegevens (PUB)

Wanneer een zorgverlener allerlei patiëntstukken toevoegt aan zijn dossier, kan hij besluiten deze patiëntstukken te publiceren, opdat deze beschikbaar komen voor landelijke opvraag door andere zorgverleners. Ook in latere instantie kan hij besluiten bepaalde patiëntstukken alsnog vrij te geven, dan wel weer af te schermen. Wanneer een zorgverlener allerlei patiëntstukken verwijdert uit zijn dossier, zijn deze uiteraard niet langer beschikbaar voor opvraag.

*Vrijgeven* van een patiëntstuk betekent ook dat het moet worden aangemeld bij de verwijsindex. Anders blijft voor andere zorgverleners onbekend dat de zorgverlener patiëntstukken beschikbaar heeft gesteld voor opvraag. Dit aanmelden kan op twee verschillende manieren:

- *atomair*: hierbij wordt ieder patiëntstuk afzonderlijk aangemeld en krijgt ieder patiëntstuk een eigen verwijzing in de verwijsindex. Dit is nuttig voor omvangrijke patiëntstukken (bijv. CT-scans) of patiëntdocumenten (bijv. ontslagbrief) die gewoonlijk afzonderlijk worden opgevraagd.
- *categoraal*: hierbij wordt een categorie van patiëntstukken (gegevenssoort) aangemeld en krijgen alle patiëntstukken één gezamenlijke verwijzing in de verwijsindex. Dit is nuttig voor patiëntstukken (bijv. medicatievoorschriften) die gewoonlijk groepsgewijs worden opgevraagd.

Per landelijke zorgtoepassing (EMD, WDH, etc.) wordt bepaald op welke manier moet worden aangemeld. In geval van categoriaal aanmelden, wordt de categorie in principe eenmalig aangemeld. Als vervolgens meer patiëntstukken van dezelfde categorie worden vrijgegeven, hoeft de categorie niet opnieuw te worden aangemeld. Wel kan het nodig zijn de actualiteit van de categorie bij te werken, zie paragraaf 5.3. Dit wordt heraanmelden genoemd. Heraanmelden kan ook nodig zijn om andere attributen in de verwijzing bij te werken, zie bijlage C.

*Afschermen* van een patiëntstuk kan betekenen dat het weer moet worden afgemeld bij de verwijsindex. Atomair aangemelde patiëntstukken moeten altijd afzonderlijk worden afgemeld. Een categorie wordt alleen afgemeld als er verder geen vrijgegeven patiëntstukken van die categorie meer zijn.

In principe moet een zorgverlener alle patiëntstukken vrijgeven van de gegevenssoorten behorende bij de landelijke zorgtoepassing waaraan de zorgaanbieder meedoet. Alleen met goede redenen kan een zorgverlener besluiten om bepaalde patiëntstukken, of zelfs alle patiëntstukken van een bepaalde gegevenssoort of een bepaalde episode, niet vrij te geven. Bijv. een patiënt/cliënt wenst dat zijn huisarts het medicatievoorschrift voor een antidepressivum afschermt, waarop de huisarts besluit alle medicatievoorschriften af te schermen, om de schijn van volledigheid te vermijden. Zie ook [Bedrijfsarchitectuur] paragraaf 9.2 opmerking bij (f).

Hoewel *aanmelden*, *heraanmelden* en *afmelden* in principe automatisch plaatsvindt na het vrijgeven of afschermen van bepaalde patiëntstukken, kan de zorgverlener een categorie *aanmelden* zonder dat patiëntstukken van die categorie zijn vrijgegeven. Bijvoorbeeld als een zorgverlener die patiëntstukken niet geschikt voor publicatie acht, of



die patiëntstukken alleen op papier heeft, maar kenbaar wil maken dat hij gebeld kan worden over deze categorie.

Een bijzonder geval is het aanmelden van een heel *patiëntdossier*. Zo kan een *eerstelijnsdossier* eenmalig categoriaal worden aangemeld, terwijl het dossier vele, verschillende patiëntstukken bevat, die afzonderlijk maar ook tezamen (in de vorm van een professionele samenvatting) kunnen worden vrijgegeven en afgeschermd.

Per landelijke zorgtoepassing (EMD, WDH, etc.) moet worden voorgeschreven op welke aggregatieniveaus de betrokken patiëntgegevens door zorgaanbieders moeten worden aan/afgemeld resp. vrijgegeven/afgeschermd.

*Afschermen* staat in principe los van het *autorisatieprofiel*. Het autorisatieprofiel is bedoeld om specifieke zorgverleners uit te sluiten van landelijke uitwisseling van patiëntgegevens. Afschermen is bedoeld om specifieke patiëntstukken uit te sluiten, zonder aanzien des persoons en ongeacht of de noodknop wordt gebruikt.

Architectuurbeslissingen:

**PUB·b01** Als gevolg van architectuurbeslissing [bat·b03] moet een zorgverlener in principe de patiëntstukken van alle gegevenssoorten vermeld in het autorisatieprotocol vrijgeven en aanmelden, *ongeacht* het autorisatieprofiel van de desbetreffende patiënt/cliënt.

**PUB·b02** Zorgverleners mogen *alleen* in staat gesteld worden landelijk patiëntgegevens aan te melden bij de verwijsindex, wanneer deze *definitief* zijn gekoppeld aan een BSN, zie bijlage A.

**PUB·b03** Als gevolg van architectuurbeslissing [VWI·b05] moet een zorgverlener op verzoek van een patiënt/cliënt alle vrijgegeven patiëntgegevens opnieuw kunnen aanmelden bij de verwijsindex, nadat de patiënt/cliënt na aanvankelijk bezwaar alsnog akkoord gaat met landelijke uitwisseling van zijn patiëntgegevens, zie bijlage C.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**PUB·s01** vrijgeven patiëntgegevens en aanmelden bij de verwijsindex,

**PUB·s02** afschermen patiëntgegevens en afmelden bij de verwijsindex.

**PUB·s03** patiëntgegevens opnieuw aanmelden bij de verwijsindex.

Bij gebruiksscenario [PUB·s01] *vrijgeven patiëntgegevens* gelden de volgende eisen en wensen:

**PUB·e01** De gebruiker moet kunnen instellen welke gegevenssoorten van patiëntstukken na toevoegen aan zijn dossier automatisch, dan wel op commando per patiëntstuk (zie paragraaf 4.5), worden vrijgegeven.

**PUB·e02** De gebruiker moet na het vastleggen van patiëntstukken in zijn dossier, deze automatisch of op commando per patiëntstuk kunnen vrijgeven.

**PUB·e03** De gebruiker moet naderhand individuele patiëntstukken in zijn dossier alsnog kunnen vrijgeven.

**PUB·e04** Bij het vrijgeven van een patiëntstuk moet de gebruiker erop kunnen vertrouwen dat:

- hij wordt gewaarschuwd indien het patiëntstuk ooit als kopie van een andere zorgverlener is ontvangen,
- ofwel het patiëntstuk atomair wordt aangemeld bij de verwijsindex,
- ofwel de categorie van het patiëntstuk wordt aangemeld bij de verwijsindex, indien dat nog niet was gedaan,
- ofwel de categorie van het patiëntstuk wordt heraangemeld bij de verwijsindex door het bijwerken van de actualiteit, indien de vorige (her-)aanmelding meer dan een bepaald tijdsinterval geleden is, zoals voorgeschreven per landelijke zorgtoepassing.
- **PUB·e05** De gebruiker moet na het definitief koppelen (zie gebruiksscenario [SPA-3]) van patiëntstukken aan een landelijk patiëntnummer, die patiëntstukken in één keer kunnen vrijgeven en aanmelden, waarbij de gebruiker vooraf per gegevenssoort kan aangeven tot hoever terug in het verleden naar relevante patiëntstukken moet worden gezocht.

**PUB·e06** { toekomst } De gebruiker moet een gegevenssoort kunnen aanmelden zonder dat patiëntstukken van die gegevenssoort zijn vrijgegeven.

Bij gebruiksscenario [PUB·s02] *afschermen patiëntgegevens* gelden de volgende eisen en wensen:

**PUB·e07** De gebruiker moet vrijgegeven patiëntstukken naderhand weer kunnen afschermen en wel op de volgende aggregatieniveaus:

- patiëntdossier,
  - patiëntdocument,
  - patiëntgegevensbijdrage,
  - patiëntgegevenselement
- waarbij de vereiste niveaus afhankelijk zijn van de zorgtoepassing.

**PUB·e08** De gebruiker moet in de volgende gevallen patiëntstukken in zijn dossier automatisch kunnen laten afschermen:

- bij het herroepen van patiëntstukken,
- bij het overdragen van patiëntstukken aan een andere zorgaanbieder.

**PUB·e09** Bij het afschermen of verwijderen van een patiëntstuk moet de gebruiker erop kunnen vertrouwen dat:

- het patiëntstuk niet meer beschikbaar is voor opvraag, ook niet in noodsituaties,
- indien het ooit atomair was aangemeld, het patiëntstuk nu wordt afgemeld,
- indien er voor de onderhavige patiënt/cliënt verder géén vrijgegeven patiëntstukken meer zijn van deze categorie, de categorie van het patiëntstuk wordt afgemeld bij de verwijsindex, waarbij de gebruiker vooraf om bevestiging wordt gevraagd,
- indien dit vrijgegeven patiëntstuk het meest actuele van die categorie was, de categorie wordt heraangemeld bij de verwijsindex, met de actualiteit van het meest actuele nog vrijgegeven patiëntstuk met deze gegevenssoort,

zoals voorgeschreven per landelijke zorgtoepassing.

Bij gebruiksscenario [PUB·s03] *opnieuw aanmelden patiëntgegevens* gelden de volgende eisen en wensen:

**PUB·e10** De gebruiker moet voor een bepaalde patiënt/cliënt alle vrijgegeven patiëntgegevens opnieuw kunnen aanmelden bij de verwijsindex.

Voor alle gebruiksscenario's geldt:

**PUB·e11** De gebruiker moet na een mislukte aanmelding, heraanmelding of afmelding als gevolg van een onbereikbare verwijsindex, in staat worden gesteld:

- de aanmeldingen, heraanmeldingen en afmeldingen automatisch laten bewaren voor latere afhandeling,
- bij de eerstvolgende keer inloggen alle klaarstaande aanmeldingen, heraanmeldingen en afmeldingen alsnog automatisch laten afhandelen,
- worden geïnformeerd of alles met succes is afgehandeld.

**PUB·e12** AORTA moet mogelijk maken dat een zorgaanbieder desgewenst kan beperken dat een verwijzing aangemeld onder beheerverantwoordelijkheid van de ene zorgverlener wordt heraangemeld of afgemeld onder beheerverantwoordelijkheid van andere zorgverleners.

Voor al deze gebruiksscenario's is het nodig dat de gebruiker heeft ingelogd als zorgverlener of gemandateerde medewerker op vertrouwensniveau *midden*, zie gebruiksscenario [INL·s01].

Opmerkingen:

- Ad eis [PUB·e01] in principe moet een zorgverlener de patiëntstukken van alle gegevenssoorten vermeld in het autorisatieprotocol vrijgeven. Toch kan een zorgverlener bijzondere redenen hebben om bepaalde patiëntstukken, of zelfs alle patiëntstukken van een bepaalde gegevenssoort of een bepaalde episode, niet vrij te geven, bijvoorbeeld op uitdrukkelijk verzoek van de patiënt/cliënt.
- Ad eis [PUB·e04] in principe mag alleen de zorgverlener die verantwoordelijk is voor een patiëntstuk deze aanmelden. Anderen die ooit een kopie hebben ontvangen, mogen dit patiëntstuk niet opnieuw of alsnog aanmelden, tenzij daar bijzondere redenen voor zijn, zie ook paragraaf 4.11.
- Ad eis [PUB·e04] en [PUB·e07] en [PUB·e12] in het dossier moet dus worden bijgehouden in hoeverre de vrijgegeven patiëntstukken zijn aangemeld aan de verwijsindex, zie bijlage C.2. Wanneer blijkt dat alle verwijzingen voor die patiënt/cliënt zijn gewist uit de verwijsindex, als gevolg van bezwaar van de patiënt/cliënt tegen landelijke uitwisseling van zijn patiëntgegevens, moet dat ook worden bijgehouden, om foutieve heraanmeldingen te voorkomen, zie bijlage C.7.
- Ad eis [PUB·e05] Als gevolg van architectuurbeslissing [PUB·b02] worden alleen *definitief* gekoppelde patiëntstukken landelijk uitgewisseld. Volgens Bbsn-z artikel 27 is het onder voorwaarden toegestaan om *niet* gekoppelde patiëntstukken zonder BSN uit te wisselen, maar AORTA kan dat niet ondersteunen. Volgens Bbsn-z artikel 28 is het onder voorwaarden ook toegestaan om *voorlopig* gekoppelde gegevens met onzeker BSN uit te wisselen, maar AORTA ondersteunt dat niet, zie bijlage A.

- Ad eis [PUB·e05] voor patiënten/cliënten zonder BSN (nieuw-ingezetenen, pasgeborenen, etc.) kunnen de patiëntgegevens pas later worden aangemeld nadat alsnog een BSN is toegekend. Daarvoor moeten de patiëntgegevens alsnog definitief worden gekoppeld, zie ook paragraaf 4.3.
- Ad eis [PUB·e06] dit kan belangrijk zijn als een zorgverlener bepaalde patiëntstukken niet elektronisch heeft, maar deze toch wil aanmelden bijv. om andere zorgaanbieders te laten weten dat hij daarover gebeld kan worden.
- Ad eis [PUB·e07] deze aggregatieniveaus komen voort uit [Bedrijfsarchitectuur] paragraaf 6.3. Een medicatieregeling is te beschouwen als een patiëntgegevens-element, de professionele samenvatting van een huisarts is te beschouwen als een patiëntdocument. Zoals uitgelegd in [Bedrijfsarchitectuur] paragraaf 8.2, opmerking bij (b), hangt het laagste niveau af van het belang van de context waarin die patiëntgegevens beschouwd moeten worden. Dit kan verschillen per zorgtoepassing en gegevenssoort. Zo is het momenteel niet mogelijk binnen een professionele samenvatting bepaalde gegevens af te schermen.
- Ad eis [PUB·e08] herroepen speelt wanneer een zorgverlener een patiëntstuk heeft vastgelegd in zijn dossier, maar later ontdekt dat het foutief is. Dan kan hij dit patiëntstuk niet verwijderen, maar wel *herroepen* door het ongeldig te maken. *Overdragen* speelt bijv. wanneer een huisarts het waarneemverslag van een HAP voor één van zijn patiënten overneemt in zijn dossier, zie verder paragraaf 4.11.
- Ad eis [PUB·e09] het categoriaal *afmelden* van een gegevenssoort zal in de praktijk niet zo vaak plaatsvinden. Na het afschermen of verwijderen van één patiëntstuk zullen vaak nog andere patiëntstukken van dezelfde gegevenssoort overblijven, zodat de aanmelding gehandhaafd moet worden. Wel kan *heraanmelden* nodig zijn de actualiteit te wijzigen.
- Ad eis [PUB·e10] dit is nodig voor een patiënt/cliënt die na aanvankelijk bezwaar alsnog akkoord gaat met landelijke uitwisseling van zijn patiëntgegevens, zie bijlage C. De patiënt/cliënt kan de zorgverlener hiertoe expliciet verzoeken, maar het akkoord kan ook impliciet blijken uit een succesvolle poging tot opvraag van patiëntgegevens. Synchronisatie kan ook nuttig zijn als een applicatie of de verwijfsindex lange tijd niet beschikbaar is geweest.
- Ad eis [PUB·e11] de applicatie moet de gebufferde aanmeldingen en afmeldingen alsnog verzenden zodra de verantwoordelijke zorgverlener weer inlogt. Het is dus niet mogelijk dat de applicatie deze in afwezigheid van de zorgverlener verzendt zodra de verwijfsindex weer bereikbaar is. De applicatie kan dit allemaal automatisch afhandelen, maar de zorgverlener moet wel worden geïnformeerd.
- Ad eis [PUB·e11] de applicatie moet onthouden dat als gevolg van het bezwaar van de patiënt/cliënt tegen landelijke uitwisseling van zijn patiëntgegevens, alle verwijfsindexen voor die patiënt/cliënt zijn gewist uit de verwijfsindex, zie bijlage C. De applicatie kan dan vervolgens stoppen met het bijhouden van de verwijfsindex totdat blijkt dat de patiënt alsnog weer akkoord is gegaan.
- Ad eis [PUB·e12] als een ziekenhuis wil voorkomen dat zorgverleners van verschillende afdelingen elkaars verwijfsindexen gaan veranderen, moet dat kunnen worden beperkt, zie bijlage C.

## 4.7 { toekomst} Abonneren Patiëntgegevens (ABO)

Wanneer een zorgverlener interesse heeft in patiëntgegevens die nu nog niet beschikbaar zijn, bijv. een labuitslag, wil hij misschien gewaarschuwd worden wanneer deze wél beschikbaar komen.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**ABO·s01** aanmelden abonnement bij de verwijfsindex,

**ABO·s02** afmelden abonnement bij de verwijfsindex.

Hierbij gelden de volgende eisen:

**ABO·e01** { toekomst} De gebruiker moet kunnen instellen of hij éénmalig of voortdurend op de hoogte gehouden wil worden van het beschikbaar komen van bepaalde gegevenssoorten van patiëntgegevens.

**ABO·e02** { toekomst} De gebruiker moet, nadat hij een melding heeft ontvangen van het beschikbaar komen van de gewenste patiëntgegevens, door eenvoudig aanklikken de gewenste patiëntgegevens kunnen opvragen.

Voor al deze gebruiksscenario's is het nodig dat de gebruiker heeft ingelogd als zorgverlener of medewerker op vertrouwensniveau *midden*, zie gebruiksscenario [INL·s01].

Deze gebruiksscenario's zullen in een latere versie van dit document worden uitgewerkt. Daarbij wordt uitgezocht of dit mechanisme bijv. kan worden gebruikt om op de hoogte te worden gebracht van adreswijzigingen in de GBA.

## 4.8 Initieel koppelen Patiëntgegevens (IKO)

Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 10.2, moet een zorgverlener bij de invoering van het landelijke patiëntnummer (BSN) zijn patiëntdossier's opschonen door alle patiëntgegevens te koppelen aan het juiste BSN. Dat is geen sinecure want:

- elke ingeschreven patiënt/cliënt moet worden gematcht aan de hand van actuele identificerende patiëntgegevens (NAW, geboortedatum, etc.), terwijl de aanwezige attributen in het patiëntdossier misschien verouderd zijn.
- het komt voor dat de gegevens van één patiënt/cliënt abusievelijk zijn opgeborgen in het patiëntdossier achter twee patiëntidentiteiten. Het omgekeerde komt ook voor.
- sommige zorgaanbieders hebben miljoenen patiënten in hun bestand. Het zal erg veel inspanning kosten om al die gegevens op te schonen, terwijl veel gegevens nooit meer opgevraagd zullen worden. Daarom willen zorgaanbieders wellicht ervoor kiezen om eerst een deel van hun patiënten/cliënten te koppelen en later misschien de rest.
- hoewel een zorgverlener zich kan laten assisteren door medewerkers, blijft hij te allen tijde zelf verantwoordelijk voor de correctheid van de patiëntdossiers, dus ook voor de koppeling van patiëntgegevens aan het juiste BSN.
- uiteindelijk moet iedere koppeling van oude patiëntgegevens aan een BSN in principe worden gecontroleerd op fouten als gevolg van mogelijke verwisseling van patiëntidentiteit in het verleden. Zonodig moet de zorgverlener het gehele patiëntdossier doornemen in aanwezigheid van de patiënt/cliënt. Het is ondoenlijk om patiënten/cliënten hiervoor op te roepen, daarom moet dit kunnen wachten tot het eerstvolgende moment dat de patiënt/cliënt toch al op spreekuur komt of anderszins contact opneemt.

Architectuurbeslissingen:

**IKO-b01** Het koppelen van patiëntgegevens aan het juiste BSN, moet kunnen worden uitgevoerd in twee stappen:

- een *voorlopige* koppeling: een bulkproces dat t.b.v. doelmatigheid deels geautomatiseerd en deels door medewerkers van de zorgaanbieder kan worden uitgevoerd,
- een *definitieve* koppeling: een proces dat t.b.v. zorgvuldigheid zonodig handmatig door de verantwoordelijke zorgverlener moet worden uitgevoerd.

**IKO-b02** Met veronderstelde toestemming kunnen alleen *definitief* gekoppelde patiëntgegevens worden aangemeld bij de verwijzindex om beschikbaar te komen voor opvraag door andere zorgverleners.

Het aanmelden bij de verwijzindex zonder expliciete toestemming van de patiënt/cliënt is mogelijk, zie [Bedrijfsarchitectuur] paragraaf 9.2. Dit heeft het grote voordeel dat in een vroeg stadium na de start van het landelijk schakelpunt reeds patiëntgegevens kunnen worden opgevraagd. Anders gaat het jaren duren voordat de verwijzindex enigszins gevuld is.

Anderzijds is het hebben opgeschoond van patiëntdossiers en het aanmelden van patiëntgegevens een voorwaarde voor aansluiting van de zorgaanbieder op het landelijk schakelpunt. Het aanmelden van patiëntgegevens zou een voorwaarde kunnen worden voor het mogen opvragen van patiëntgegevens van andere zorgaanbieders.

Het achteraf koppelen van patiëntgegevens kan echter niet garanderen dat die gegevens inderdaad betrekking hebben op de aangegeven patiënt/cliënt. Bijvoorbeeld, patiëntgegevens die ooit zijn ingevoerd onder een valse identiteit van een patiënt/cliënt, worden keurig gekoppeld aan het BSN behorende bij die valse identiteit. Wanneer de echte patiënt/cliënt met zijn WID verschijnt, komt dat niet aan het licht. Alleen als de zorgverlener ter verificatie de gekoppelde patiëntgegevens inhoudelijk met hem doorneemt, zou dit aan het licht kunnen komen.

Daarom moeten zorgverleners voor iedere initieel gekoppelde patiënt/cliënt zo spoedig mogelijk de extra controles rond de invoering van het BSN uitvoeren, bijv. bij het eerste contact na de initiële koppeling, zie bijlage A, paragraaf 4. Het is echter mogelijk dat een zorgaanbieder heel zeker is over de identiteit van al zijn patiënten en de juistheid van hun patiëntdossiers. In dat geval kunnen de extra controles genoemd in paragraaf 4.3 achterwege blijven.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**IKO-s01** voorlopig koppelen patiëntgegevens aan landelijk patiëntnummer,

**IKO-s02** definitief koppelen patiëntgegevens aan landelijk patiëntnummer.

Bij gebruiksscenario [IKO-s01] *voorlopig koppelen* gelden de volgende eisen en wensen:

**IKO-e01** De gebruiker moet van de patiënten/cliënten in de eigen patiëntenindex of alle patiëntdossier's het interne patiëntnummer en andere identificerende gegevens, kunnen verzamelen, waarbij hij kan kiezen voor:

- alleen de *actieve* patiënten/cliënten,
- *alle* ingeschreven patiënten/cliënten,
- alleen de patiënten/cliënten die patiëntgegevens van bepaalde gegevenssoorten van na een bepaalde datum in het dossier hebben.

**IKO-e02** De gebruiker moet de verzameling identificerende gegevens kunnen opsturen naar het landelijke patiëntenregister (BVBSN via SBV-Z).

**IKO-e03** De gebruiker moet de verzameling identificerende gegevens verrijkt met koppelresultaten kunnen ontvangen van het landelijke patiëntenregister (BVBSN via SBV-Z).

**IKO-e04** De gebruiker moet van de ontvangen koppelresultaten de toegevoegde BSN's met de eventueel aanvullende attributen in één keer kunnen overnemen naar de eigen patiëntenindex of patiëntdossier's, waarbij automatisch wordt vastgelegd:

- de bron van het BSN (landelijk patiëntenregister),
- datum en tijd van koppelen,
- zorgverlener-id of andere identificatie van de gebruiker.

**IKO-e05** De gebruiker moet de onderstaande situaties handmatig kunnen langslopen, zonodig corrigeren en/of zonodig ontkoppelen van het BSN:

- patiënten voor wie uitzonderingen waren gevonden, zoals gedefinieerd in [Hbsn-z] bijlage 1,
- patiënten met verschillende interne patiëntnummers die aan éénzelfde BSN waren gekoppeld,
- patiënten voor wie het eventueel aanwezige BSN onjuist blijkt te zijn,
- patiënten die helemaal niet gekoppeld konden worden.

Bij gebruiksscenario [IKO·s02] *definitief koppelen* gelden dezelfde eisen en wensen als voor de gebruiksscenario onder [SPA] *selecteren patiënt/cliënt*.

Voor al deze gebruiksscenario's is het nodig dat de gebruiker lokaal heeft ingelogd als zorgverlener of medewerker op vertrouwensniveau *laag* of *midden*, zie gebruiksscenario [INL·s01].

Opmerkingen:

- Ad gebruiksscenario [IKO·s01] De uitwisseling van identificerende gegevens met de SBV-Z kan zowel bestandsgewijs als met berichten (web services) plaatsvinden. In dit gebruiksscenario gaat het erom dat een grote groep patiënten wordt geselecteerd waarvoor het opvragen van het BSN groepsgewijs wordt afgehandeld.
- Ad eis [IKO·e01] In principe moeten alle patiëntgegevens worden gekoppeld, maar het kan verstandig zijn voorrang te geven aan *actieve* patiënten/cliënten. In geval van een ziekenhuis zijn dit de *onder behandeling zijnde* patiënten. In geval van een huisarts zijn dit de *nog niet uitgeschreven* patiënten. Een zorgaanbieder kan ook besluiten eerst alleen de patiënten/cliënten te koppelen voor wie in het afgelopen halfjaar bijv. medicatiegegevens zijn vastgelegd.
- Ad eis [IKO·e01] In geval van een ziekenhuis heeft men de keuze om alleen de centrale patiëntnummers in het ZIS of de MPI te koppelen, dan wel alle ZIS, ZAIS, RIS, LIS, etc. afzonderlijk te koppelen.
- Ad eis [IKO·e04] In geval van een ziekenhuis waar het ZAIS, RIS, LIS, etc. een eigen patiëntnummer voeren, kan men ervoor kiezen de koppeling met het BSN vanuit het ZIS te propageren naar die systemen, opdat de definitieve koppeling aldaar afzonderlijk kan worden gedaan.
- Ad eis [IKO·e04] Merk op dat het interne patiëntnummer niet wordt *vervangen door* maar *aangevuld met* het BSN, opdat een abusievelijk gemaakte koppeling eventueel weer ongedaan kan worden gemaakt.
- Ad eis [IKO·e05] Waar nodig en zinvol kunnen attributen handmatig worden gecorrigeerd of aangevuld, eventueel na raadpleging van andere dossiers en/of contact met de desbetreffende patiënten. Desnoods wordt een voorlopige koppeling weer ongedaan gemaakt. Na afloop kan voor deze groep patiënten het proces van voorlopige koppeling worden herhaald.
- Let op de analogie tussen gebruiksscenario [IKO] *initieel koppelen* en gebruiksscenario [SPA] *selecteren patiënt/cliënt*. Deelscenario [IKO·s01] is vergelijkbaar met deelscenario [SPA·s01], maar dan voor een grote verzameling patiënten/cliënten, die bovendien niet aanwezig zijn. Deelscenario [IKO·s02] is in principe gelijk aan deelscenario [SPA·s02] en verder, maar zal in de praktijk toch beginnen met deelscenario [SPA·s01].



## 4.9 Opvragen Patiëntgegevens (OPV)

Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 8.2, moet een zorgverlener patiëntgegevens kunnen opvragen. Voor sommige zorgvragen weet een zorgverlener precies welke patiëntgegevens hij nodig heeft om zijn patiënt/cliënt te helpen. Hij kan aldus een gerichte opvraag formuleren die precies de benodigde gegevens oplevert. Voor sommige andere zorgvragen weet de zorgverlener niet direct welke opvraag hij moet formuleren. Hij heeft dan baat bij een *overzicht* van beschikbare gegevenssoorten zoals vermeld in de verwijzindex.

Voorbeeld is een huisarts die wegens een vage klacht van een patiënt/cliënt eerst eens wil kijken wat er allemaal bekend is over deze patiënt. De opvraag zou er als volgt kunnen uitzien, aangenomen dat de huisarts in 2003 alle feiten sinds het jaar 1993 wil zien:

<i>Actie</i>				
<kiezen>	<i>Patiëntnr (BSN)</i>	1234567890	<i>Geboortedatum</i>	11-11-1911
<index>	<i>Geboortenaam</i>	Jong	<i>Geboorteplaats</i>	Amsterdam
...	...	...	...	...
<i>Plaats</i>	<i>Zorgaanb.naam</i>	<i>Zorgaanb.functie</i>	<i>Gegevens.soort</i>	<i>Actualiteit</i>
[alle]	[alle]	[alle]	[alle]	[1993]

Het resultaat na het aanklikken van <index> zou er als volgt kunnen uitzien:

<i>Actie</i>				
<kiezen>	<i>Patiëntnr (BSN)</i>	1234567890	<i>Geboortedatum</i>	11-11-1911
<opvragen>	<i>Geboortenaam</i>	Jong	<i>Geboorteplaats</i>	Amsterdam
...	...	...	...	...
<i>Plaats</i>	<i>Zorgaanb.naam</i>	<i>Zorgaanb.functie</i>	<i>Gegevens.soort</i>	<i>Actualiteit</i>
Amsterdam	Amstelapotheek	apotheker	medic.verstrek.	2003
Amsterdam	IJ-apotheek	apotheker	medic.verstrek.	2003
Amstelveen	Veenapotheek	apotheker	medic.verstrek.	2003
Rotterdam	Maasapotheek	apotheker	medic.verstrek.	2002
Schiedam	Schieapotheek	apotheker	medic.verstrek.	1999
Amsterdam	Jansen	arts, huisarts	1 <sup>e</sup> lijnsdossier	2003
Amsterdam	Jansen	arts, huisarts	medic.voorsch.	2003
Amsterdam	Jansen	arts, huisarts	kcl-labaanvr.	2002
Rotterdam	Pietersen	arts, huisarts	1 <sup>e</sup> lijns dossier	1999
Rotterdam	Pietersen	arts, huisarts	verwijsbrief	1999
Schiedam	Jacobsen	arts, huisarts		1993
Amsterdam	Amstelziekenhuis	arts, inwendige	diagnose	2002
Amsterdam	Amstelziekenhuis	arts, inwendige	spec.brief	2002
Amsterdam	Amstelziekenhuis	arts, klinische	kcl-labuitslag	2002
Rotterdam	Maasziekenhuis	arts, orthopedie		1999
Rotterdam	Maasziekenhuis	arts, pathologie	spec.brief	1999
Amsterdam	Amstelziekenhuis	arts, radiologie	röntgenuitslag	2002
Rotterdam	Willemsen	fysiotherapeut	brief	1999
Amsterdam	Amstelziekenhuis	verpleging	opname	2002
<begin>	<vorige 20>		<volgende 20>	<eind>

Op basis van deze index zou de huisarts door middel van aanklikken van <opvragen> de inhoudelijke patiëntgegevens van de aangegeven soort bij een specifieke zorgaanbieder kunnen opvragen.

Architectuurbeslissingen:

**OPV·b01** Zorgaanbieders moeten een index van beschikbare patiëntstukken kunnen opvragen alvorens zij de inhoudelijke patiëntgegevens zelf opvragen.

**OPV·b02** Zorgverleners mogen *altijd* in staat gesteld worden landelijk patiëntgegevens op te vragen, ook indien de vereiste identificatie en authenticatie van de patiënt/cliënt en diens dossier nog niet is uitgevoerd, zie bijlage A.

**OPV·b03** {toekomst} Ten behoeve van de toezichthouder moet de situatie voor een willekeurige datum in het verleden kunnen worden gereconstrueerd, tot aan een afgesproken reconstructiehorizon, zie [Bedrijfsarchitectuur] paragraaf 9.3.

Voor zo'n index is het belangrijk dat:

- de index voldoende details geeft, opdat de zorgverlener kan bepalen of het zinvol is daarop verder in te zoomen,
- de index snel op het scherm verschijnt, opdat de zorgverlener niet in de verleiding komt te stoppen met zoeken,
- de index compleet is, opdat de patiëntgegevens van de dossiers die op het moment van opvraag niet bereikbaar zijn, ook worden weergegeven.

Tenslotte kan de zorgverlener multimediale patiëntstukken apart opvragen. Deze aparte opvraag is handig voor röntgenfoto's, hartfilms, etc. waarvan het overhalen veel tijd kost.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**OPV·s01** opvragen index van beschikbare patiëntstukken.

**OPV·s02** opvragen inhoudelijke patiëntstukken.

**OPV·s03** opvragen multimediale patiëntstukken.

Bij gebruiksscenario [OPV·s01] *opvragen index* gelden de volgende eisen en wensen:

**OPV·e01** De gebruiker moet, uitgaande van een geselecteerde patiënt/cliënt (zie gebruiksscenario [SPA.s01]) een totaaloverzicht van alle beschikbare gegevenssoorten gepresenteerd krijgen, met daarin de volgende attributen per indexregel:

- beheerverantwoordelijke:
  - *identiteit* van de zorgaanbieder,
  - *identiteit* van de zorgverlener,
  - *functie* van de zorgverlener,
- inhoudverantwoordelijke, indien afwijkend van beheerverantwoordelijke:

- *identiteit* van de zorgaanbieder,
- *identiteit* van de zorgverlener,
- *functie* van de zorgverlener,
- *gegevenssoort* bij die zorgaanbieder,
- *actualiteit* van die gegevenssoort bij die zorgaanbieder,
- {toekomst} indicatie van de *beschikbaarheid* van die gegevens.

**OPV·e02** De gebruiker moet de presentatie van indexregels kunnen *dosereren*, bijv. door steeds de volgende 20 items te laten presenteren.

**OPV·e03** De gebruiker moet de presentatie van indexregels kunnen *sorteren*, bijv. door ze in oplopende of aflopende volgorde van een bepaald attribuut te zetten.

**OPV·e04** De gebruiker moet door eenvoudig aanklikken van een indexregel een overzicht van alle patiëntstukken voor die gegevenssoort gepresenteerd krijgen, zie gebruiksscenario [OPV·s02].

**OPV·e05** De gebruiker moet binnen 2 seconden na opvraag de index gepresenteerd krijgen.

**OPV·e06** {toekomst} De toezichthouder wil de situatie voor een willekeurige datum in het verleden kunnen reconstrueren. Hierbij is de bovengenoemde responstijd niet van toepassing.

Bij gebruiksscenario [OPV·s02] *opvragen patiëntstukken* gelden de volgende eisen en wensen:

**OPV·e07** De gebruiker moet desgewenst kunnen *selecteren* welke patiëntstukken opgevraagd worden, aan de hand van één of meer van de volgende kenmerken/attributen:

- over welke *patiënt/cliënt* de gegevens gaan,
- inhoudverantwoordelijke:
  - *identiteit* van de zorgaanbieder,
  - *identiteit* van de zorgverlener,
  - *functie* van de zorgverlener,
- van welke *gegevenssoort* de gegevens zijn,
- tot welke *episode* de gegevens behoren, indien van toepassing,
- op welke *tijdsperiode* de gegevens slaan,
- eventueel nog specifieke criteria, afhankelijk van de gegevenssoort.

**OPV·e08** De zorgverlener moet kunnen *verklaren* waarvoor hij de patiëntstukken nodig heeft, door het invoeren van de volgende zaken:

- {toekomst} voor welke *episode* de gegevens nodig zijn, indien van toepassing,
- {toekomst} wat de *betrokkenheid* van de zorgverlener bij de zorgvraag is,
- {toekomst} de *reden* waarom de patiëntgegevens nodig zijn,
- of er sprake is van een *noodsituatie*.

**OPV·e09** De gebruiker moet de presentatie van patiëntstukken, afhankelijk van de omvang, kunnen *dosereren*, bijv. door steeds de volgende 20 items te laten presenteren.

**OPV·e10** De gebruiker moet de presentatie van patiëntstukken uit verschillende patiëntdossiers kunnen *sorteren*, door patiëntgegevens op volgorde van bepaalde kenmerken te zetten.

**OPV·e11** De gebruiker moet de opgeleverde patiëntstukken na uitlezen:

- geheel of gedeeltelijk kunnen *opnemen* in het eigen patiëntdossier, aangemerkt als kopie, onder vermelding van datum en tijd van overnemen,
- en anders binnen 48 uur na de oplevering *wissen*.

**OPV·e12** De gebruiker moet binnen 5 seconden na opvraag de patiëntstukken gepresenteerd krijgen.

**OPV·e13** { toekomst } De toezichthouder wil de situatie voor een willekeurige datum in het verleden kunnen reconstrueren. Hierbij is de bovengenoemde responstijd niet van toepassing.

Bij gebruiksscenario [OPV·s03] *opvragen multimediale patiëntstukken* gelden de volgende eisen en wensen:

**OPV·e14** { toekomst } Een gebruiker moet de multimediale patiëntstukken kunnen opvragen door eenvoudig aanklikken vanuit gebruiksscenario [OPV·s02].

**OPV·e15** { toekomst } De gebruiker moet binnen 10 seconden na opvraag de multimediale patiëntstukken gepresenteerd krijgen.

**OPV·e16** { toekomst } De toezichthouder wil de situatie voor een willekeurige datum in het verleden kunnen reconstrueren. Hierbij is de bovengenoemde responstijd niet van toepassing.

Voor al deze gebruiksscenario's geldt:

**OPV·e17** Als een gebruiker voor een patiënt/cliënt landelijk patiëntgegevens opvraagt, waarbij :

- het BSN nog niet is geverifieerd bij het landelijke patiëntenregister,
- de benodigde extra WID-controles nog niet zijn uitgevoerd,
- het dossier nog niet inhoudelijk is gecontroleerd met de patiënt/cliënt, mogen de opgeleverde patiëntgegevens niet worden opgenomen in het patiëntdossier als zijnde voorlopig of definitief gekoppeld aan het BSN.

**OPV·e18** De gebruiker mag alleen gepresenteerd krijgen:

- indexregels die verwijzen naar patiëntstukken waarvoor hij geautoriseerd is,
- patiëntstukken waarvoor hij geautoriseerd is, waarbij geen reden wordt opgegeven indien niet alle gepresenteerde stukken compleet waren.

Voor al deze gebruiksscenario's is het nodig dat de gebruiker heeft ingelogd als zorgverlener of gemandateerde medewerker op vertrouwensniveau *midden*, zie gebruiksscenario [INL·s01].

Opmerkingen:

- De tweede figuur toont slechts een voorbeeld van hoe een indexoverzicht gepresenteerd zou kunnen worden aan een huisarts. Een apotheker zou alleen de medicatievoorschriften, -verstrekkingen en allergieën zien. Ook de getoonde gegevenssoorten zijn vooral voorbeelden, waarvan slechts enkele werkelijk zijn gedefinieerd. Tenslotte toont de figuur slechts een deel van de beschikbare informatie in de verwijzindex. Het is aan de leveranciers van zorgaanbiederapplicaties om te bepalen welke gegevens op welke wijze getoond worden. Zo kan het bijv. nuttig zijn op elke indexregel de naam of het type van de zorgaanbieder te vermelden.
- De eisen zijn bedoeld als generieke functionaliteit. Of deze functionaliteit ook werkelijk beschikbaar is voor een specifieke zorgtoepassing, hangt geheel af van de soort patiëntstukken. Zo zal per zorgtoepassing bepaald moeten worden welke opvraagcriteria mogelijk én zinvol zijn.
- De hierboven gestelde responstijden zijn wensen en houden géén garantie in dat deze altijd gerealiseerd kunnen worden. Zo zijn deze responstijden wellicht niet haalbaar voor patiënten/cliënten die een lange medische historie hebben bij vele zorgaanbieders. Echter het grootste deel van de patiënten/cliënten heeft een beperkt aantal zorgaanbieders.
- Per zorgtoepassing kunnen karakteristieke opvraagpatronen gedefinieerd worden, al dan niet parametrizeerbaar, om zorgverleners niet te hoeven vermoeien met cryptische opvraagcriteria. Vermoedelijk zullen zorgapplicaties ook steeds intelligenter worden, zodanig dat:
  - de zorgverlener slechts een bepaalde medische vraag hoeft te stellen,
  - de zorgapplicatie deze intern vertaalt naar een opvraag aan de basisinfrastructuur,
  - de zorgapplicatie de opgeleverde patiëntgegevens op een intelligente wijze interpreteert en verwerkt,
  - de zorgapplicatie slechts een bondig antwoord presenteert aan de zorgverlener, Voorbeeld is een medicatievoorschrijffapplicatie die een vraag kan beantwoorden als “zijn er complicaties te verwachten als deze patiënt het medicijn ABC zou gebruiken?”. Het blijft natuurlijk de verantwoordelijkheid van een arts om zich al of niet op een dergelijke intelligente applicatie te verlaten.
- Ad eis [OPV·e01] Bij het presenteren van de *identiteit* van de zorgaanbieder is het niet altijd zinvol abstracte identificatienummers te tonen. In plaats daarvan kan bijv. de naam en de vestigingsplaats van de zorgaanbieder worden getoond, zoals in het voorbeeld is weergegeven. Die attributen worden dan bijvoorbeeld ‘onder water’ opgehaald uit de zorgaanbiedergids, op basis van de zorgaanbieder-id.
- Ad eis [OPV·e01] en [OPV·e13] Indien bepaalde patiëntstukken niet beschikbaar zijn wegens afscherming of een autorisatieprofiel dat afzonderlijke zorgverleners uitsluit, mag dat niet vermeld worden, want dat zo’n vermelding is zelf vertrouwelijk.
- Ad eis [OPV·e07], [OPV·e15] en [OPV·e18] De toezichthouder kan dit nodig hebben om te reconstrueren wat een zorgverlener gezien zou hebben als hij op een bepaald tijdstip in het verleden bepaalde patiëntgegevens zou hebben opgevraagd. Dit tijdstip kan niet verder in het verleden liggen dan een afgesproken reconstructiehorizon.
- Ad eis [OPV·e08] In grote zorginstellingen worden de patiëntgegevens van alle patiënten/cliënten die op het spreekuur verwacht worden, ruim tevoren opgevraagd, veelal automatisch. Deze gewoonte stamt uit het papieren tijdperk, toen

patiëntdossiers gemakkelijk konden zoekraken. Het *automatisch* opvragen van *landelijk beschikbare* patiëntgegevens is echter juridisch niet toegestaan. Op grond van de WGBO moet in individuele gevallen bepaald worden of een opvraag nodig is.

- Ad eis [OPV.e07] De *gegevenssoort* geeft niet alleen de aard van de informatie aan, maar impliciet ook het aggregatieniveau van de informatie. Zo is een brief een patiëntdocument, een diagnose een patiëntgegevensbijdrage, een bloeddruk een patiëntgegevenselement, zie verder [Bedrijfsarchitectuur] paragraaf 6.3.
- Ad eis [OPV.e08] Deze verklaring kan nodig zijn voor de logging, zodat een toezichthouder beter kan beoordelen of de opvraag rechtmatig was.
- Ad eis [OPV.e11] Een zorgverlener mag opgevraagde patiëntstukken alleen *opnemen* in zijn eigen dossier, voor zover dit voor de behandeling *op dat moment* noodzakelijk is. Bijvoorbeeld een huisarts die bepaalde labuitslagen overneemt in een eigen verwijsbrief voor een specialist. In andere gevallen moeten de opgevraagde patiëntgegevens na uitlezen worden gewist.
- Ad eis [OPV.e11] Het is dus niet toegestaan dat zorgverleners patiëntgegevens gaan opvragen, en daarvan lokaal een kopie gaan vastleggen om ze “alvast bij de hand te hebben”. Immers, van kopieën weet men nooit of de inhoud actueel is. De behoefte aan lokaal kopiëren kan overigens worden verminderd door ervoor te zorgen dat de verwijsindex voldoende snel en beschikbaar is. Vandaar de bovenvermelde responstijden. Niettemin hebben sommige zorgaanbieders de behoefte om een dag voor het spreekuur alle relevante patiëntgegevens van de bezoekende patiënten/cliënten alsvast klaar te zetten voor de dienstdoende zorgverleners.
- Ad eis [OPV.e17] Volgens Wbsn-z artikel 12 mag een zorgverlener in spoedeisende gevallen zonder BSN-verificatie of WID-controle patiëntgegevens opvragen, maar mag deze dan niet vastleggen met dat BSN of verder uitwisselen met dat BSN. Welke extra WID-controles anders nodig zouden zijn geweest, is ter beoordeling van de zorgaanbieder.
- Architectuurbeslissing [OPV.b03] staat nog ter discussie, wegens de mogelijk te zware consequenties voor het LSP en ieder GBZ.

Openstaande punten:

- De eisen en wensen van de *patiënt/cliënt* t.a.v. het opvragen van eigen patiëntgegevens zijn nog niet uitgewerkt, maar zijn veelal een deelverzameling van de bovenstaande.

## 4.10 Versturen Patiëntgegevens (STU)

Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 8.3, moet een zorgverlener verschillende soorten patiëntberichten via het landelijk schakelpunt veilig kunnen versturen naar andere zorgverleners: opdracht, antwoord en melding. Voor het schakelpunt is dat onderscheid niet zichtbaar. Het zijn de zorgaanbiederapplicaties die op grond van de berichtsoort kunnen bepalen dat bijv. een opdracht moet leiden tot een antwoord.

Wanneer bijv. een huisarts een recept uitschrijft maar dit niet kan versturen, omdat de patiënt/cliënt nog niet weet bij welke apotheek hij de medicijnen wil afhalen, heeft de zorgverlener twee mogelijkheden, zie bijlage B:

- het patiëntbericht versturen naar een informatiedoorgever, volgens NEN7503,
- het patiëntbericht klaarzetten en aanmelden in de verwijsindex.

Wanneer een zorgverlener een of meer patiëntberichten wil versturen maar het schakelpunt blijkt op dat moment niet bereikbaar, dan moet de zorgverlener deze patiëntberichten kunnen bewaren voor latere verzending.

Architectuurbeslissingen:

**STU·b01** {toekomst} Zorgverleners moeten een patiëntbericht kunnen klaarzetten zonder te versturen, door het aan te melden in de verwijsindex, zodat een andere zorgverlener het kan ophalen.

**STU·b02** Zorgverleners mogen *niet* in staat gesteld worden landelijk patiëntgegevens te versturen, anders dan wanneer deze definitief zijn gekoppeld aan een BSN, zie bijlage A.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**STU·s01** sturen patiëntbericht naar een andere zorgverlener,

**STU·s02** ontvangen patiëntbericht van een andere zorgverlener,

**STU·s03** klaarzetten ongeadresseerd patiëntbericht,

**STU·s04** ophalen ongeadresseerd patiëntbericht.

Bij gebruiksscenario [STU·s01] *versturen patiëntbericht* gelden de volgende eisen en wensen:

**STU·e01** De gebruiker moet bij het samenstellen van een patiëntbericht het volgende kunnen aangeven:

- het type patiëntbericht: opdracht, antwoord en melding,
- het BSN van de onderhavige patiënt/cliënt, door deze te selecteren uit een lijst van patiënten/cliënten in het eigen patiëntdossier,
- of de aflevering van het patiëntbericht in de juiste postbus aan de afzender wel of niet onmiddellijk bevestigd moet worden.

- STU·e02** De gebruiker moet bij het samenstellen van een patiëntbericht de inhoud op verschillende manieren kunnen invullen:
- door het kiezen van een berichtsoort en het handmatig of automatisch invullen van de velden,
  - {toekomst} door het kiezen van een vrij tekstformaat en het handmatig invullen van het bericht,
  - door het bijvoegen van een kopie van een patiëntstuk uit het eigen patiëntdossier,
  - {toekomst} door het aangeven van de identificatie van een patiëntstuk uit het eigen patiëntdossier.

- STU·e03** De gebruiker moet, indien het samenstellen, adresseren en verzenden van een patiëntbericht automatisch plaatsvindt, de mogelijkheid hebben om:
- de inhoud of strekking van het patiëntbericht te beoordelen,
  - de verzending van het patiëntbericht te continueren of te stoppen.

- STU·e04** De gebruiker moet bij het samenstellen van een patiëntbericht de bestemming op verschillende manieren kunnen aangeven:
- door de afzender van een ander patiëntbericht automatisch over te nemen als bestemming,
  - door één of meer zorgaanbieders te selecteren uit de zorgaanbiedergids, zie paragraaf 4.4, of eventueel uit een eigen zorgaanbiederadresboek,
  - door rechtstreeks het HL7-adres in te voeren.

- STU·e05** De gebruiker moet na een mislukte poging tot versturen van een patiëntbericht wegens onbereikbaar schakelpunt of onbereikbare postbus van de bestemde zorgaanbieder:
- ervoor kunnen kiezen om het patiëntbericht te bewaren voor latere verzending,
  - bij de eerstvolgende keer inloggen erop worden geattendeerd dat er patiëntberichten klaarstaan voor verzending,
  - alle klaarstaande patiëntberichten alsnog kunnen verzenden.

Bij gebruiksscenario [STU·s02] *ontvangen patiëntbericht* gelden de volgende eisen en wensen:

- STU·e06** De gebruiker moet na het ontvangen van een patiëntbericht de inhoud op de volgende manieren kunnen ontsluiten:
- door het selecteren van het bijgevoegde patiëntstuk,
  - {toekomst} door het selecteren van de *identificatie* van een patiëntstuk genoemd in het patiëntbericht en het opvragen daarvan uit het patiëntdossier van de afzender.

- STU·e07** De gebruiker moet na het ontsluiten van de inhoud van patiëntgegevens in een patiëntbericht, deze op de volgende manieren kunnen afhandelen:
- door het *uitlezen* daarvan door de zorgverlener,
  - door het automatisch *uitlezen* daarvan door een applicatie,
  - door het *opnemen* daarvan in het eigen patiëntdossier, aangemerkt als kopie,
  - door het *wissen* ervan.



**STU·e89** De gebruiker moet na het ontvangen van een patiëntbericht van het type opdracht, een patiëntbericht van het type antwoord kunnen terugsturen en daarbij:

- automatisch de afzender van het ontvangen patiëntbericht overnemen als bestemming,
- automatisch de referentie naar de identificatie van het ontvangen patiëntbericht vermelden,
- automatisch de identificatie van de onderhavige patiënt/cliënt overnemen,
- aangeven of de opdracht wordt geaccepteerd of afgewezen.

Bij gebruiksscenario [STU·s03] *klaarzetten patiëntbericht* gelden de volgende eisen en wensen:

**STU·e09** { toekomst } De gebruiker moet een patiëntbericht kunnen klaarzetten zonder te versturen, opdat een andere zorgaanbieder het patiëntbericht zelf kan opvragen, waarbij geldt:

- zonder vermelde bestemming kan iedere geautoriseerde zorgaanbieder het bericht opvragen,
- met vermelde bestemming kan iedere vermelde, geautoriseerde zorgaanbieder het bericht opvragen.

Bij gebruiksscenario [STU·s04] *ophalen patiëntbericht* gelden de volgende eisen en wensen:

**STU·e10** { toekomst } De gebruiker moet uitgaande van een geselecteerde patiënt/cliënt (zie use case 0.3.1) een totaaloverzicht van alle klaargezette patiëntberichten gepresenteerd krijgen, met daarin vermeld voor ieder patiëntbericht:

- *zorgaanbieder-functie* van die zorgaanbieder,
- *berichtsoorten* bij die zorgaanbieder,
- *actualiteit* van die berichtsoort bij die zorgaanbieder,
- *indicatie* van de beschikbaarheid van die patiëntberichten.

**STU·e11** { toekomst } De gebruiker moet, uitgaande van het totaaloverzicht, door eenvoudig aanklikken een patiëntbericht kunnen ophalen.

Bij gebruiksscenario [STU·s01] *versturen patiëntbericht* en gebruiksscenario [STU·s03] *klaarzetten patiëntbericht* geldt bovendien:

**STU·e12** De gebruiker mag voor een patiënt/cliënt alleen definitief gekoppelde patiëntstukken landelijk versturen of klaarzetten.

Voor al deze gebruiksscenario's is het nodig dat de gebruiker heeft ingelogd als zorgverlener of gemandateerde medewerker op vertrouwensniveau *midden*, zie gebruiksscenario [INL·s01].

Opmerkingen:

- Ad gebruiksscenario [STU·s01] Het versturen van patiëntberichten wordt idealiter ondersteund door een zorgaanbiederapplicatie die de zorgverlener afschermt van de vele, bovengenoemde keuzemogelijkheden en het versturen zonedig combineert met andere acties. Zo zal een elektronisch voorschrijfsysteem het opstellen van een medicatievoorschrift én het vastleggen daarvan als patiëntstuk in het eigen dossier én

het versturen daarvan als patiëntbericht naar een andere zorgaanbieder, als één gecombineerde actie aan de gebruiker presenteren.

- Ad eis [STU·e01] De aard van het patiëntbericht geeft aan of het onderdeel is van een reeks samenhangende interacties. Zo is een melding een vrijblijvend patiëntbericht, waarop niet gereageerd hoeft te worden. Een opdrachtbericht kan het begin zijn van een transactie, met status *verstuurd*. Daarop kunnen antwoordberichten komen, die de status van de transactie veranderen in *geaccepteerd* of *afgewezen*, dan wel *uitgevoerd*. Daarop kunnen nog andere berichten volgen, die telkens de status veranderen. Dit verschilt per zorgtoepassing.
- Ad eis [STU·e03] Wegens de foutgevoeligheid is het niet wenselijk dat zorgverleners eigenhandig HL7-adressen gaan intoetsen. Toch kan het noodzakelijk zijn, bijv. als een zorgaanbieder (nog) niet vermeld staat in de zorgaanbiedergids.
- Ad eis [STU·e03] In plaats van steeds de *landelijke* zorgaanbiedergids raadplegen, kan het doelmatiger zijn om bereikbaarheidsgegevens over te nemen naar een *eigen* zorgaanbiederbestand. Momenteel gebruiken zorgaanbieders vaak een zogenaamd *derdenbestand* waarin voor iedere patiënt/cliënt onder meer de eigen huisarts en de vaste apotheek wordt vastgelegd. Het nadeel van deze alternatieven is dat ze de keuzevrijheid van de patiënt/cliënt beperken.
- Ad eis [STU·e05] Ook als een zorgaanbiederapplicatie, zoals een elektronisch voorschrijfsysteem, de zorgverlener afschermt van het bewerkelijke invullen van een patiëntbericht, blijft de zorgverlener verantwoordelijk voor het resultaat. Daarom moet hij de kans hebben om het resultaat te beoordelen en de verzending eventueel af te breken.
- Ad eis [STU·e07] Het *uitlezen* van een ontvangen patiëntstuk kan automatisch plaatsvinden door bijv. een werkstroomapplicatie die opdrachten als medicatievoorschriften of labaanvragen, etc. automatisch toewijst aan beschikbare medewerkers.
- Ad eis [STU·e07] Overigens mag een zorgverlener conform de WGBO kopieën van patiëntstukken alleen opnemen in het eigen dossier voorzover het *op dat moment* noodzakelijk is voor de behandeling.
- Ad eis [STU·e08] De identificatie van een ontvangen patiëntbericht is nodig opdat zorgaanbiederapplicaties eventueel transacties kunnen ondersteunen. Van een transactie is pas sprake als de opdrachtgevende applicatie na ontvangst van een antwoordbericht een statusverandering in het eigen patiëntdossier doorvoert. Merk op dat het schakelpunt slechts interacties voorbij ziet komen en dus geen transacties bewaakt. De transactie moet dus door de beide zorgaanbiederapplicaties worden bewaakt.
- Ad eis [STU·e10] Het ophalen van een patiëntbericht is vergelijkbaar met het opvragen van een patiëntstuk zoals beschreven in eis [OPV·e11]. Een belangrijk verschil is echter: na het ophalen van een patiëntbericht wordt, net als bij het positief beantwoorden van een opdrachtbericht, de uitvoeringsverantwoordelijkheid voor dat verzoek geaccepteerd. Daarbij verandert de status van de transactie naar *verstuurd*.
- Ad eis [STU·e12] Als gevolg van architectuurbeslissing [STU·b02] worden alleen *definitief* gekoppelde patiëntstukken landelijk uitgewisseld. Volgens Bbsn-z artikel 27 is

het onder voorwaarden toegestaan om *niet* gekoppelde patiëntstukken zonder BSN uit te wisselen, maar AORTA kan dat niet ondersteunen. Volgens Bbsn-z artikel 28 is het onder voorwaarden ook toegestaan om *voorlopig* gekoppelde gegevens met onzeker BSN uit te wisselen, maar AORTA ondersteunt dat niet, zie bijlage A.

## 4.11 Overdragen patiëntgegevens (OVD)

Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 8.3 moet een zorgverlener de verantwoordelijkheid van bepaalde patiëntstukken, of zelfs een heel patiëntdossier, via het schakelpunt veilig kunnen overdragen aan een andere zorgverlener.

Het overdragen van patiëntstukken houdt in dat de ene zorgverlener bepaalde patiëntstukken aanmerkt als *kopie* in het eigen patiëntdossier, de stukken als *origineel* verstuurt in een opdrachtbericht naar een andere zorgverlener, waarna die andere zorgverlener de verantwoordelijkheid kan accepteren of weigeren.

Bij acceptatie legt die andere zorgverlener de aangeboden patiëntstukken vast in het eigen dossier als *origineel*, geeft ze vrij voor opvraag door derden (met zonodig een aanmelding bij de verwijsindex) en stuurt een acceptatiebericht terug. Daarna kan de eerste zorgverlener de patiëntstukken afschermen voor opvraag door derden (met zonodig een afmelding bij de verwijsindex) en eventueel verwijderen.

Bij weigering stuurt die andere zorgverlener een weigerbericht terug. Daarna kan de eerste zorgverlener de patiëntstukken weer als *origineel* aanmerken.

Architectuurbeslissingen:

**OVD·b01** Zorgverleners mogen *niet* in staat gesteld worden landelijk patiëntgegevens over te dragen indien de vereiste identificatie en authenticatie van de patiënt/cliënt en diens dossier nog niet zijn uitgevoerd, zie bijlage A.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**OVD·s01** verzoeken overdracht van patiëntstukken,

**OVD·s02** beantwoorden overdracht van patiëntstukken,

**OVD·s03** afronden overdracht van patiëntstukken.

Bij gebruiksscenario [OVD·s01] *verzoeken overdracht* gelden de volgende eisen en wensen:

**OVD·e01** De gebruiker moet met behulp van een overdrachtsverzoek de mogelijkheid hebben om:

- patiëntstukken ter overdracht *aan te bieden* aan een andere zorgverlener,
- patiëntstukken ter overdracht *te vragen* van een andere zorgverlener.

**OVD·e02** De gebruiker moet een overdrachtsverzoek kunnen samenstellen door:

- vermelden van het BSN van de onderhavige patiënt/cliënt door te selecteren uit een lijst van patiënten/cliënten in het eigen patiëntdossier,
- selecteren van bepaalde patiëntstukken uit het eigen patiëntdossier.

**OVD·e03** De gebruiker moet een overdrachtsverzoek kunnen adresseren door:

- een zorgaanbieder te selecteren uit een eigen zorgaanbiederadresboek of

- {toekomst} een zorgaanbieder te selecteren uit de zorgaanbiedergids, zie paragraaf 4.4, of
- door rechtstreeks het HL7-adres in te voeren.

Bij gebruiksscenario [OVD-s02] *beantwoorden overdracht* gelden de volgende eisen en wensen:

**OVD-e04** De gebruiker moet de overdracht kunnen beoordelen door het inzien van de aangeboden patiëntstukken.

**OVD-e05** De gebruiker moet de overdracht kunnen weigeren door:

- vermelden van de reden van de weigering,
- in geval de overdracht werd *aangeboden*:
  - vastleggen van de aangeboden patiëntstukken in het eigen patiëntdossier, aangemerkt als kopie,
- in geval de overdracht werd *gevraagd*:
  - de patiëntstukken in het eigen patiëntdossier ongewijzigd blijven,
- versturen van een weigerbericht aan de verzoekende zorgverlener.

**OVD-e06** De gebruiker moet de overdracht kunnen accepteren door:

- in geval de overdracht werd *aangeboden*:
  - vastleggen van de aangeboden patiëntstukken in het eigen patiëntdossier, aangemerkt als origineel,
  - eventueel vrijgeven van de aangeboden patiëntstukken voor opvraag door derden (met zonodig een aanmelding of heraanmelding bij de verwijfsindex),
- in geval de overdracht werd *gevraagd*:
  - de gevraagde patiëntstukken in het eigen patiëntdossier worden aangemerkt als kopie,
  - eventueel afschermen van de aangeboden patiëntstukken voor opvraag door derden (met zonodig een heraanmelding of afmelding bij de verwijfsindex),
- versturen van een acceptatiebericht aan de verzoekende zorgverlener.

Bij gebruiksscenario [OVD-s03] *afronden overdracht* gelden de volgende eisen en wensen:

**OVD-e07** De gebruiker moet een weigerbericht kunnen verwerken door kennisneming van de opgegeven reden van weigering.

**OVD-e08** De gebruiker moet een acceptatiebericht kunnen verwerken door:

- in geval de overdracht werd *aangeboden*:
  - afschermen van de overgedragen patiëntstukken voor opvraag door derden (met zonodig een afmelding of heraanmelding bij de verwijfsindex),
  - aanmerken van de overgedragen patiëntstukken in het eigen patiëntdossier als kopie,
- in geval de overdracht werd *gevraagd*:
  - vrijgeven van de overgedragen patiëntstukken voor opvraag door derden (met zonodig een aanmelding of heraanmelding bij de verwijfsindex),
  - aanmerken van de overgedragen patiëntstukken in het eigen patiëntdossier als origineel,

**OVD·e09** De gebruiker moet erop kunnen vertrouwen dat een onbeantwoord overdrachtsverzoek na overschrijding van een instelbare termijn automatisch wordt geweigerd.

Bij gebruiksscenario [OVD·s01] *verzoeken overdracht* en gebruiksscenario [OVD·s02] *beantwoorden overdracht* geldt bovendien:

**OVD·e10** De gebruiker mag voor een patiënt/cliënt de overdracht van patiëntstukken kunnen verzoeken resp. accepteren, alleen voor definitief gekoppelde patiëntstukken.

Voor al deze gebruiksscenario's is het nodig dat de gebruiker heeft ingelogd als zorgverlener of gemandateerde medewerker op vertrouwensniveau *midden*, zie gebruiksscenario [INL·s01].

Opmerkingen:

- De overdracht van patiëntstukken is een transactie tussen twee zorgaanbieder-applicaties. Merk op dat het schakelpunt slechts interacties voorbij ziet komen en dus geen transacties bewaakt. De transactie moet dus door de beide zorgaanbieder-applicaties worden bewaakt.
- Gedurende de transactie staan de desbetreffende patiëntstukken mogelijk twee keer vermeld in de verwijzindex. Bij opvragen zal blijken dat het kopieën van elkaar zijn.
- Ad eis [OVD·e01] Het verzoek tot overdracht is hier gecombineerd met de onderhavige patiëntstukken, zoals dat bijvoorbeeld passend is voor het overdragen van een waarneemverslag bij huisartswaarneming. In geval van overdracht van een dossier is het verstandiger om eerst het verzoek te laten accepteren of weigeren en daarna pas het dossier over te sturen. Daarbij kan nog onderscheid gemaakt worden tussen een haal-mechanisme en een breng-mechanisme. Dit wordt in een latere versie van dit document uitgewerkt.
- Ad eis [OVD·e03] Ondanks de weigering kan de andere zorgverlener de ontvangen patiëntstukken opnemen in zijn patiëntdossier, maar dan wel als kopie. Merk op dat het plaatsen van een los patiëntstuk in een bepaalde context van een dossier nieuwe toegevoegde waarde kan hebben.
- Ad eis [OVD·e06] In principe mogen patiëntstukken niet worden verwijderd uit een patiëntdossier, maar in geval van overdracht tussen twee zelfstandige artsen, mogen geen kopieën worden achtergehouden conform de KNMG-richtlijnen, zie [Bedrijfs-architectuur] paragraaf 7.1.

## 4.12 Beheren autorisatieprotocol (BAT)

Bij het autorisatieprotocol beschreven in [Bedrijfsarchitectuur] paragraaf 9.2, moet onderscheid gemaakt worden tussen:

- een *algemeen* autorisatieprotocol, waarin de bevoegdheden van alle zorgpartijen grofmazig staan vermeld, per gegevensklasse.
- een *medisch* autorisatieprotocol, waarin de bevoegdheden nader zijn uitgesplitst naar de functie van de zorgaanbieders en de gegevenssoort binnen de klasse van medische gegevens.

Zo'n *algemeen* autorisatieprotocol zou er als volgt kunnen uitzien:

Reagerende zorgpartij	Agerende zorgpartij	patiënt/ cliënt	zorg- aanbieder	zorg- verzeker.	zorg- coördin.
	gegevens- klasse				
patiënten- register	persoonlijk	O, eigen	O	O	O
patiënt/cliënt	persoonlijk	O, eigen	O	O, eigen	O
zorgaanbieder	persoonlijk	O, eigen	O	O	O
	medisch	O, eigen	M	-	-
	logistiek	O, eigen	O	-	O
	financieel	O, eigen	-	O, eigen	-
zorgverzeker.	financieel	O, eigen	O, eigen	-	-
...					

De *agerende* zorgpartij is degene die een gebruikersinteractie (bijv. opvragen patiëntgegevens) initieert. De reagerende partij is degene die de gebruikersinteractie beantwoordt (bijv. door het opleveren van de gevraagde patiëntgegevens).

De bevoegdheid kan per vakje worden aangeduid, bijv.:

- O = bevoegd tot *opvragen* van deze patiëntgegevens,
- V = bevoegd tot *versturen* van deze patiëntgegevens,
- M = zie medisch autorisatieprotocol.

De reikwijdte van de bevoegdheid kan per vakje worden beperkt, bijv.:

- eigen = alleen patiëntgegevens van de eigen patiënt.

De derde kolom geeft bijv. aan dat een zorgverzekeraar toegang heeft tot de volgende patiëntgegevens:

- persoonlijke gegevens in het landelijke patiëntenregister (BVBSN via SBV-Z),
- persoonlijke gegevens in de patiëntkluizen van alleen de *eigen* cliënten,
- persoonlijke gegevens in de dossiers van zorgaanbieders,
- logistieke gegevens in de dossiers van zorgaanbieders,
- financiële gegevens in de dossiers van zorgaanbieders van alleen de *eigen* cliënten.

De bovenstaande invulling van bevoegdheden is slechts illustratief. Het algemene autorisatieprotocol is vooralsnog alleen van toepassing op het opvragen van het BSN. Pas na uitwerking van relevante landelijke toepassingen, kunnen meer representatieve voorbeelden worden gegeven.

Zo'n *medisch* autorisatieprotocol zou er als volgt kunnen uitzien:

Landelijke toepassing:	EMD						WDH		
Gebruikers-interactie:	Public medic voor schrft	Verstu medic voor schrft	Opvra medic voor schrft	Public medic ver strekk	Verstu medic ver strekk	Opvra medic ver strekk	Public 1-lijns doss	Opvra samenvatt DWH	Verstuslag DWH
Zorgverlener-functie:									
Apotheker,stad			V	V	V	V			
Apotheker,zkh			V	V	V	V			
...									
Arts,allergolo..	V	V	V			V			
Arts,cardiolog..	V	V	V			V			
Arts,dermatol..	V	V	V			V			
Arts,gastro-e..	V	V	V			V			
Arts,huisarts...	V	V	V	V	V	V	V	V	V
...									

In de praktijk zal weinig gebruik gemaakt worden van alle mogelijke differentiaties. Zo zullen de meeste artsen vermoedelijk dezelfde bevoegdheden krijgen, ongeacht hun specialisme en betrokkenheid.

De tabellen met het algemene en het medische autorisatieprotocol kunnen worden:

- bijgehouden door autorisatiebeheerders op direct of indirect verzoek van de medische beroepsverenigingen in samenwerking met de patiëntenvereniging, nadat zij onderling een nieuw of gewijzigd autorisatieprotocol zijn overeengekomen.
- {toekomst} geraadpleegd door zorgverleners die willen weten welke bevoegdheden zij hebben. Anders zullen zij proefondervindelijk moeten vaststellen welke gegevenssoorten wel/niet toegankelijk zijn voor hen.

Architectuurbeslissingen:

**BAT·b01** {toekomst} Zorgverleners moeten het autorisatieprotocol kunnen raadplegen.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**BAT·s01** raadplegen autorisatieprotocol en autorisatielog.

**BAT·s02** aanpassen *algemeen* autorisatieprotocol.

**BAT·s03** aanpassen *medisch* autorisatieprotocol.

Bij gebruiksscenario [BAT·s01] gelden de volgende eisen en wensen:



**BAT·e01** De gebruiker moet het algemene en het medische autorisatieprotocol kunnen *raadplegen*, waarbij hij kan kiezen voor:

- de actuele situatie,
- de toekomstige wijzigingen,
- een historische situatie, door invoer van een bepaalde datum in het verleden.

**BAT·e02** De gebruiker moet de autorisatielog kunnen raadplegen, waarin wordt bijgehouden welke autorisatiebeheerder op welk tijdstip welke wijziging heeft doorgevoerd.

Bij gebruiksscenario [BAT·s02] *aanpassen algemeen autorisatieprotocol* gelden de volgende eisen en wensen:

**BAT·e03** De gebruiker moet het algemene autorisatieprotocol kunnen *aanpassen*, door voor iedere combinatie van:

- opvragende zorgpartij
- opleverende zorgpartij
- de gegevensklasse

de bevoegdheid vast te leggen met:

- de bevoegde algemene gebruikersinteractie(s), zie [Technische Architectuur] paragraaf 5.1,
- {toekomst} autorisatieniveau
- vereiste vertrouwensniveau: laag, midden, hoog
- vereiste logging: wel, niet
- ingangsdatum van wijziging

behalve voor de combinatie *zorgaanbieder/zorgaanbieder/medisch*, want daarvoor geldt het *medische* autorisatieprotocol.

Bij gebruiksscenario [BAT·s03] *aanpassen medisch autorisatieprotocol* gelden de volgende eisen en wensen:

**BAT·e04** De gebruiker moet het medische autorisatieprotocol kunnen *aanpassen*, door voor iedere combinatie van

- de functie van de zorgverlener
- de betrokkenheid van de zorgverlener: hoofdbehandelaar, waarnemer, medebehandelaar

de bevoegdheid vast te leggen met:

- de bevoegde medische gebruikersinteractie(s), zie [Technische Architectuur] paragraaf 4.1,
- {toekomst} autorisatieniveau
- {toekomst} vereiste vertrouwensniveau: laag, midden, hoog
- ingangsdatum van wijziging

Voor al deze gebruiksscenario's is het nodig dat de gebruiker heeft ingelogd als autorisatiebeheerder of lokale beheerder op vertrouwensniveau *midden*, zie gebruiksscenario [INL·s01].

Opmerkingen:

- De architectuurbeslissing [BAT.b01] is als {toekomst} aangemerkt, omdat daarvoor eerst HL7v3-berichten gedefinieerd moeten worden.

- Ad eis [BAT·e03] In het *algemene* autorisatieprotocol kan worden ingesteld of bijv. het opvragen van persoonlijke patiëntgegevens (bijv. BSN) wel of niet gelogd moet worden. Indien de bron (SBV-Z) zelf de logging verzorgt, zou het schakelpunt dat niet hoeven te doen.
- Ad eis [BAT·e03] De beheerder moet een ingangsdatum kunnen instellen opdat hij een nieuwe autorisatieregel ruim van tevoren kan voorbereiden. Een einddatum is niet nodig omdat autorisatieregels in principe voor onbepaalde tijd worden gedefinieerd. De eventuele einddatum van een autorisatieregel wordt in de praktijk impliciet bepaald door de ingangsdatum van een nieuw toegevoegde autorisatieregel die de bevoegdheid van een oudere autorisatieregel overschrijft.
- Ad eis [BAT·e04] In het *medische* autorisatieprotocol kan niet worden ingesteld of bepaalde gebruikersinteracties wel of niet gelogd moeten worden, want dat zou fraudegevoelig zijn. Gebruikersinteracties met medische gegevens moeten altijd worden gelogd.
- Ad eis [BAT·e03] en [BAT·e04] Het autorisatieniveau heeft voorlopig geen betekenis. In de toekomst kunnen verschillende niveaus onderkend worden, in lijn met de gevoeligheidsniveaus gehanteerd in [prENV13606:2003] en [HL7v3].
- Ad eis [BAT·e04] De gegevenssoorten in het medisch autorisatieprotocol moeten overeenkomen met die in de gegevenssoortentabel, zie paragraaf 5.4.
- De autorisatiebeheerder werkt direct of indirect in opdracht van de medische beroepsverenigingen in samenwerking met de patiëntenvereniging.
- *Medewerkers* staan niet vermeld in het autorisatieprotocol, want zij kunnen hooguit onder verantwoordelijkheid van een mandaterende zorgverlener toegang krijgen, zie [Bedrijfsarchitectuur] paragraaf 9.4. Eventueel zou het landelijke autorisatieprotocol gebruikt kunnen worden om een landelijke grens te stellen aan de mandateringen van afzonderlijke zorgverleners, indien daar behoefte aan is.

## 4.13 Bijhouden autorisatieprofiel (BAF)

Het autorisatieprofiel van een patiënt/cliënt, zoals beschreven in [Bedrijfsarchitectuur] paragraaf 9.2, bestaat uit:

- een vlag om aan te geven of de patiënt/cliënt überhaupt akkoord gaat met elektronische, landelijke uitwisseling van zijn patiëntgegevens,
- nadere wensen om bepaalde zorgpartijen uit te sluiten van inzage, als inperking op het generieke autorisatieprotocol,
- {toekomst} vlaggen om aan te geven of de patiënt/cliënt akkoord gaat met elektronisch inkijken in zijn autorisatieprofiel, toegangslg resp. elektronisch wijzigen van zijn autorisatieprofiel.

Zo'n autorisatieprofiel zou er als volgt kunnen uitzien:

<i>Patiënt/cliënt</i>	BSN		<i>Akkoord uitw.pat.geg.</i>	ja	
<i>Laatst gewijzigd:</i>	dd-mm-jjjj		<i>Akkoord inkijk log</i>	ja	
			<i>Akkoord inkijk profiel</i>	ja	
			<i>Akkoord wijzig profiel</i>	nee	
<i>Gegevensklasse &gt;</i>		Persoonlijk	Medisch	Logistiek	Financieel
<i>Zorgpartij</i>					
zorgverleners	alle	N	N	N	N
arts, huisarts...	Jansen	A	A	A	A
apothekers	alle	T	T	T	T
apotheker	Pietersen	N	N	N	N
zorgverzekeraars	alle	X	X	X	X
	Algemeene	A	X	A	A
...					

De bevoegdheid kan per vakje worden aangeduid als, bijv.:

- A = altijd
- N = alleen in noodgeval
- T = alleen na expliciete toestemming
- X = nooit

De patiënt/cliënt heeft in het bovenstaande voorbeeld aangegeven:

- akkoord te gaan met elektronische uitwisseling van zijn patiëntgegevens conform het autorisatieprotocol, met de navolgende uitzonderingen,
- dat zorgverleners in het algemeen geen inzage krijgen, met uitzondering van:
  - een huisarts met UZI-nr 123 die alles mag inzien,
  - alle apothekers die alleen met expliciete toestemming alles mogen inzien,
  - echter met uitzondering van apotheker met UZI-nr 234,
- dat zorgverzekeraars in het algemeen geen inzage krijgen, met uitzondering van:

- verzekeringsmij "De Algemeene" met UZOVI-nr 123 die alles mag inzien behalve medische gegevens.

Het autorisatieprofiel van een patiënt/cliënt kan worden bijgehouden door:

- autorisatiebeheerders in opdracht van de autorisatiemanager na verzoek van die patiënt/cliënt. Afhankelijk van de werklust die dit zal opleveren voor de autorisatiebeheerders, kan dit beperkt blijven tot het wijzigen van het al/of niet akkoord gaan met elektronische uitwisseling.
- zorgaanbieders op verzoek van die patiënt/cliënt. Afhankelijk van de inrichting, kan dit beperkt blijven tot het interne autorisatieprofiel bij die zorgaanbieder, in welk geval de patiënt/cliënt langs elk van zijn zorgaanbieders moet.
- de patiënt/cliënt zelf, bijvoorbeeld via het Internet wanneer hij beschikt over een geschikt elektronisch vertrouwensmiddel. Verwacht wordt dat iedere burger in de toekomst een e-NIK heeft.

Wanneer een patiënt/cliënt niet akkoord gaat met elektronische uitwisseling van zijn patiëntgegevens, mogen zijn gegevens ook niet worden opgenomen in de verwijsindex, zie architectuurbeslissing [VWI-b05]. Nadeel daarvan is dat, wanneer hij later alsnog akkoord gaat, aan de verwijsindex niet te zien is waar inmiddels allemaal patiëntgegevens van hem liggen en dat deze gegevens dus ook niet opgevraagd kunnen worden. Patiënten/cliënten dienen daarover duidelijk te worden voorgelicht.

In plaats daarvan kan een patiënt/cliënt ervoor kiezen wél akkoord te gaan met elektronische uitwisseling, maar alle bevoegdheden op *nooit* laten zetten. Op deze wijze worden zijn patiëntgegevens wél aangemeld aan de verwijsindex, maar zijn ze voor niemand zichtbaar.

Wanneer een patiënt/cliënt niet akkoord gaat met elektronische uitwisseling van zijn patiëntgegevens, moet het voor zorgaanbieders mogelijk blijven om diens BSN op te vragen uit het landelijke patiëntenregister. Zorgaanbieders zijn immers verplicht om het BSN ook te gebruiken voor papieren uitwisseling van patiëntgegevens.

In principe moet een patiënt/cliënt in zijn autorisatieprofiel willekeurige zorgpartijen kunnen uitsluiten:

- zorgaanbieders, individuele zorgverleners en gemandateerde medewerkers,
- {toekomst} zorgverzekeraars.

Het is denkbaar dat een patiënt/cliënt in zijn autorisatieprofiel de bevoegdheden van bepaalde zorgverleners zou willen *verruimen* ten opzichte van die in het autorisatieprotocol. Daarvoor is niet gekozen, want dit zou de werking van autorisatie nog complexer maken dan het al is. Bovendien is het zeer de vraag of een zorgverlener met verruimde bevoegdheden eraan zal denken voor die ene patiënt/cliënt een opvraag te doen waarvoor hij gewoonlijk niet geautoriseerd is.

Als voor een patiënt/cliënt géén autorisatieprofiel is ingevuld (en dat zal aanvankelijk voor de meeste patiënten/cliënten het geval zijn), gelden *verstekwaarden* voor de "akkoord"-velden. Hoewel wordt gestreefd naar veronderstelde toestemming voor elektronisch uitwisseling van patiëntgegevens voor alle patiënten/cliënten die geen bezwaar aantekenen, zie [Bedrijfsarchitectuur] paragraaf 9.2, de toelichting op punt (d),

is nog onzeker of dat lukt. Aldus moeten verstekwaarden voor *akkoord* kunnen worden ingesteld. Dit wordt dus een aparte algemene tabel.

Architectuurbeslissingen:

**BAF·b01** Autorisatieprofielen zijn alleen van toepassing op patiëntgegevens afkomstig uit dossiers van zorgpartijen, niet op gegevens uit publieke registers.

**BAF·b02** Autorisatieprofielen geven een inperking van bevoegdheden ten opzichte van die in het autorisatieprotocol.

**BAF·b03** Zorgverleners kunnen de autorisatieprofielen niet raadplegen, wegens de vertrouwelijkheid, zie paragraaf 5.6.

**BAF·b04** Zorgaanbieders kunnen de eventuele interne uitwisseling van patiëntgegevens regelen met interne autorisatieprofielen, die *niet* kunnen worden overgenomen van de landelijke autorisatieprofielen.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**BAF·s01** raadplegen autorisatieprofiel.

**BAF·s02** aanpassen akkoord.

**BAF·s03** aanpassen autorisatieprofiel.

**BAF·s04** vastleggen bewijs.

Bij gebruiksscenario [BAF·s01] *raadplegen autorisatieprofiel* gelden de volgende eisen en wensen:

**BAF·e01** De gebruiker moet het autorisatieprofiel van een patiënt/cliënt kunnen *raadplegen*, waarbij hij kan kiezen voor:

- de actuele situatie,
- een historische situatie, door invoer van een datum in het verleden.

Bij gebruiksscenario [BAF·s02] *aanpassen akkoord* gelden de volgende eisen en wensen:

**BAF·e02** De gebruiker moet voor alle patiënten/cliënten kunnen wijzigen:

- de verstekwaarde voor het wel/niet akkoord gaan met elektronische uitwisseling van zijn patiëntgegevens door zorgaanbieders,
- {toekomst} de verstekwaarde voor het wel/niet akkoord gaan met elektronisch inkijken in de toegangslag door hemzelf,
- {toekomst} de verstekwaarde voor het wel/niet akkoord gaan met elektronisch inkijken van zijn autorisatieprofiel door hemzelf,
- {toekomst} de verstekwaarde voor het wel/niet akkoord gaan met elektronisch wijzigen van zijn autorisatieprofiel door hemzelf.

**BAF·e03** De gebruiker moet voor een patiënt/cliënt kunnen wijzigen het wel/niet akkoord gaan met *elektronische uitwisseling van zijn patiëntgegevens door zorgaanbieders*, waarbij:

- in geval van “niet akkoord” de gebruiker vooraf wordt gewaarschuwd als de verwijzindex nog verwijzingen naar deze patiënt/cliënt bevat,
- in geval van “niet akkoord” na bevestiging van de gebruiker, die verwijzingen worden verwijderd uit de verwijzindex,
- in geval van “niet akkoord” voortaan alle aanmeldingen van zorgaanbieders worden geweigerd,
- in geval van “wel akkoord” voortaan alle aanmeldingen van zorgaanbieders worden toegevoegd aan de verwijzindex.
- wijziging door de patiënt/cliënt zelf wordt geëffectueerd aan het eind van de dag.

**BAF·e04** {toekomst} De gebruiker moet voor een patiënt/cliënt kunnen wijzigen het wel/niet akkoord gaan met *elektronisch inkijken in de toegangsllog door hemzelf*, waarbij:

- wijziging door de patiënt/cliënt zelf wordt geëffectueerd aan het eind van de dag.

**BAF·e05** {toekomst} De gebruiker moet voor een patiënt/cliënt kunnen wijzigen het wel/niet akkoord gaan met *elektronisch inkijken van zijn autorisatieprofiel door hemzelf*, waarbij:

- wijziging door de patiënt/cliënt zelf wordt geëffectueerd aan het eind van de dag.

**BAF·e06** {toekomst} De gebruiker moet voor een patiënt/cliënt kunnen wijzigen het wel/niet akkoord gaan met *elektronisch wijzigen van zijn autorisatieprofiel door hemzelf*, waarbij:

- wijziging door de patiënt/cliënt zelf wordt geëffectueerd aan het eind van de dag.

Bij gebruiksscenario [BAF·s03] *aanpassen autorisatieprofiel* gelden de volgende eisen en wensen:

**BAF·e07** De gebruiker moet het autorisatieprofiel van een patiënt/cliënt kunnen aanpassen door voor iedere combinatie van

- zorgpartij, eventueel uitgedrukt in functie of identiteit
- de gegevensklasse

de bevoegdheid tot toegang vast te leggen met:

- altijd
- alleen in noodsituatie
- {toekomst} na expliciete toestemming
- nooit
- ingangsdatum

zodanig dat de autorisatieregels in de opgegeven volgorde worden toegepast bij het opvragen en versturen van diens patiëntgegevens:

Bij gebruiksscenario [BAF·s04] *vastleggen bewijs* gelden de volgende eisen en wensen:

**BAF·e08** De gebruiker moet een juridisch geldig bewijs vastleggen (op papier of elektronisch) van het feit dat de patiënt/cliënt de nieuwe instellingen heeft gezien en daarmee uitdrukkelijk akkoord gaat.

Voor al deze gebruiksscenario's is het nodig dat de gebruiker heeft ingelogd als landelijke autorisatiebeheerder op vertrouwensniveau *midden*, zie gebruiksscenario [INL·s01]. Een

gebruiker die heeft ingelogd als lokale autorisatiebeheerder binnen een zorgaanbieder, kan gebruiksscenario [BAF·s03] uitvoeren voor interne profielen. In de toekomst kan een gebruiker die heeft ingelogd als patiënt/cliënt de gebruiksscenario's [BAF·s01], [BAF·s02] en [BAF·s03] uitvoeren op zijn eigen autorisatieprofiel.

Opmerkingen:

- Het niet akkoord gaan van een patiënt/cliënt met elektronische, landelijke uitwisseling van patiëntgegevens zoals vastgelegd in het autorisatieprofiel, moet niet worden verward met het *afschermen* van patiëntgegevens. *Afschermen* is bedoeld om specifieke patiëntstukken uit te sluiten van landelijke uitwisseling, zie ook paragraaf 4.6.
- Ad eis [BAF·e02] Wanneer het BSN wordt ingevoerd in de zorg, zal iedere burger daarover waarschijnlijk worden geïnformeerd per brief. Het is raadzaam de burger daarbij te vragen schriftelijk wel/niet akkoord te gaan met elektronische uitwisseling van patiëntgegevens. Bij voorkeur wordt "wel akkoord" als verstekwaarde gehanteerd, zie [Bedrijfsarchitectuur] paragraaf 9.2, toelichting op punt (d). De antwoorden van de burgers kunnen worden verwerkt door de autorisatiebeheerders in gebruiksscenario 5.2.
- Ad eis [BAF·e03] tot en met [BAF·e06] Het zou een te zware eis zijn, als wijzigingen via het Internet onmiddellijk moesten worden geëffectueerd. Tevens wordt enige drempel opgeworpen voor patiënten/cliënten die onvoorbereid wijzigingen doorvoeren en daarop onmiddellijk weer terugkomen met nieuwe inzichten. In geval van (c) is dat bovendien ter bescherming van hemzelf, want als de verwijzindex éénmaal is geleegd, kan deze niet meer hersteld worden.
- Ad eis [BAF·e05] Logischerwijze kan een patiënt/cliënt zelf via het Internet:
  - wel instellen dat hij *niet* akkoord gaat,
  - niet instellen dat hij *wel* akkoord gaat,met elektronisch wijzigen van zijn autorisatieprofiel door hemzelf. In het laatste geval zal de patiënt/cliënt zich moeten wenden tot de autorisatiemanager.
- Ad eis [BAF·e06] Een autorisatieregel koppelt een doelgroep aan een bevoegdheid. Autorisatieregels kunnen qua doelgroep elkaar (al dan niet deels) overlappen en kunnen qua bevoegdheid een tegengestelde werking hebben. Het op volgorde toepassen van overlappende autorisatieregels geeft daardoor de mogelijkheid tot verfijnde autorisatie met weinig regels.
- Ad eis [BAF·e06] Behalve zorgverleners kunnen ook medewerkers worden uitgesloten. Daartoe moet wel diens UZI-nummer bekend zijn. Medewerkers met een UZI-pas *niet op naam* hebben geen vast UZI-nummer, maar zij hoeven ook niet uitgesloten te worden, omdat zij überhaupt geen toegang tot *medische* patiëntgegevens krijgen.
- Ad eis [BAF·e07] Meestal zal een patiënt/cliënt een autorisatieregel onmiddellijk willen laten ingaan. Alleen in speciale gevallen zou hij een ingangsdatum willen instellen, bijv. in geval van verhuizing naar een andere woonplaats en dus voor een nieuwe huisarts.

Openstaande punten:

- Als *zorgpartij* kennen we voorlopig slechts zorgaanbieders, zorgverleners en medewerkers. Deze kunnen worden geïdentificeerd aan de hand van hun UZI-

abonnee-nr resp. UZI-nummer, voorzover ingeschreven bij het UZI-register. In de toekomst zijn andere zorgpartijen denkbaar, maar daarvoor moeten dan wel identificatie-nummers beschikbaar zijn.

- Ad eis [BAF.e02] Overwogen kan worden de patiënt/cliënt nog beter tegen zichzelf te beschermen, bijv. door de patiënt/cliënt per brief nog eens te informeren over de consequenties van het intrekken van het akkoord en pas na diens bevestiging de verwijfsindex te wissen.
- Ad eis [BAF.e02] Een patiënt/cliënt die pas later akkoord geeft, heeft op dat moment een nog lege verwijfsindex. Er is momenteel geen mechanisme gedefinieerd om historische aanmeldingen met terugwerkende kracht te doen uitvoeren.



## 4.14 Raadplegen toegangslog (RLO)

Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 9.3, moet de toezichthouder en een patiënt/cliënt kunnen (laten) achterhalen welke patiëntgegevens ooit landelijk (of eventueel intramuraal) zijn opgevraagd of verstuurd, door raadplegen van een toegangslog. Zo'n toegangslog zou als volgt kunnen worden gepresenteerd:

Toegangslog				datum dd-mm-jjjj		
Patiëntnr (BSN)		123456789	Geboorte datum		11-11-1911	
Geboorte naam		Jansen	Geboorte plaats		Amsterdam	
Agerende zorgpartij			Gebruikers-interactie	Datum / Tijd	Reagerende zorgpartijen	
Zorgaanbie..	Functie	Zorgverlener			Zorgaanbie..	Functie
J. Jansen	huisarts	J. Jansen	Opvragen medicatie voorschrift...	10:20...	P. Pietersen	huisarts
					Amstelziek...	internist
					Amstelziek...	cardioloog
J. Jansen	medew... namens huisarts	A. Arendsen	Opvragen medicatie verstrekki...	10:21...	Amstelapot...	apotheker
		J. Jansen			Veenapoth...	apotheker
					Maasapoth...	apotheker
J. Jansen	huisarts	J. Jansen	Versturen medicatie voorschrift	10:22...	Veenapoth...	apotheker
Veenapoth...	medew... namens apothek...	B. Berendsen	Versturen medicatie verstrekking	10:42...	J. Jansen	huisarts
		G. Gerritsen				

De toegangslog kan worden geraadpleegd door:

- logbeheerders die in opdracht van de toezichthouder periodiek willen nagaan *welke zorgaanbieders* mogelijk onrechtmatig patiëntgegevens hebben opgevraagd of verstuurd, dan wel dit ten onrechte hebben nagelaten.
- logbeheerders die in opdracht van de toezichthouder na verzoek van een patiënt/cliënt willen achterhalen *welke zorgverleners* patiëntgegevens over deze patiënt/cliënt hebben opgevraagd of ontvangen, bijv. bij vermoeden van onrechtmatige toegang of wanneer de patiënt zijn patiëntdossier wil laten vernietigen en dus wil achterhalen waar eventuele kopieën van die patiëntstukken liggen.
- zorgverleners/medewerkers die zelf willen achterhalen *welke patiëntgegevens* door andere zorgverleners/medewerkers zijn opgevraagd uit zijn patiëntdossier.
- zorgverleners/medewerkers die op verzoek van een patiënt/cliënt willen achterhalen *welke patiëntgegevens* over deze patiënt/cliënt door andere zorgverleners/medewerkers zijn opgevraagd uit het eigen patiëntdossier.
- patiënten/cliënten, wanneer zij beschikken over een geschikt elektronisch vertrouwensmiddel. De toegang blijft beperkt tot het deel dat hun eigen patiëntgegevens betreft.

Merk op dat de toezichthouder en zijn logbeheerders niet zijn geautoriseerd om patiëntgegevens inhoudelijk te bekijken. Als een patiënt/cliënt wil weten wat een andere zorgverlener/medewerker precies gezien heeft, zal hij zich moeten wenden tot de zorgaanbieder die verantwoordelijk is voor die patiëntgegevens. Hij zal een bericht-id nodig hebben om de onderhavige patiëntstukken precies te kunnen traceren.

De toegangslog bevat in principe alleen verkeersgegevens, geen patiëntgegevens. Toch is de inhoud van de toegangslog privacygevoelig. Denk aan de combinatie van patiënt-id, zorgverlener-functie (bijv. psychiater) en gegevenssoort (bijv. medicatie). Dit betekent dat een toezichthouder alleen met uitdrukkelijke toestemming van de patiënt voor hem de toegangslog mag laten raadplegen door een logbeheerder. Dit heeft als consequenties:

- als een patiënt de toezichthouder vraagt om raadpleging van de toegangslog, mag die toestemming worden verondersteld. Bij voorkeur zou de toezichthouder de aanvrager expliciet laten tekenen voor toestemming. In hoeverre deze zich daarbij moet vergewissen van de identiteit van de aanvrager, moet nader uitgezocht worden
- als de toezichthouder preventief, op eigen initiatief, verdachte opvraagpatronen wil laten onderzoeken door zijn logbeheerders, zal hij niet alle betrokken patiënten willen of kunnen vragen om toestemming. Dat is ook niet nodig als de geproduceerde rapportages slechts geanonimiseerde of gepseudonimiseerde gegevens bevatten. Pas bij sterke vermoedens van onrechtmatige opvraag hoeven de betrokken patiënten te worden gevraagd mee te werken aan nader onderzoek.

Een zorgaanbieder zal ook de eventuele interne uitwisseling van patiëntgegevens tussen afzonderlijke zorgverleners moeten loggen en ter beschikking van een toezichthouder moeten kunnen stellen. Dit speelt vooral voor grote zorginstellingen met verschillende gespecialiseerde afdelingen. Interne uitwisseling valt in principe buiten het werkkterrein van NICTIZ, maar het ligt voor de hand dergelijke eisen hier toch een plaats te geven.

Architectuurbeslissingen:

**RLO·b01** Logbeheerders krijgen alleen inzage in *verkeersgegevens*. Alleen de beheerverantwoordelijke zorgverlener en de patiënt/cliënt krijgen inzage in de *inhoudelijke* patiëntgegevens.

**RLO·b02** Logbeheerders moeten ook kunnen achterhalen of een zorgverlener een index van beschikbare gegevenssoorten heeft opgevraagd (gebruiksscenario [OPV·s01]) en welke gegevenssoorten van patiëntstukken ooit zijn aangemeld of afgemeld in de verwijfsindex (gebruiksscenario's onder [PUB]).

**RLO·b03** Logbeheerders mogen alleen voor een specifieke patiënt-id alle verkeersgegevens inzien. Anders mogen zij alleen geanonimiseerde of gepseudonimiseerde verkeersgegevens inzien.

**RLO·b04** Zorgaanbieders moeten zelf de eventuele *interne* uitwisseling van patiëntgegevens kunnen loggen.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**RLO·s01** opvragen *verkeersgegevens* over landelijk uitgewisselde patiëntstukken voor een specifieke patiënt/cliënt.

**RLO·s02** opvragen *inhoud van de patiëntstukken* die ooit door een bepaalde zorgaanbieder landelijk zijn uitgewisseld voor een specifieke patiënt/cliënt.

Bij gebruiksscenario [RLO·s01] gelden de volgende eisen en wensen:

**RLO·e01** De toegang tot logregels moet als volgt worden beperkt:

- een logbeheerder mag alle logregels inzien, mits geanonimiseerd, en na de bewaartermijn verwijderen,
- een zorgverlener mag alle logregels inzien en na de bewaartermijn verwijderen m.b.t. patiëntgegevens waarvoor hij verantwoordelijk is,
- een patiënt/cliënt mag alle logregels inzien m.b.t. patiëntgegevens over zichzelf.

**RLO·e02** De gebruiker moet een lijst van logregels kunnen oproepen, die per logregel de attributen kan tonen, zoals vermeld in paragraaf 5.8.

**RLO·e03** De gebruiker moet voor de lijst van logregels kunnen selecteren dat uitsluitend worden getoond:

- logregels met een bepaalde agerende zorgpartij,
- logregels met een bepaalde reagerende zorgpartij,
- logregels voor een bepaalde patiënt/cliënt, zie gebruiksscenario [SPA],
- logregels binnen een bepaald tijdvenster,
- logregels met bepaalde gebruikersinteracties,
- bepaalde attributen per logregel.

**RLO·e04** De gebruiker moet in de lijst van logregels:

- kunnen bladeren,
- kunnen bepalen volgens welk attribuut de logregels op volgorde worden gezet,
- kunnen zoeken naar logregels met een aangegeven waarde voor één of meer van de attributen,
- een te selecteren deel van de logregels kunnen afdrukken,
- een te selecteren deel van de logregels kunnen exporteren naar een intelligent analysegereedschap.

**RLO·e05** De gebruiker moet logregels:

- tot een instelbare bewaartermijn kunnen raadplegen,
- na die instelbare bewaartermijn kunnen verwijderen.

**RLO·e06** De gebruiker moet voor een bepaalde patiënt/cliënt:

- logregels jonger dan 3 maanden binnen 5 seconden kunnen oproepen,
- logregels ouder dan 3 maanden binnen 1 uur kunnen oproepen.

**RLO·e07** De gebruiker moet de zekerheid hebben:

- dat eenmaal aan de toegangslog toegevoegde logregels niet meer kunnen worden gewijzigd of verwijderd voor het einde van de bewaartermijn,
- dat eenmaal na de bewaartermijn verwijderde logregels geen onbedoelde sporen nalaten.

Bij gebruiksscenario [RLO·s02] gelden de volgende eisen en wensen:

**RLO·e08** { toekomst} De gebruiker moet op basis van een bericht-id de inhoud van het bericht kunnen raadplegen, binnen 1 dag.

Voor gebruiksscenario [RLO·s01] is het nodig dat de gebruiker heeft ingelogd als logbeheerder, zorgverlener, gemandateerde medewerker of { toekomst} patiënt/cliënt op vertrouwensniveau *midden*, zie gebruiksscenario [INL·s01]. Voor gebruiksscenario [RLO·s02] is het nodig dat de gebruiker heeft ingelogd als zorgverlener, gemandateerde medewerker of { toekomst} patiënt/cliënt (zie gebruiksscenario) op vertrouwensniveau *midden*, zie gebruiksscenario [INL·s01].

Opmerkingen:

- In paragraaf 5.8 zal blijken dat er een *centrale* toegangslag bij het schakelpunt moet komen en *lokale* toegangslags bij de zorgaanbieders. Dat is een architectuurbeslissing die in principe niet relevant is voor de alhier beschreven gebruiksscenario's, behalve dat een lokale toegangslag minder logregels en minder attributen per logregel bevat, zie hieronder.
- Ad eis [RLO·e01] de logbeheerder moet *alle* logregels zoals gelogd door het schakelpunt kunnen inzien, de zorgverlener *alleen* de logregels die betrekking hebben op patiëntgegevens uit zijn dossiers, de patiënt/cliënt *alleen* de logregels die betrekking hebben op zichzelf.
- Ad eis [RLO·e01] en [RLO·e03] Hoewel een logbeheerder alleen geanonimiseerde logregels (dus zonder vermelding van patiënt-id of andere identificerende gegevens) mag inzien, moet de logbeheerder op verzoek van de toezichthouder toch de logregels voor één specifieke patiënt/cliënt kunnen selecteren. Daarbij zal de toezichthouder bepaalde identificerende gegevens moeten overhandigen aan de logbeheerder.
- Ad eis [RLO·e02] de zorgverlener(s) als onderdeel van de reagerende zorgaanbieder kan zijn:
  - (in geval van versturen) de zorgverlener voor wie de verstuurd patiëntgegevens bestemd zijn, zoals vermeld in het opdrachtbericht,
  - (in geval van opvragen) de zorgverlener(s) die verantwoordelijk zijn voor de opgeleverde patiëntgegevens, zoals vermeld in de opleverberichten, maar in de praktijk zijn deze velden vaak leeg.
- Ad eis [RLO·e02] Niet alle attributen kunnen door de zorgaanbiederapplicatie worden gelogd. De attributen die niet kunnen worden gelogd zijn voor de zorgverlener ook niet zichtbaar.
- Ad eis [RLO·e02] In geval van *opvragen index* is er geen sprake van een bepaalde gegevenssoort, maar wordt *index* vermeld. Dergelijke logregels kunnen alleen door het schakelpunt worden gelogd.
- Ad eis [RLO·e05] De bewaartermijn van logregels is nog niet vastgesteld. Daarom is deze instelbaar gemaakt. Deze bewaartermijn heeft overigens weinig te maken met de wettelijke bewaartermijn van patiëntgegevens, zie [Bedrijfsarchitectuur] paragraaf 7.1. Immers een logregel kan betrekking hebben op een opvraag die patiëntgegevens van 1 dag oud en patiëntgegevens van bijna 15 jaar oud heeft opgeleverd. Het lijkt onwaarschijnlijk dat de bewaartermijn van de toegangslag langer wordt dan de bewaartermijn van patiëntgegevens. Daarom mag een maximum van 15 jaar worden aangehouden.

- Ad eis [RLO·e06] Voor het oplossen van operationele en technische problemen (zie onder meer gebruiksscenario 6) moeten de logregels van de laatste 3 maanden on-line raadpleegbaar blijven. Voor het achterhalen van al dan niet rechtmatige toegang tot patiëntgegevens moet men verder terug in de tijd kunnen, maar laat de responstijd toe oudere logregels op een off-line medium te archiveren en off-line te doorzoeken (bijv. door een verzameling DVD-schijfjes één voor één te laden en te doorzoeken).
- Ad eis [RLO·e02] en [RLO·e08] Als gevolg van foutsituaties (autorisatie, onbereikbare patiëntdossiers, etc.) kan het opvragen of versturen van patiëntstukken geheel of deels mislukken. Bij een gedoseerde opvraag kan de opvragende zorgaanbieder bovendien de stroom opleverberichten tussentijds afbreken. Daarom is het belangrijk te weten welke indexregels en patiëntstukken daadwerkelijk zijn verzonden aan een zorgaanbieder.
- Ad eis [RLO·e05] Bij vernietiging van een patiëntdossier zouden idealiter ook alle referenties naar dat dossier vanuit de toegangslog worden verwijderd. In de praktijk zal dit nauwelijks realiseerbaar zijn als toegangslog zal worden gearchiveerd op een off-line medium.
- Ad eis [RLO·e07] De mate van zekerheid m.b.t. de volledigheid van de toegangslog moet in verhouding staan tot de mate van onweerlegbaarheid van de inhoud, zoals moet blijken in de juridische praktijk.
- Ad eis [RLO·e08] Deze eis pakt verschillend uit voor het schakelpunt resp. de zorgaanbieder, zie ook paragraaf 5.8:
  - het schakelpunt als bron van indexregels moet berichten met indexregels inhoudelijk loggen,
  - {toekomst} zorgaanbieders moeten berichten met patiëntgegevens inhoudelijk loggen.
 Merk op dat hiervoor een ruime responstijd geldt.

#### Openstaande punten:

- De bevoegdheden van de toezichthouder en diens logbeheerders worden idealiter wettelijk vastgesteld en anders geregeld in een bewerkersovereenkomst tussen het LSP en de aangesloten zorgaanbieders. Afhankelijk van de uiteindelijke wettelijke bevoegdheden kan het in de toekomst nodig zijn de toegang van de logbeheerders geheel te beperken tot gepseudonimiseerde verkeersgegevens.
- De toezichthouders en zijn logbeheerders zijn noch zorgverlener, noch medewerker van een zorgaanbieder. Zij zullen daarom geen UZI-pas kunnen krijgen. In plaats daarvan zullen voor hen andere waarborgen op vertrouwensniveau *midden* nodig zijn.
- Zorgaanbieder kunnen een interne logbeheerder aanstellen, bijv. om de zorgverleners te ontlasten van verzoeken van patiënten/cliënten tot inzage in de toegangslog. Binnen AORTA is deze rol (nog) niet onderkend. Niettemin kunnen zorgverleners een medewerker mandateren tot inzage in de toegangslog.
- De toegangslog is niet bedoeld voor de systeembeheerder om het berichtenverkeer te bewaken, ook al bevat de toegangslog voor hem zeer bruikbare gegevens. Wellicht is het nodig zijn om gebruiksscenario's te definiëren voor een dergelijke systeembeheerder.

## 4.15 Bijhouden mandateringen (BMD)

Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 9.4, moet een zorgverlener als hoofdbehandelaar kunnen vastleggen in een mandateringstabel welke andere zorgverleners (als medebehandelaar) en/of medewerkers (met UZI-pas op naam) zijn gemandateerd om namens hem landelijk patiëntgegevens uit te wisselen. De gemandateerde zorgverlener of medewerker geniet dan de bevoegdheden van de mandaterende zorgverlener, zoals bepaald in het autorisatieprotocol. Om te voorkomen dat een zorgverlener een uitsluiting door een patiënt/cliënt kan omzeilen door zijn medewerker te mandateren, zal de voor gemandateerde ook de eventuele uitsluitingen van de mandaterende, zoals vastgelegd in autorisatieprofielen, moeten gelden.

Zo'n mandateringstabel zou er als volgt kunnen uitzien:

<i>Mandaterende:</i>					
<i>Naam:</i>	<i>Functie:</i>				
Jacobsen	Arts, internist				
	<i>Gebruikers-interactie:</i>	Publiceren medicatie voorschrift	Opvragen medicatie voorschrift	Versturen medicatie voorschrift	...
<i>Gemandateerde:</i>					
<i>Naam:</i>	<i>Functie:</i>				
Jansen	Arts, internist	V	V	V	...
Gerritsen	Arts, basisarts	V	V	V	...
Pietersen	medewerker		V		...
Willemsen	medewerker		V		...
...	...	...	...	...	...

In het bovenstaande voorbeeld mandeert een internist:

- een collega internist resp. een basisarts (bijv. een arts in opleiding) tot het landelijk aanmelden, afmelden, opvragen en versturen,
- twee medewerkers (bijv. co-assistenten) tot alleen landelijk opvragen van patiëntgegevens.

De mandaterende zorgverlener blijft verantwoordelijk voor de handelingen van de door hem gemandateerde medebehandelaren en medewerkers. Daarom is het belangrijk dat de mandaterende zorgverlener goed grip houdt op zijn mandateringen, zonder onnodige rompslomp. Zo zal een zorgverlener zijn vaste medewerkers voor onbepaalde tijd willen mandateren. Voor tijdelijke medewerkers zal hij een verlooptijd willen specificeren.

Architectuurbeslissingen:

- BMD-b01** Een zorgverlener kan een andere zorgverlener of medewerker van dezelfde zorgaanbieder mandateren om namens hem landelijk patiëntgegevens uit te wisselen, waarbij de gemandateerde krijgt overgedragen resp. opgelegd:
- één of meer bevoegdheden van de mandaterende, zoals hij geniet op grond van zijn zorgverlener-functie, zoals bepaald in het autorisatieprotocol,
  - de uitsluitingen van de mandaterende door patiënten/cliënten, zoals vastgelegd in autorisatieprofielen.

**BMD·b02** Alleen zorgverleners als hoofdbehandelaar worden in staat gesteld tot het vastleggen, raadplegen, wijzigen en verwijderen van hun eigen mandateringen. Daarnaast krijgen alleen gemandateerde medebehandelaren en medewerkers inzage in de aan hen toegekende mandateringen.

**BMD·b03** Omdat men door verscheidene zorgverleners kan worden gemandateerd, zal bij het uitoefenen van een gemandateerde bevoegdheid moeten worden aangeven (automatisch door de applicatie of handmatig door de gebruiker) namens wie een gemandateerde medebehandelaar of medewerker handelt.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**BMD·s01** *bijwerken mandateringen.*

**BMD·s02** *inzien mandateringen.*

Bij gebruiksscenario [BMD·s01] *bijwerken mandateringen* gelden de volgende eisen en wensen:

**BMD·e01** De gebruiker moet hebben ingelogd als zorgverlener op vertrouwensniveau *midden*, zie gebruiksscenario [INL·s01].

**BMD·e02** De gebruiker moet namens hemzelf een nieuwe mandatering kunnen vastleggen door het kiezen van:

- de identiteit van te mandateren zorgverlener of medewerker,
- de bevoegde medische gebruikersinteractie(s), zie [Technische Architectuur] paragraaf 4.1,
- een ingangsdatum,
- eventueel een verloopdatum

en het automatisch overnemen uit het vertrouwensmiddel van de gebruiker:

- de identiteit van de mandaterende zorgverlener waarbij verzekerd wordt dat de mandaterende en gemandateerde tot dezelfde zorgaanbieder behoren.

**BMD·e03** De gebruiker moet een lijst van alle door hemzelf vastgelegde mandateringen kunnen raadplegen.

**BMD·e04** De gebruiker moet uitsluitend een door hemzelf vastgelegde mandatering kunnen wijzigen.

**BMD·e05** De gebruiker moet uitsluitend een door hemzelf vastgelegde mandatering kunnen verwijderen.

Bij gebruiksscenario [BMD·s02] *inzien mandateringen* gelden de volgende eisen en wensen:

**BMD·e06** De gebruiker moet hebben ingelogd als zorgverlener of medewerker op vertrouwensniveau *midden*, zie gebruiksscenario [INL·s01].

**BMD·e07** De gebruiker moet een lijst van alle aan hem toegekende mandateringen kunnen raadplegen.

**BMD·e08** De gebruiker moet een mandaterende zorgverlener kunnen kiezen als hoofdbehandelaar namens wie hij patiëntgegevens gaat beheren of uitwisselen.

Opmerkingen:

- Afhankelijk van de zorgtoepassing, zou gebruiksscenario 7.2 automatisch kunnen volgen op het inloggen van een medewerker of automatisch voorafgaan aan een poging tot het landelijk uitwisselen van patiëntgegevens. Het is ook denkbaar dat een applicatie op grond van het BSN van de onderhavige patiënt automatisch kan bepalen wie de hoofdbehandelaar is en namens wie de medewerker dus moet handelen. Dit is belangrijk voor een gezondheidscentrum, waar een medewerker door verscheidene huisartsen gemandateerd kan worden, maar afhankelijk van de bellende patiënt altijd één mandaterende huisarts moet kiezen.
- Ad eis [BMD·b01] Een medewerker van een zorgaanbieder kan ook zelf worden uitgesloten door een patiënt/cliënt in zijn autorisatieprofiel. Een gemandateerde medewerker geniet dus behalve de uitsluitingen van de mandaterende zorgverlener ook de eigen uitsluitingen.
- Ad eis [BMD·e02] De met de UZI-pas ingelogde zorgverlener is dus automatisch de mandaterende zorgverlener. Het is dus niet mogelijk dat een lokale beheerder even alle mandateringen regelt, want een zorgverlener wordt zelf persoonlijk aangesproken als een gemandateerde medewerker onrechtmatig patiëntgegevens opvraagt. Wel is het denkbaar dat een zorginstelling-verantwoordelijke alle mandateringen voorbereidt, zodat een mandaterende zorgverlener deze slechts met een druk op de knop hoeft te bekrachtigen. Dit is belangrijk voor een HAP, waar veel medewerkers door veel waarnemende huisartsen gemandateerd moeten worden.



## 4.16 Aan/afsluiten zorgaanbiederapplicatie m.b.t. schakelpunt (ASL)

Nadat een zorgaanbiederapplicatie eenmaal is gekoppeld aan het schakelpunt, zie paragraaf 4.17, kunnen andere applicaties via het schakelpunt in principe berichten sturen naar deze zorgaanbiederapplicatie. Dat is echter niet altijd gewenst, bijvoorbeeld wanneer de applicatie nog niet operationeel is bij de zorgaanbieder, of in onderhoud gaat, etc.

Daarom moet men een zorgaanbiederapplicatie kunnen aansluiten op, en afsluiten van, het schakelpunt. Daartoe moet de beheerder melden aan het schakelpunt wat de beschikbaarheidstoestand van die applicatie is. Deze toestand omvat:

- *koppeldoestand* die aangeeft of de applicatie op de *operationele* ZIM, de *uitwijk*-ZIM of de *test*-ZIM wordt aangesloten, zie het document [Technische Architectuur] onder *aansluiting van applicatie op schakelpunt*,
- *actiemodus* die aangeeft of de applicatie *actief* is om berichten uit te wisselen en te verwerken, *gereed* is om actief te worden, dan wel gepland in *onderhoud* is of onverhoopt in *storing* is, zie het document [Technische Architectuur] onder *beschikbaarheidstoestanden*.

Idealiter stuurt de applicatie een bericht naar het schakelpunt voor iedere toestandsverandering. Het schakelpunt weet dan of die applicatie wel of niet beschikbaar is om berichten te verwerken. In geval van storing zal een applicatie dat vaak niet meer kunnen melden. In geval van onderhoud kan de beheerder erbij vermelden hoe lang het gaat duren.

Echter, voor toestandsveranderingen zijn nog geen berichten gedefinieerd. Aldus zal de applicatiebeheerder dergelijke toestandsveranderingen voorlopig telefonisch moeten melden aan de schakelpuntbeheerders, waarna zij de nieuwe toestand handmatig kunnen vastleggen. De eisen in deze paragraaf zijn daarom allemaal voorzien van het etiket {toekomst}.

Ontwerpbeslissingen:

**ASL·b01** De beheerder van een zorgapplicatie meldt een nieuwe beschikbaarheidstoestand telefonisch of per e-mail aan de beheerders van het schakelpunt.

**ASL·b02** {toekomst} Een zorgapplicatie meldt aan het schakelpunt een nieuwe beschikbaarheidstoestand door het sturen van een bericht over een beveiligde verbinding die is opgezet met het systeemvertrouwensmiddel.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**ASL·s01** aansluiten applicatie op schakelpunt,

**ASL·s02** schakelpunt legt verbinding met applicatie,

**ASL·s03** afsluiten applicatie van schakelpunt.

Bij gebruiksscenario [ASL-s01] *aansluiten op schakelpunt* gelden de volgende eisen en wensen:

**ASL-e01** { toekomst } De gebruiker moet voor zijn zorgaanbiederapplicatie de volgende stuurparameters kunnen instellen:

- koppeltoestand: operationeel, uitwijk of test,
- actiemodus: gereed, actief, onderhoud of storing,

**ASL-e02** { toekomst } De gebruiker moet zijn applicatie kunnen aansluiten op het schakelpunt door:

- het opzetten van een beveiligde verbinding op basis van het systeemgebonden vertrouwensmiddel,
- en het sturen van een toestandsbericht met de actiemodus *actief*,

Bij gebruiksscenario [ASL-s02] *schakelpunt legt verbinding met applicatie* gelden de volgende eisen en wensen:

**ASL-e03** De zorgapplicatie moet na aansluiten op het schakelpunt toestaan dat het schakelpunt een beveiligde verbinding opzet.

Bij gebruiksscenario [ASL-s03] *afsluiten van schakelpunt* gelden de volgende eisen en wensen:

**ASL-e04** { toekomst } De gebruiker moet zijn applicatie kunnen afsluiten van het schakelpunt door:

- het opzetten van een beveiligde verbinding op basis van het systeemgebonden vertrouwensmiddel,
- het sturen van een toestandsbericht met de volgende gegevens:
  - de nieuwe actiemodus, *onderhoud* of *storing*,
  - reden van afsluiten,
  - verwachte tijdstip van weer beschikbaar zijn,
- het afsluiten van de beveiligde verbinding.

Voor gebruiksscenario [ASL-s01] en [ASL-s03] is het nodig dat de gebruiker heeft ingelogd als beheerder.

Opmerkingen:

- Ad eis [ASL-e01] Door het instellen van de koppeltoestand wordt bepaald op welke ZIM (operationele ZIM, test-ZIM of uitwijk-ZIM) zal worden aangesloten.
- Ad eis [ASL-e02] Het melden van de actiemodus aan het schakelpunt kan in de toekomst worden gecombineerd met het synchroniseren van allerlei stuurparameters uit het schakelpunt.
- Ad eis [ASL-e03] Dit is eigenlijk geen gebruikersscenario, maar iets dat optreedt als onderdeel van andere scenario's.
- Ad eis [ASL-e04] De beheerder kan behalve onderhoud ook een storing van zijn zorgaanbiederapplicatie melden. Dat moet dan vermoedelijk geschieden met een andere applicatie.

- Het kunnen verzenden van een toestandsbericht over een beveiligde verbinding op basis van het systeemgebonden vertrouwensmiddel, geeft de mogelijkheid dat een beheerder zonder UZI-pas, maar wel met een lokaal vertrouwensmiddel, deze taken kan uitvoeren.

## 4.17 Beheren zorgaanbiederapplicatie (BZA)

Voordat een zorgaanbiederapplicatie kan worden aangesloten op een schakelpunt, zie paragraaf 4.16, moet het volgende gebeuren:

- het zorgsysteem waarvan deze applicatie onderdeel uitmaakt, moet na goedkeuring als GBZ, eenmalig worden gekoppeld aan de ZIM door het wederzijds vastleggen van GBZ-id, URI en andere configuratieparameters, zie ook paragraaf 4.18 eis [BSC·e16], waarna het GBZ kan worden opengesteld door de schakelpuntbeheerder, zie eis [BSC·e15].
- de aan te sluiten zorgapplicatie moet vervolgens eenmalig worden voorzien van een applicatie-id en worden geassocieerd met een UZI-servicescertificaat in het GBZ, die tezamen met andere configuratieparameters worden vastgelegd in het schakelpunt, zie paragraaf 4.18 eis [BSC·e16].

Omdat een zorgaanbiederapplicatie naar keuze moet kunnen worden aangesloten op de operationele ZIM, de uitwijk-ZIM of de test-ZIM, zie [Technische Architectuur] paragraaf 7.2, moeten de bovenstaande koppelingen in principe voor alle ZIM's worden geconfigureerd.

Daarnaast moet per applicatie worden vastgelegd welke toepassingsrollen worden geactiveerd. Immers, een bepaalde applicatie kan zijn gekwalificeerd voor zowel WDH als EMD, terwijl de huisarts aanvankelijk slechts WDH wil activeren. Tenslotte kunnen bereikbaarheidsgegevens van de beheerder van het GBZ of de applicatie worden ingevoerd.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**BZA·s01** koppelen van een GBZ aan een ZIM.

**BZA·s02** koppelen van een applicatie aan een schakelpunt.

Bij gebruiksscenario [BZA·s01] *koppelen GBZ aan ZIM* gelden de volgende eisen en wensen:

**BZA·e01** De gebruiker moet de volgende configuratieparameters kunnen instellen voor zijn GBZ:

- GBZ-id,
- URI en hostnaam van het GBZ,
- URI en hostnaam van de operationele ZIM,
- URI en hostnaam van de test ZIM,
- URI en hostnaam van de uitwijk ZIM,
- naam van het GBZ zoals bekend bij de zorgaanbieder,
- naam van de zorgaanbieder,
- abonneenummer van de zorgaanbieder in het UZI-register,
- E-mailadres van de beheerder,
- telefoonnummer van de beheerder.

Bij gebruiksscenario [BZA·s01] *koppelen applicatie aan schakelpunt* gelden de volgende eisen en wensen:

**BZA·e02** De gebruiker moet binnen zijn GBZ verscheidene zorgapplicaties kunnen toevoegen en verwijderen, en daarvoor de volgende configuratieparameters kunnen instellen per zorgapplicatie:

- applicatie-id van de zorgapplicatie,
- applicatie-id van het operationele schakelpunt waarop kan worden aangesloten,
- applicatie-id van het test-schakelpunt waarop kan worden aangesloten,
- applicatie-id van het uitwijk-schakelpunt waarop kan worden aangesloten,
- UZI-nr van het UZI-servicescertificaatwaarmee het is geassocieerd,
- fabrikaat en type van de zorgapplicatie,
- naam van de zorgapplicatie zoals bekend bij de zorgaanbieder,
- naam van de zorgaanbieder,
- E-mailadres van de beheerder,
- telefoonnummer van de beheerder,
- toepassingsrollen die worden geactiveerd,
- HL7v3-conformancetabel van de zorgapplicatie,
- HL7v3-release gebruikt door de zorgapplicatie.

Voor al deze gebruiksscenario's is het nodig dat de gebruiker heeft ingelogd als beheerder.

Opmerkingen:

- Als het gehele GBZ slechts één beheerder heeft, kunnen diens bereikbaarheidsgegevens bij [BZA·e01] worden opgegeven. Als iedere applicatie een afzonderlijke beheerder heeft, kunnen diens bereikbaarheidsgegevens bij [BZA·e02] worden opgegeven. Combinaties van beide zijn ook mogelijk. Een applicatie kan deze gegevens meegeven in de Transport Wrapper van HL7v3-berichten. In de toekomst zouden deze gegevens eventueel automatisch bij (de eerste) aansluiting op de ZIM kunnen worden doorgegeven aan de ZIM in een toestandsbericht.
- De naam van de zorgaanbieder, moet altijd worden meegegeven in de ControlAct Wrapper van HL7v3-berichten. Deze naam is gewoonlijk voor het gehele GBZ hetzelfde, maar er kan de behoefte zijn om per applicatie bijv. de naam van de afdeling toe te voegen. Idealiter komt deze naam overeen met die in de zorgaanbiedergids.

## 4.18 Beheren schakelpunt (BSC)

Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 12.2, moet een schakelpuntbeheerder de goede werking van de schakelpunten en alle daarop aangesloten objecten kunnen bewaken en besturen. In theorie heeft ieder beheerobject *variabelen* die kunnen worden bewaakt en *parameters* die kunnen worden bestuurd. Beheerders kunnen worden gealarmeerd door grenswaarden op variabelen te zetten.

Zoals zal blijken in hoofdstuk 5 vallen sommige objecten binnen een DCN of een GBZ en vallen ze daarmee onder besturing van netwerkdienstverleners of zorgaanbieders. De *aansluitingen* van de GBZ'en en DCN'en op de ZIM's liggen in beide besturingsdomeinen:

- Om te kunnen aansluiten, moeten het GBZ en de ZIM elkaars hostnamen en eventueel elkaars URI kennen. Daartoe moeten de schakelpuntbeheerder en de zorgaanbieder elkaars configuratieparameters in hun eigen systeem invoeren.
- Om daadwerkelijk aan te sluiten, moet de schakelpuntbeheerder de koppeling openstellen, na verificatie dat de ZIM inderdaad een GBZ-status heeft. Daarna kan de zorgaanbieder zijn GBZ pas communiceren met de ZIM.

De schakelpuntbeheerder kan de GBZ'en en DCN'en alleen indirect beïnvloeden, bijv. door telefonisch aanwijzingen te geven aan die andere beheerders, bijv. om een GBZ opnieuw te laten synchroniseren met de verwijzindex. Daartoe moet de schakelpuntbeheerder die andere objecten wel kunnen bewaken, bijv. door het bijhouden van foutentellers van ieder GBZ. Merk op dat er naast de operationele ZIM ook een uitwijk-ZIM en een test-ZIM kunnen zijn.

Binnen een GBZ kunnen meerdere applicaties draaien, zie het document [Technische Architectuur] onder *capaciteit en schaalbaarheid*. Die applicaties kunnen afzonderlijk worden aangesloten op het schakelpunt. Alle aangesloten objecten moeten een uniek ID hebben. Hoewel zorgaanbieders zelf zouden kunnen zorgen voor unieke GBZ-id's en applicatie-id's, is het veiliger de schakelpuntbeheerder deze ID's te laten uitgeven.

Architectuurbeslissingen:

**BSC·b01** De schakelpuntbeheerder moet de ZIM's en alle daarop aangesloten DCN'en en GBZ'en kunnen *bewaken*.

**BSC·b02** De schakelpuntbeheerder moet de ZIM kunnen *configureren* en *besturen* tot en met het openstellen dan wel blokkeren van afzonderlijke koppelingen met DCN'en en GBZ'en.

**BSC·b03** Een zorgaanbieder moet een GBZ kunnen bewaken, besturen en configureren tot en met het aansluiten van het GBZ op de ZIM via een DCN en het eventueel afsluiten daarvan.

**BSC·b04** De schakelpuntbeheerder geeft voor ieder aan te sluiten GBZ en iedere applicatie een uniek GBZ-id resp. applicatie-id uit.

Hier zijn aldus de volgende gebruiksscenario's te onderkennen:

**BSC·s01** beheren ZIM.

**BSC·s02** beheren DCN-koppeling aan ZIM.

**BSC·s03** beheren GBZ-koppeling aan ZIM.

**BSC·s04** beheren alarmmeldingen.

Bij alle gebruiksscenario's gelden de volgende eisen en wensen:

**BSC·e01** Bij het oproepen van een overzicht van variabelen van beheerobjecten, moet de gebruiker kunnen kiezen uit:

- *actuele* waarden: lopende gemiddelden/totalen over een instelbaar dynamisch tijdsinterval (bijv. seconde, minuut, uur).
- *historische* waarden: gerealiseerde gemiddelden/totalen over een instelbaar historisch tijdsinterval (bijv. jaar, maand, week, dag).

**BSC·e02** Bij het oproepen van een overzicht van variabelen van beheerobjecten, moet de gebruiker kunnen kiezen uit:

- *grafiek*: grafische presentatie van het verloop van de actuele of historische waarden van te kiezen variabelen over een instelbaar tijdsinterval.
- *tabel*: tabellarische presentatie van het verloop van de historische waarden van te kiezen variabelen over een instelbaar tijdsinterval met instelbare tussenstappen (bijv. alle maandelijkse waarden van een jaar).
- *diagram*: presentatie van een statisch diagram (dat bijv. de aansluiting van een GBZ voorstelt) waarin de actuele waarden van te kiezen variabelen dynamisch worden gepresenteerd, in de kleur die overeenkomt met de eventuele alarmtoestand, zie gebruiksscenario 6.4.
- *log*: chronologische lijst van gewijzigde variabelen, waarbij in geval van stuurparameters of configuratieparameters wordt vermeld welke gebruiker op welk tijdstip welke wijziging heeft doorgevoerd.

**BSC·e03** Na het oproepen van een overzicht van variabelen van beheerobjecten, moet de gebruiker kunnen kiezen voor:

- *export*: vastleggen van geselecteerde historische waarden in een exportbestand dat kan worden geladen in een intelligent analyse-gereedschap.
- *rapportage*: vastleggen van het gepresenteerde in een rapport, dat kan worden opgeslagen, teruggehaald, gepresenteerd, afgedrukt en per E-mail verstuurd.

Bij gebruiksscenario [BSC·s01] *beheren ZIM* gelden de volgende eisen en wensen:

**BSC·e04** De gebruiker moet een overzicht kunnen oproepen van de volgende *variabelen* voor iedere geconfigureerde ZIM:

- beschikbaarheid van deze ZIM,
- aantal GBZ'en dat:
  - geconfigureerd is voor aansluiting op de ZIM,
  - daadwerkelijk is aangesloten op de ZIM,
- aantal gebruikers dat:
  - nieuw heeft ingelogd,
  - vergeefs heeft geprobeerd in te loggen,

- actief ingelogd is,
  - zojuist heeft uitgelogd,
  - gebruikte on-line opslagruimte door de:
    - berichtenwachtrij,
    - toegangslog,
    - autorisatielog,
    - systeemlog,
    - alarmlog.
  - tijdstip van de laatste volledige resp. incrementele backup,
  - alle stuurparameters en configuratieparameters voor deze ZIM,
- en de volgende variabelen voor ieder afzonderlijk schakelpunt binnen deze ZIM, plus de totalen/gemiddelden over alle schakelpunten van deze ZIM indien zinvol:
- beschikbaarheid van het schakelpunt, zie [Technische Architectuur] paragraaf 9.4,
  - per gebruikersinteractie:
    - aantal interacties per seconde,
    - aantal mislukte interacties, uitgesplitst naar foutsoort,
    - aantal interacties dat via een ander schakelpunt afgehandeld moest worden,
    - gemiddeld aantal uitgewisselde patiëntstukken per interactie,
    - gemiddeld aantal uitgewisselde bytes per interactie,
    - minimum, gemiddelde en maximum responstijd,
  - aantal applicaties dat:
    - geconfigureerd is voor aansluiting op het schakelpunt,
    - daadwerkelijk aangesloten is op het schakelpunt,
  - alle stuurparameters en configuratieparameters van dit schakelpunt.

**BSC·e05** De gebruiker moet de volgende *stuurparameters* kunnen instellen voor iedere geconfigureerde ZIM:

- status van de koppeling van deze ZIM met andere ZIM's:
  - opengesteld,
  - geblokkeerd,
- bereikbaarheid van de ZIM, zie [Technische Architectuur] paragraaf 9.4,
- beschikbare on-line opslagruimte voor de:
  - berichtenwachtrij,
  - toegangslog,
  - autorisatielog,
  - systeemlog,
  - alarmlog,
  - parametertabel, zie paragraaf 5.14,
- maximum aantal gelijktijdige SSL/TLS-sessies met een GBZ-gebruiker (gebruikerssessies) per GBZ,
- en de volgende stuurparameters kunnen instellen voor iedere afzonderlijk schakelpunt, dan wel voor alle schakelpunten tegelijk indien zinvol:
- beschikbaarheid van het schakelpunt, zie [Technische Architectuur] paragraaf 9.4,
- actiemodus van het schakelpunt, zie [Technische Architectuur] paragraaf 9.4,
- per gegevenssoort:
  - maximum aantal patiëntstukken dat het schakelpunt per opvraag zal opleveren aan een opvragende applicatie,



- maximum aantal patiëntstukken dat het schakelpunt per opvraag zal opvragen bij een achterliggende applicatie,
- tijdsinterval na een aanmelding bij de verwijfsindex, waarbinnen de applicatie nieuwe patiëntgegevens niet opnieuw hoeft aan te melden,
- maximum tijdsinterval dat het schakelpunt wacht op een opleverende applicatie, voordat het schakelpunt een foutmelding teruggeeft aan de opvragende applicatie,
- maximum tijdsinterval dat het schakelpunt wacht op een ontvangstbevestiging, voordat het schakelpunt een foutmelding teruggeeft aan de versturende applicatie.

**BSC·e06** { toekomst } De gebruiker moet een nieuw ingestelde actiemodus van een schakelpunt kunnen melden aan alle aangesloten applicaties door het sturen van een bericht met de volgende gegevens:

- de nieuwe modus, zie [Technische Architectuur] paragraaf 9.4,
- in geval van *onderhoud* met vermelding van:
  - tekstuele toelichting,
  - verwachte tijdstip van weer beschikbaar zijn.

**BSC·e07** De gebruiker moet binnen iedere ZIM schakelpunten kunnen toevoegen en verwijderen, en voor de ZIM de volgende *configuratieparameters* kunnen instellen:

- URI,
- E-mailadres van de schakelpuntbeheerder,
- telefoonnummer van de schakelpuntbeheerder,

en voor ieder afzonderlijk schakelpunt:

- applicatie-id,
- naam van het schakelpunt zoals gebezigd door de beheerders,
- ondersteunde toepassingsrollen,
- HL7v3 conformancetabel,
- gebruikte HL7v3-release.

**BSC·e08** De gebruiker moet voor iedere ZIM de volgende acties kunnen ondernemen m.b.t. de verwijfsindex:

- verwijderen van alle verwijfsingen naar een bepaalde applicatie van een bepaald GBZ,
- synchroniseren met de verwijfsindices van de andere ZIM's,
- kopiëren van de inhoud van de verwijfsindex van een andere ZIM.

**BSC·e09** De gebruiker moet voor iedere ZIM de volgende acties kunnen ondernemen m.b.t. de logboeken (toeganglog, autorisatielog, systeemlog, alarmlog):

- archiveren van de logboeken op een off-line opslagmedium,
- terughalen van (een deel van) een logboek naar de on-line opslagruimte.

**BSC·e10** De gebruiker moet voor iedere ZIM de volgende acties kunnen ondernemen:

- maken van een volledige back-up,
- maken van een incrementele back-up,
- terughalen van een back-up.

Bij gebruiksscenario [BSC.s02] *beheren DCN-koppeling aan ZIM* gelden de volgende eisen en wensen:

**BSC.e11** De gebruiker moet een overzicht kunnen oproepen van de volgende *variabelen* voor ieder geconfigureerd DCN:

- netwerkbelasting van HL7v3-verkeer met de ZIM,
- netwerkbelasting van overig IP-verkeer met ieder ander DCN.

**BSC.e12** De gebruiker moet de volgende *stuurparameters* kunnen instellen voor ieder geconfigureerd DCN:

- status van de koppeling van het DCN aan de ZIM:
  - opengesteld,
  - geblokkeerd,
- maximum aantal aangesloten GBZ'en via dit DCN.

**BSC.e13** De gebruiker moet een DCN-koppeling kunnen toevoegen en verwijderen, en daarbij de volgende *configuratieparameters* kunnen instellen:

- DCN-id,
- eventuele IP-adresreeks voor het DCN,
- naam van het DCN zoals bekend bij de ZSP en de zorgaanbieders,
- E-mailadres van de netwerkbeheerder,
- telefoonnummer van de netwerkbeheerder,
- DCN-kwalificatieniveau,
- datum eerste toelating,
- tekstuele toelichting,
- URI van de ZIM waarop dit DCN primair wordt aangesloten,
- URI van de uitwijk-ZIM waarop dit DCN kan terugvallen.

Bij gebruiksscenario [BSC.s03] *beheren GBZ-koppeling aan ZIM* gelden de volgende eisen en wensen:

**BSC.e14** De gebruiker moet een overzicht kunnen oproepen van de volgende *variabelen* voor ieder geconfigureerd GBZ:

- bereikbaarheid van het GBZ, zie [Technische Architectuur] paragraaf 9.4,
- alle stuurparameters en configuratieparameters voor dat GBZ,
- per gebruikerssessie:
  - UZI-nr. van de gebruiker,
  - vertrouwensniveau van de sessie,
  - tijdstip van inloggen,

en de volgende variabelen voor iedere afzonderlijke applicatie binnen dat GBZ, plus de totalen/gemiddelden over alle applicaties van dat GBZ indien zinvol:

- beschikbaarheidsmodus van de applicatie, zie [Technische Architectuur] paragraaf 9.4,
- per gebruikersinteractie:
  - aantal interacties per seconde,
  - aantal mislukte interacties, uitgesplitst naar foutsoort,
  - aantal interacties dat via een ander schakelpunt afgehandeld moest worden,
  - minimum, gemiddelde en maximum responstijd bij actie,
  - minimum, gemiddelde en maximum responstijd bij reactie,
  - gemiddeld aantal uitgewisselde patiëntstukken per interactie,
  - gemiddeld aantal uitgewisselde bytes per interactie,
- alle stuurparameters en configuratieparameters voor die applicatie.

**BSC·e15** De gebruiker moet de volgende *stuurparameters* kunnen instellen voor ieder geconfigureerd GBZ:

- status van de koppeling van het GBZ aan de ZIM:
  - opengesteld,
  - geblokkeerd,

en de volgende stuurparameters kunnen instellen voor iedere afzonderlijke applicatie, dan wel voor alle applicaties van dat GBZ tezamen indien zinvol:

- actiemodus van de applicatie, zie [Technische Architectuur] paragraaf 9.4.

**BSC·e16** De gebruiker moet een GBZ-koppeling kunnen toevoegen en verwijderen, en daarbij de volgende *configuratieparameters* kunnen instellen:

- GBZ-id,
- URI van het GBZ,
- UZI-nr van het UZI-servicescertificaat,
- naam van het GBZ zoals bekend bij de zorgaanbieder,
- naam van de zorgaanbieder,
- abonneenummer van de zorgaanbieder in het UZI-register (URA),
- E-mailadres van de beheerder,
- telefoonnummer van de beheerder,
- GBZ-kwalificatieniveau,
- datum eerste toelating,
- tekstuele toelichting,
- DCN-id van het DCN waarop dit GBZ is aangesloten,

en binnen dat GBZ verscheidene applicaties kunnen toevoegen en verwijderen, en daarvoor de volgende configuratieparameters kunnen instellen:

- applicatie-id
- fabrikaat en type van de applicatie,
- naam van de applicatie zoals bekend bij de zorgaanbieder,
- naam van de zorgaanbieder,
- toepassingsrollen waarvoor een (type-) goedkeuring is verkregen,
- HL7v3 conformancetabel van de applicatie,
- datum eerste toelating,
- tekstuele toelichting,
- gebruikte HL7v3-release.

**BSC·e17** { toekomst } De gebruiker moet een bij eis **BSC·e16** nieuw ingestelde actiemodus, deze kunnen afdwingen bij de desbetreffende applicatie door het sturen van een bericht met de volgende gegevens:

- de nieuwe actiemodus,
- een tekstuele toelichting.

**BSC·e18** { toekomst } De gebruiker moet een tekstbericht kunnen sturen naar alle GBZ-gebruikers van:

- één bepaald GBZ,
- alle GBZ'en aangesloten op een bepaalde DCN of ZIM,
- alle GBZ'en van alle ZIM's.

Bij gebruiksscenario [BSC.s04] *beheren alarmmeldingen* gelden de volgende eisen en wensen:

**BSC.e19** De gebruiker moet voor iedere variabele van ieder type beheerobject één of meer alarmtoestanden kunnen definiëren met de volgende eigenschappen:

- de grenswaarde die bij onder- of overschrijding leidt tot een alarmtoestand,
- de alarmklasse waarin de variabele wordt gezet bij passeren van de grenswaarde,
- een tekstuele omschrijving van de alarmtoestand.

**BSC.e20** De gebruiker moet verscheidene alarmklassen kunnen definiëren met de volgende eigenschappen:

- in welke kleur de alarmtoestand moet worden getoond in de lijst van alarmregels en in een overzicht van variabelen,
- of bij eerste optreden een visueel en/of auditief signaal moet worden gegeven.

**BSC.e21** De gebruiker moet een lijst van alarmregels kunnen oproepen, die per alarmregel de volgende attributen kunnen tonen:

- de identiteit van het object,
- de grenswaarde die was onder- of overschreden,
- de opgetreden alarmklasse,
- het tijdstip van dit optreden,
- een tekstuele omschrijving van de alarmtoestand,
- een indicatie of de alarmmelding reeds is "erkend",
- de afhandelingstatus van de alarmtoestand,
- de identificatie van de gebruiker die de afhandelingstatus laatst heeft gewijzigd,
- een tekstuele toelichting van die gebruiker,

waarbij de kleur van de alarmregel overeenkomt met de alarmklasse.

**BSC.e22** De gebruiker moet voor de lijst van alarmregels kunnen selecteren dat uitsluitend worden getoond:

- alarmregels van bepaalde typen object,
- alarmregels opgetreden binnen een bepaald tijdvenster,
- alarmregels van bepaalde alarmklassen,
- alarmregels met bepaalde afhandelingstatus,
- bepaalde attributen per alarmregel.

**BSC.e23** De gebruiker moet:

- kunnen bladeren door de lijst van alarmregels,
- kunnen bepalen volgens welk attribuut de alarmregels in de lijst op volgorde worden gezet,
- de afhandelingstatus van een alarmregel kunnen wijzigen in:
  - nieuw,
  - erkend,
  - afgehandeld,
- een tekstuele toelichting kunnen toevoegen aan een alarmregel,
- een te bepalen deel van de lijst kunnen afdrukken,
- een te bepalen deel van de lijst kunnen exporteren naar een intelligent analysegereedschap.

Voor al deze gebruiksscenario's is het nodig dat de gebruiker heeft ingelogd als schakelpuntbeheerder, zie gebruiksscenario [INL-s01].

Opmerkingen:

- Ad eis [BSC-e06] Het melden van een actiemodus aan een applicatie kan in de toekomst worden gecombineerd met het synchroniseren van allerlei stuurparameters uit het schakelpunt. In afwachting van deze functie kan de schakelpuntbeheerder de telefoon pakken of een e-mail sturen.
- Gebruiksscenario's worden gewoonlijk top-down afgeleid uit de voorgaande paragrafen. Dit gebruiksscenario is echter deels bottom-up afgeleid uit navolgende hoofdstukken. Voor een goed begrip van de bovenstaande eisen is lezing van de navolgende hoofdstukken noodzakelijk.
- De taken van de schakelpuntbeheerder worden bij voorkeur verdeeld over gespecialiseerde beheerders:
  - systeembeheerders voor het instellen van de parameters en het bewaken van de variabelen van:
    - de operationele ZIM, uitwijk-ZIM en test-ZIM
    - de koppeling van DCN'en aan iedere ZIM,
    - de koppeling van GBZ'en aan iedere ZIM,
  - applicatiebeheerders voor de implementatie van:
    - nieuwe soorten en versies van HL7-berichten,
    - nieuwe gegevenssoorten,
    - nieuwe zorgverlenerfuncties,
    - nieuwe programmatuur voor de ZIM,
- klantenondersteuning die ten behoeve van netwerkbeheerders en zorgaanbieders en andere gebruikers inzicht moeten hebben in:
  - de variabelen van de operationele ZIM,
  - de variabelen van DCN'en gekoppeld aan die ZIM,
  - de variabelen van GBZ'en gekoppeld aan die ZIM,
- test- & demo-beheerders die ten behoeve van XIS-leveranciers en XIS-beheerders moeten kunnen configureren:
  - bewaken van de variabelen van de test-ZIM,
  - instellen van de parameters voor de koppeling van XIS'en aan de test-ZIM.

## 4.19 Beheren patiëntenregister (BPR)

Dit gebruiksscenario wordt overgelaten aan het BSN-programma.

## 4.20 Beheren zorgaanbiederregister (BZR)

Dit gebruiksscenario wordt overgelaten aan het UZI-project.

## 4.21 Beheren zorgaanbiedergids (BZG)

Dit gebruiksscenario wordt overgelaten aan het UZI-project.

## 5 Objecten

De ICT-voorzieningen in de zorg omvatten tenminste de onderstaande objecten:

- *schakelpunt*, een algemeen toegangspunt voor het uitwisselen van patiëntgegevens
- *verwijsindex*, een tabel die de toegang tot alle patiëntdossiers mogelijk maakt
- *toegangsglog*, een lijst waarin alle toegang tot patiëntdossiers via het schakelpunt wordt gelogd
- *autorisatieprotocol*, een tabel die de toegang van zorgpartijen tot patiëntdossiers in het algemeen autoriseert
- *autorisatieprofiel*, een tabel die de toegang tot de patiëntdossiers van een specifieke patiënt/cliënt autoriseert
- *identificatie & authenticatie-module*, een module die de geldigheid van vertrouwensmiddelen verifieert,
- *patiëntdossier*, een verzameling patiëntstukken onder verantwoordelijkheid van één zorgaanbieder
- *zorgaanbiederpostbus*, een verzameling patiëntberichten ontvangen door één zorgaanbieder
- *zorgaanbieder-applicatie*, een applicatie die een zorgverlener toegang kan verschaffen tot zijn eigen patiëntdossier
- *patiënt-applicatie*, een applicatie die een patiënt/cliënt toegang kan verschaffen tot een verwijsindex
- *zorgaanbiederregister*, een register met identificerende gegevens van zorgaanbieders
- *zorgaanbiederuids*, een gids met aangeboden zorgdiensten en bereikbaarheidsgegevens van zorgaanbieders
- *patiëntenregister*, een register met identificerende gegevens van patiënten/cliënten
- *patiëntenadresboek*, een adresboek met bereikbaarheidsgegevens van patiënten/cliënten
- *schakelbeheer-applicatie*, een applicatie die een schakelpuntbeheerder toegang kan verschaffen tot het schakelpunt en de daaraan gekoppelde objecten
- *autorisatiebeheer-applicatie*, een applicatie die een autorisatiebeheerder toegang kan verschaffen tot het autorisatieprotocol en alle autorisatieprofielen
- *logbeheer-applicatie*, een applicatie die een logbeheerder toegang kan verschaffen tot de toegangsglog
- *registerbeheer-applicatie*, een applicatie die een registerbeheerder toegang kan verschaffen tot het patiëntenregister en/of het zorgaanbiedersregister.
- *mandateringstabel*, een tabel waarin een zorgverlener andere zorgverleners kan mandateren om namens hem/haar patiëntgegevens uit te wisselen.

De belangrijkste van deze objecten worden in de navolgende paragrafen nader gespecificeerd. De structuur van de verwijsindex en die van het autorisatieprotocol is sterk afhankelijk van die van het patiëntdossier. Daarom wordt eerst het patiëntdossier gespecificeerd.

## 5.1 Patiëntdossier (PDO)

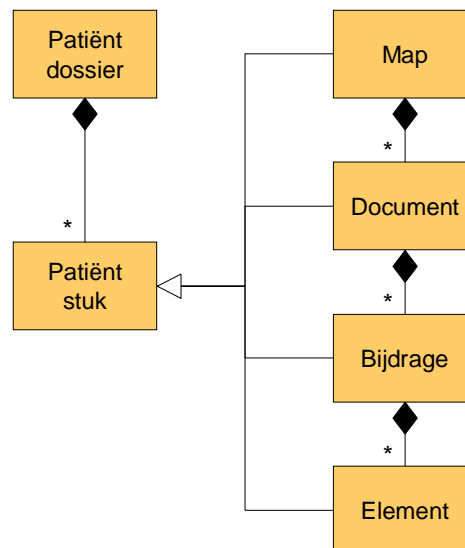
Het patiëntdossier wordt hier gedefinieerd als een *verzameling van (persoonlijke, logistieke, medische en/of financiële) patiëntgegevens van één patiënt/cliënt, die via één zorgaanbieder toegankelijk is.*

Niettemin kan een zorgaanbieder, bijv. een ziekenhuis, meerdere, aparte patiëntdossiers van één patiënt/cliënt onderhouden, bijv. een medisch dossier per afdeling. In dat geval is er vaak een intern patiëntenregister, ook wel *patiëntenindex* genoemd, waarin de persoonlijke, identificerende gegevens centraal worden bijgehouden.

Zoals beschreven in [Bedrijfsarchitectuur] paragraaf 6.3 en 6.5, kan een patiëntdossier worden gezien als een verzameling van patiëntmappen met één of meer patiëntdocumenten, ieder bestaande uit één of meer patiëntgegevensbijdragen, die ieder weer bestaan uit één of meer patiëntgegevenselementen: de kleinste eenheid van patiëntgegevens waarin een patiëntdossier kan worden opgebroken zonder dat de betekenis verloren gaat.

Ieder aggregatieniveau van patiëntstuk kan in principe als uittreksel van dat patiëntdossier worden uitgewisseld. In de praktijk zal dit afhangen van de zorgtoepassing en de gegevenssoort, welke patiëntstukken zinvol kunnen worden uitgewisseld. HL7v3 ondersteunt momenteel uitwisseling op het niveau patiëntdocument en patiëntgegevenselement.

De onderstaande figuur toont de compositie van een patiëntdossier, in een UML class diagram.



Het bovenstaande betekent niet dat ieder patiëntdossier intern daadwerkelijk zo gestructureerd dient te zijn. Bestaande zorgsystemen hebben ieder een eigen structurering van patiëntgegevens, waarbij een bepaald patiëntgegevenselement vaak betekenis ontleent aan zijn context: de exacte plaats in het patiëntdossier waar het element is opgeslagen. Wanneer zo'n element nu wordt opgevraagd, en dus uit zijn



context wordt gehaald, dient dit element te worden voorzien van attributen die het dreigende verlies aan betekenis compenseren.

Het bovenstaande betekent wél dat ieder patiëntdossier na opvraag van patiëntgegevens, op dezelfde wijze patiëntstukken aan de opvrager moet opleveren. Dit betekent dat bestaande zorgsystemen zullen moeten worden voorzien van een adapter die de interne structurering van patiëntgegevens vertaalt naar patiëntstukken volgens onderstaande specificatie.

Architectuurbeslissingen:

**PDO.b01** {toekomst} Als gevolg van architectuurbeslissing [ovg.b03] mogen in ieder patiëntdossier de patiëntstukken niet worden gewijzigd of verwijderd, tenzij het gehele dossier wordt vernietigd.

Ieder patiëntstuk zal, voor zover relevant, de volgende *inhoud* hebben:

- generieke attributen,
- specifieke attributen, bijv. medicijn, hoeveelheid, omschrijving, etc.
- specifieke bulkinhoud, bijv.: vrije tekst, digitaal beeld, digitaal geluid, etc.

De standaardisering van de *specifieke* inhoud is het werkterrein van het programma Zorgtoepassingen. De standaardisering van de generieke kenmerken behoort tot de basisinfrastructuur en wordt hier aldus gespecificeerd.

Ieder *patiëntstuk* zal de volgende *generieke* attributen kunnen bevatten:

- het *landelijke patiëntnummer* (BSN) van de onderhavige patiënt/cliënt
- {toekomst} de *integriteit* van de koppeling aan deze patiënt/cliënt,
- de *inhoudverantwoordelijke*, die het patiëntstuk heeft bekrachtigd:
  - de *identiteit* van de zorgaanbieder,
  - de *identiteit* van de zorgverlener,
  - de *functie* van de zorgverlener,
- het *dossier* waaruit dit patiëntstuk afkomstig is,
- het *tijdstip* waarop het patiëntstuk is aangemaakt
- het *patiëntstuk-id*, een unieke identificatie, zie [Technische Architectuur] paragraaf 12.4.

Ieder *patiëntdocument* zal bovendien de volgende *generieke* attributen kunnen bevatten:

- de *gegevenssoort* van dit patiëntdocument.
- de *samensteller* die dit patiëntdocument heeft gefiatteerd,
- het *tijdstip* waarop dit patiëntdocument is gefiatteerd,
- de *episode* waartoe de zorgdienst behoort, indien van toepassing,
- de *periode* waarin deze zorgdienst is gepland of heeft plaatsgevonden.

Iedere *patiëntgegevensbijdrage* zal bovendien de volgende *generieke* attributen kunnen bevatten:

- de *gegevenssoort* van deze bijdrage.
- de *vastlegger* die deze bijdrage heeft vastgelegd,
- het *tijdstip* waarop deze bijdrage is vastgelegd,
- de *betrokkenheid* van deze vastlegger,
- de *handeling* van deze vastlegger.

Ieder *patiëntgegevenselement* zal bovendien de volgende *generieke* attributen kunnen bevatten:

- de *gegevenssoort* van dit element,
- de *gegevensbron* die dit element heeft gegenereerd,
- het *tijdstip* waarop dit element is gegenereerd,

Voor een verklaring van *verantwoordelijke, samensteller, vastlegger* en *gegevensbron*, zie [Bedrijfsarchitectuur] paragraaf 7.3.

De *gegevenssoort* is een manier om de vele verschillende soorten patiëntstukken te typeren, zie ook [Bedrijfsarchitectuur] paragraaf 6.2, zoals:

- medicatieverstrekking
- labuitslag
- professionele samenvatting
- dossier

De definitie van *medische* gegevenssoorten en de daarmee samenhangende standaardisering van de specifieke inhoud per gegevenssoort, is het werkterrein van het programma Zorgtoepassingen. Niettemin is in dit document ook behoefte aan gegevenssoorten uit de persoonlijke, logistieke en financiële gegevensklassen. De opnieuw in ontwikkeling zijnde standaard [prENV13606] is hier nog niet meegenomen. Dit zal in een latere versie van dit document geschieden.

De *episode* duidt (conform [prENV13940] "episode\_of\_care") op een reeks van samenhangende zorgcontacten die een zorgaanbieder heeft met een bepaalde patiënt/cliënt in het kader van een bepaalde zorgvraag.

De *periode* (conform [prENV13940] "period\_of\_service") kan de datum van een afspraak, observatie of rekening zijn, maar ook een tijdsinterval waarvoor een medicatie is voorgeschreven.

Het *dossier* is het adres van de applicatie waarlangs het patiëntstuk toegankelijk is. Voor de basisinfrastructuur is het niet van belang of het element ook daadwerkelijk in dat systeem ligt opgeslagen. Zo kan een ZIS binnen een ziekenhuis eventueel fungeren als interne verwijzindex en aldus een opvraag doorschakelen naar bijv. een RIS of LIS aangesloten op dat ZIS.

De *koppelintegriteit* is een maat voor de zekerheid dat de patiëntstukken werkelijk horen bij deze patiënt/cliënt, zoals een zorgaanbieder moet bijhouden in het patiëntendossier of een lokaal patiëntenregister, zie paragraaf 5.10. In overleg met VWS is besloten deze koppelintegriteit niet mee te zenden met patiëntstukken.

Het patiëntdossier dient de volgende *operaties* te kunnen afhandelen:

- Een externe opvraag van patiëntgegevens dient te worden beantwoord met het opleveren van:
  - (index) een lijst met alle beschikbare gegevenssoorten, inclusief de actualiteit van het laatst toegevoegde patiëntstuk van die gegevenssoort,
  - (inhoud) *alle* patiëntstukken, *inclusief* attributen maar *exclusief* multimedia, die voldoen aan de opvraagcriteria,
  - (multimedia) *één* specifiek multimediaal patiëntstuk, dat voldoet aan de opvraagcriteria,

Indien het patiëntdossier niet in staat is alle opvraagcriteria te interpreteren (legacy), dient het patiëntdossier de desbetreffende opvraagcriteria te negeren en slechts de overige te interpreteren.

- Bij het lokaal invoeren, overdragen of verwijderen van patiëntstukken, dient het patiëntdossier te melden aan de verwijsindex dat dit patiëntdossier wèl of géén patiëntstukken heeft met de kenmerken/attributen genoemd in de verwijsindex, tenzij:
  - dit aan de vermelding in de verwijsindex niets verandert,
  - het patiëntstuk van deze gegevenssoort volgens het autorisatieprofiel überhaupt niet opvraagbaar is (ook niet in noodgevallen),
- bij vermoede onjuistheden in de verwijsindex, dient het patiëntdossier al zijn vermeldingen in de verwijsindex bij te werken (synchroniseren). Dit speelt bijv. in de volgende gevallen:
  - wanneer het patiëntdossier enige tijd niet beschikbaar is geweest voor de verwijsindex,
  - wanneer de verwijsindex enige tijd niet beschikbaar is geweest voor het patiëntdossier.

Opmerkingen:

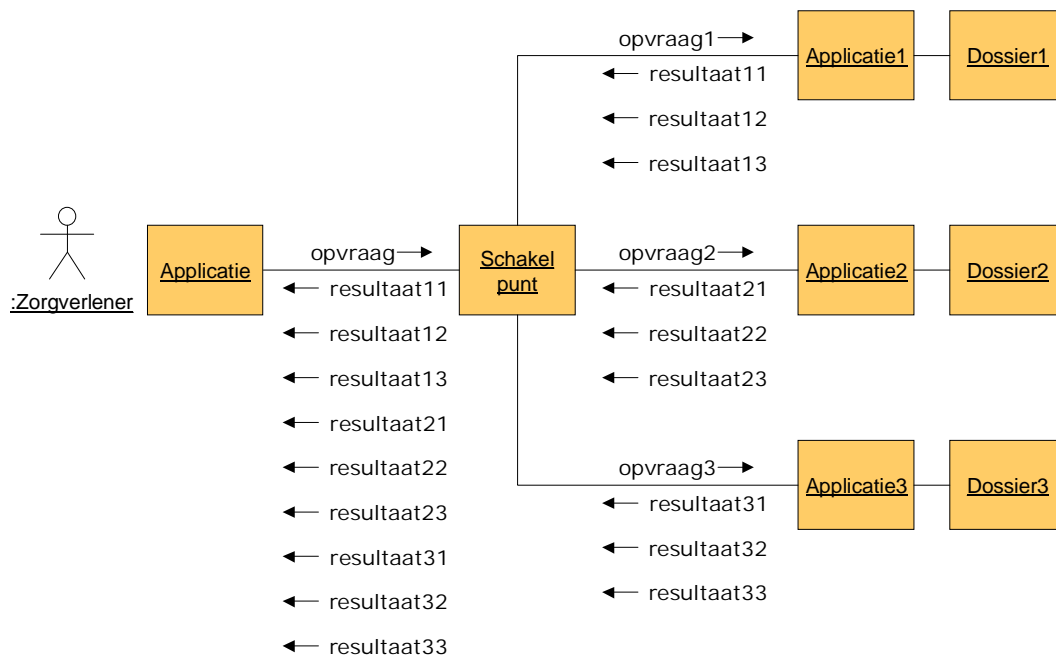
- De bovengenoemde generieke attributen van patiëntstukken zijn nog in onderzoek; idealiter zijn ze in lijn met prEN13606 en passen ze bovendien binnen HL7v3. In de HL7 Berichtdefinities zal blijken dat dit nog niet helemaal mogelijk is.
- Merk op dat een patiëntstuk geen attribuut heeft, dat aangeeft dat het patiëntstuk een kopie is.
- Het bovenstaande specificeert geenszins de wijze waarop een patiëntdossier intern gestructureerd moet zijn. Het specificeert slechts de wijze waarop de patiëntstukken naar buiten opgeleverd kunnen worden.

## 5.2 Schakelpunt (SCH)

Het schakelpunt wordt hier gedefinieerd als:

- een loket voor het *opvragen* van patiëntgegevens:
  - waar alle opvragen van patiëntgegevens door een zorgaanbiederapplicatie of patiëntapplicatie kunnen worden geplaatst,
  - dat deze opvragen vervolgens doorschakelt naar de juiste patiëntdossiers en/of andere schakelpunten,
  - dat alle resultaten van die patiëntdossiers en/of andere schakelpunten ontvangt en doorschakelt naar de opvrager.
- een doorgeefluik voor het *versturen* van patiëntgegevens:
  - waar alle berichten door een zorgaanbiederapplicatie of patiëntapplicatie kunnen worden gepost,
  - dat deze berichten vervolgens doorschakelt naar juiste postbussen en/of andere schakelpunten.

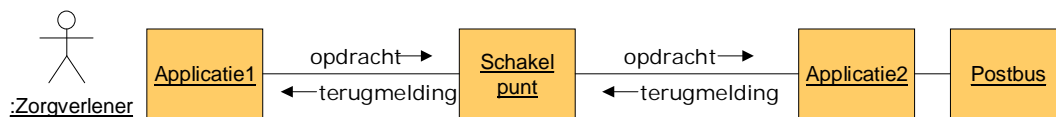
Bij het *opvragen* van patiëntgegevens is het schakelpunt verantwoordelijk voor het raadplegen van de verwijzindex, het doorschakelen van de opvraag naar alle daarin vermelde dossiers, het verzamelen van alle opgeleverde resultaten en het terugsluizen daarvan naar de opvrager. De onderstaande figuur toont dat één opvraag kan leiden tot zeer vele resultaten. In het document [Technische Architectuur] wordt uitgewerkt hoe de uitwisseling van patiëntgegevens kan worden gerealiseerd met behulp van HL7v3-berichtenverkeer en welke opties van *bundelen*, *groeperen*, *doseren* en *sorteren* door het schakelpunt moeten worden ondersteund.



Wanneer de verwijzindex inconsistent raakt, kan het gebeuren dat het schakelpunt een opvraag richt aan een dossier, maar het dossier vervolgens geen resultaten kan

opleveren. Om dergelijke gevallen bij te houden voor de schakelpuntbeheerder, kan het schakelpunt deze fouten zelf loggen of doorgeven aan de verwijfsindex. De laatste optie verdient de voorkeur. Voor de zorgaanbiedergids geldt een analoge redenering.

Bij het *versturen* van patiëntgegevens is het schakelpunt verantwoordelijk voor het afleveren van opdrachten en meldingen in de juiste zorgaanbiederpostbus na raadplegen van een adrestabel. In het document [Technische Architectuur] wordt uitgewerkt hoe deze uitwisseling van patiëntgegevens kan worden gerealiseerd met behulp van HL7v3-berichtenverkeer en welke opties door het schakelpunt moeten worden ondersteund: het eventueel bevestigen van het resultaat en het moment waarop : *onmiddellijk of mettertijd?* In het eerste geval zal het niet beschikbaar zijn van de postbus onmiddellijk leiden tot een bevestiging dat de aflevering mislukt is (*instant messaging* mechanisme). In het tweede geval heeft het schakelpunt de tijd om het nog eens te proberen als de postbus weer beschikbaar is (*store & forward*-mechanisme).



In het document [Technische Architectuur] wordt uitgelegd dat het schakelpunt niet zozeer de dossiers en postbussen moet adresseren, maar de applicaties die deze dossiers en postbussen ontsluiten, wegens de werkwijze van HL7v3.

Uit oogpunt van *doelmatigheid* moet het schakelpunt alle in de verwijfsindex genoemde applicaties bevragen, behalve de opvragende applicatie. Anders zou het schakelpunt onnodig patiëntgegevens gaan rondpompen. Er zijn omstandigheden denkbaar van complexe applicaties waarvoor dit rondpompen toch wenselijk is. In de toekomst kan die optie wellicht worden geboden.

Uit oogpunt van *doelmatigheid* moet het schakelpunt ten behoeve van één opvraag alle in de verwijfsindex genoemde applicaties slechts één maal bevragen, ook als een applicatie toevallig meerdere keren in de verwijfsindex staat met de gevraagde patiënt en gegevenssoort. Dit kan bijvoorbeeld gebeuren als verschillende specialismen van één ziekenhuis vanuit dezelfde applicatie dezelfde gegevenssoort hebben aangemeld. Dubbele bevestigingen zouden namelijk leiden tot dubbele antwoorden.

Uit oogpunt van *vertrouwelijkheid* mag het schakelpunt geen patiëntgegevens opslaan langer dan nodig is om een opvraagssessie af te ronden of om een patiëntbericht af te leveren. Dit betekent dat buffers met patiëntgegevens na gebruik telkens moeten worden gewist of anderszins beschermd tegen abusievelijk uitlekken. Denk daarbij aan het afdanken van computers met achtergebleven gegevens, nieuwsgierige beheerders, etc.

Uit oogpunt van *integriteit* mag het schakelpunt geen berichten wijzigen, filteren of inzien anders dan nodig voor het afleveren op de juiste bestemming.

Uit oogpunt van *beschikbaarheid* en *schaalbaarheid* zijn meerdere schakelpunten mogelijk, al dan niet regionaal verspreid. Dit is alleen beheersbaar als de schakelpunten landelijk door één partij worden beheerd.

Architectuurbeslissingen:

- SCH·b01** Er komt één landelijk schakelpunt, dat kan bestaan uit meerdere interne schakelpunten t.b.v. doelmatige opschaling van de capaciteit.
- SCH·b02** Het schakelpunt moet voorkomen dat buffers met patiëntgegevens na een afgeronde of afgebroken gebruikersinteractie abusievelijk uitlekken.
- SCH·b03** Het schakelpunt mag niet het dossier van de opvragende applicatie bevragen, {toekomst} anders dan op uitdrukkelijk verzoek van de opvragende applicatie.
- SCH·b04** Het schakelpunt moet ten behoeve van één opvraag alle in de verwijzindex genoemde applicaties slechts éénmaal bevragen, ook als een applicatie toevallig meerdere keren in de verwijzindex staat met de gevraagde patiënt en gegevenssoort.
- SCH·b05** Als gevolg van architectuurbeslissing [vwi·b05] moet het schakelpunt foute verwijzingen en foute adressen terugmelden aan de verwijzindex resp. de zorgaanbieder/gids.

Het schakelpunt dient de volgende *operaties* te kunnen afhandelen:

- Een verzoek tot inloggen door een gebruiker via een applicatie dient te leiden tot:
  - het raadplegen van de identificatie&authenticatie-module, om de identiteit van de aanvrager te authenticeren,
  - het opzetten van een sessie waarlangs gebruikersinteracties kunnen worden afgehandeld (zie beneden),
  - het afbreken van de sessie na uitloggen van de gebruiker,
  - het afbreken van de sessie na de time-out na niet gebruiken van de opgezette sessie,
  - het loggen van het opzetten en afbreken in de toeganglog.
- Een gebruikersinteractie van een ingelogde gebruiker via een applicatie dient te leiden tot:
  - het raadplegen van het autorisatieprotocol om te controleren of de gebruiker op grond van zijn functie, of die van diens mandaterende zorgverlener, de gebruikersinteractie mag uitvoeren op de gegevenssoort,
  - het raadplegen van het autorisatieprofiel om te controleren of:
    - de patiënt/cliënt ooit toestemming heeft gegeven voor elektronische uitwisseling van patiëntgegevens,
    - zo ja, of de gebruiker niet expliciet is uitgesloten voor de gegevensklasse,
  - het omzeilen van de autorisatie indien de gebruiker een beroep heeft gedaan op noodgeval,
  - het controleren of het bericht met de gebruikersinteractie afkomstig is van de gebruiker die heeft ingelogd,
  - het uitvoeren van de gebruikersinteractie (zie beneden),
  - het loggen van de gebruikersinteractie in de toeganglog met een indicatie van het succes van die gebruikersinteractie.
- Een opvraag van patiëntgegevens (via een applicatie of een ander schakelpunt) dient te leiden tot:
  - het raadplegen van de verwijzindex om de relevante applicaties met patiëntdossiers te bepalen,
  - het controleren in de configuratietabel of de vermelde applicaties deze gebruikersinteractie kunnen verwerken,

- het doorschakelen van de opvraag naar de relevante applicaties, eventueel ook naar andere schakelpunten,
  - het ontvangen en het doorschakelen van de opgeleverde resultaten naar de aanvrager,
  - het doorgeven van eventuele foute verwijzingen aan de verwijsindex,
  - het doorgeven van eventuele foute adressen aan de configuratietabel.
- Een aanmelding of afmelding van patiëntgegevens (via een applicatie of een ander schakelpunt) dient te leiden tot:
    - het aanmaken of verwijderen van een verwijzing in/uit de verwijsindex,
    - het doorgeven daarvan aan alle andere schakelpunten, behalve het aanmeldende schakelpunt.
- {toekomst} Een verzoek tot synchronisatie (via een applicatie of een andere verwijsindex) dient te leiden tot:
    - het verwijderen van alle verwijzingen uit de verwijsindex, voorzover ze op de aanmelder slaan,
    - het opnieuw toevoegen van verwijzingen in de verwijsindex,
    - het doorgeven daarvan aan alle andere schakelpunten, behalve het aanmeldende schakelpunt.
- Een opdracht (via een applicatie of een ander schakelpunt) dient te leiden tot:
    - het controleren in de configuratietabel of de vermelde applicatie deze HL7-interactie kan verwerken
    - het doorschakelen van de opdracht naar de juiste applicatie met zorgaanbiederpostbus, eventueel via andere schakelpunten,
    - het doorgeven van eventuele foute adressen aan de configuratietabel,
    - het ontvangen en het doorschakelen van de bevestiging aan de opdrachtgever.

### 5.3 Verwijsindex (VWI)

De verwijsindex wordt hier gedefinieerd als een tabel met verwijzingen naar patiëntdossiers waar patiëntgegevens met bepaalde kenmerken/attributen beschikbaar zijn voor opvraag. Doel van de verwijsindex is het doelmatig uitvragen van alleen *dé* dossiers die de gevraagde gegevens bevatten, zie [Bedrijfsarchitectuur] paragraaf 8.2.

Om überhaupt te kunnen functioneren, zijn per verwijzing de volgende attributen *noodzakelijk* in de verwijsindex:

- patiënt-id,
- dossier-id.

In plaats van het dossier-id zal in de praktijk de applicatie-id worden gebruikt van de applicatie die het desbetreffende dossier ontsluit, zie het document [Technische Architectuur]. In geval van meerdere schakelpunten die ieder een eigen verwijsindex onderhouden, kan de applicatie-id van een ander schakelpunt worden gebruikt.

Uit oogpunt van *doelmatigheid* is het belangrijk de onderstaande attributen op te nemen in de verwijsindex. Dan kan een opvraagverzoek op basis van de zoekcriteria gericht worden doorgezet en wordt onnodig berichtenverkeer voorkomen:

- inhoudverantwoordelijke:
  - zorgaanbieder-id.
  - zorgverlener-functie,
  - zorgverlener-id,
- actualiteit,
- gegevenssoort.

De actualiteit kan naar keuze met een resolutie van een jaar, een maand, een dag, een uur, etc. worden bijgehouden. Een te scherpe resolutie zal er toe leiden dat er meer heraanmeldingen bij de verwijsindex worden gedaan dan er opvragingen bespaard worden. Waar de balans precies zit is moeilijk te voorspellen en kan bovendien verschillen per gegevenssoort. Daarom is het verstandig deze resolutie als instelbare parameter eerst op één jaar te zetten en deze te verscherpen wanneer dat nodig blijkt.

Uit oogpunt van *actualiteit* van de verwijsindex zelf moet een nieuwe aanmelding aan de verwijsindex snel worden gedaan. Bijv. om te voorkomen dat een apotheker aan de verwijsindex niet kan zien, dat de huisarts een half uur eerder voor een patiënt/cliënt voor het eerst de allergieën heeft aangemeld, wordt voorgesteld voor nieuwe aanmeldingen 1 kwartier aan te houden.

Uit oogpunt van *beheerbaarheid* is het belangrijk de onderstaande attributen op te nemen in de verwijsindex:

- beheerverantwoordelijke:
  - zorgaanbieder-id.
  - zorgverlener-functie,
  - zorgverlener-id,
- patiëntgegevens-id.

De patiëntgegevens-id is nodig bij heraanmelden of afmelden om de bedoelde verwijzing te identificeren. In geval van een atomaire aanmelding kan hier de identificatie van het aangemelde patiëntstuk worden gebruikt, zie ook paragraaf 4.6 en [Technische



Architectuur] paragraaf 12.4. In geval van een categorale aanmelding kan hier een willekeurige identificatie worden gebruikt, zolang de aanmeldende applicatie die identificatie onthoudt voor latere heraanmelding en eventuele afmelding.

Uit oogpunt van *leesbaarheid* zou de verwijzindex behalve de zorgaanbieder-id resp. zorgverlener-id ook herkenbare identificerende en/of bereikbaarheidsgegevens kunnen bevatten. Maar dan zou de verwijzindex veel redundante gegevens bevatten. Een applicatie die de inhoud van de verwijzindex toegangslog toont, kan deze id's beter vertalen naar herkenbare gegevens met behulp van de zorgaanbieder *gids*. In afwachting van de zorgaanbieder *gids*, zouden deze herkenbare gegevens tijdelijk alsnog in de toegangslog kunnen worden opgenomen, maar doelmatiger is het gebruik van een aparte zorgaanbieder *tabel*, zie verder paragraaf 5.13.

Uit oogpunt van *vertrouwelikhed* mag een verwijzindex buiten een zorgaanbieder geen patiëntgegevens of verwijzingen daarnaar bevatten. Dit vergt aldus speciale juridische en organisatorische maatregelen om tenminste verwijzingen te kunnen opnemen. Daarnaast is het de vraag of de verwijzindex ook verwijzingen mag bevatten voor patiënten/cliënten die bezwaar hebben gemaakt tegen elektronische uitwisseling van hun patiëntgegevens, zie ook paragraaf 4.13. Geredeneerd vanuit de WBP is het antwoord "nee", zie bijlage C.

Uit oogpunt van *integriteit* mag een verwijzing alleen worden gewijzigd of verwijderd door de beheerverantwoordelijke zorgaanbieder. Of de verschillende zorgverleners binnen een zorgaanbieder elkaars verwijzingen mogen wijzigen of verwijderen, is aan de zorgaanbieder. Welke attributen precies kunnen worden gewijzigd bij heraanmelden, wordt uiteengezet in bijlage C.

Uit oogpunt van *betrouwbaarheid* moet de verwijzindex worden teruggemeld indien de verwijzingen niets hebben opgeleverd. Op basis van foutentellers kunnen schakelpuntbeheerders bepalen of een beheerverantwoordelijke zorgaanbieder moet worden aangesproken op correct aan/afmelden en regelmatig synchroniseren. De foutenteller is een verborgen attribuut en dus niet zichtbaar of wijzigbaar voor zorgaanbieders.

Uit oogpunt van *schaalbaarheid* is het mogelijk dat verscheidene schakelpunten ieder een eigen verwijzindex hebben. Daarbij is het de vraag of iedere verwijzindex moet aangeven van welke patiënten/cliënten gegevens beschikbaar zijn via een ander schakelpunt of niet:

- Zo ja, dan zal iedere verwijzindex in de praktijk grotendeels gevuld zijn met verwijzingen naar andere verwijzindices. Nadeel is dat iedere *aanmelding* altijd naar alle andere verwijzindices moet worden gedivergeerd.
- Zo nee, dan zal iedere verwijzindex alleen verwijzingen binnen de regio bevatten. Nadeel is dat iedere *opvraag* altijd naar alle andere verwijzindices moet worden doorgestuurd. Voordeel is dat aanmeldingen juist binnen de regio blijven.

Het voorstel is te kiezen voor "ja", omdat er naar verwachting meer opvragingen dan aanmeldingen zullen zijn. Nog beter zou zijn, deze keuze aan de schakelpuntbeheerder te laten, zodat hij afhankelijk van het gegevensverkeer in de praktijk zijn verwijzindex kan optimaliseren.

Een variant van de hier beschreven verwijzindex is de zogenaamde Master Patiënt Index (MPI). Dit is een verwijzindex waarin voor iedere verwijzing naar een lokaal

patiëntdossier, ook het interne patiëntnummer wordt vermeld. Hiervoor wordt nadrukkelijk niet gekozen, want:

- iedere zorgaanbieder is zelf verantwoordelijk voor de koppeling tussen zijn lokaal gebruikte patiëntnummer met een ander nummer. Een MPI zou die verantwoordelijkheid op een centrale plek neerleggen.
- een MPI zou het probleem van de vele, verschillende patiëntnummers *deels* kunnen oplossen, maar zonder de waarborgen die het BSN wel biedt.

Architectuurbeslissingen:

**VWI · b01** De verwijfsindex zal bestaan uit een reeks verwijfsingen die ieder bestaan uit de volgende attributen:

- |                               |                                      |
|-------------------------------|--------------------------------------|
| • patiënt-id (BSN)            | verplicht, niet wijzigbaar           |
| • applicatie-id               | verplicht, wijzigbaar                |
| • beheerverantwoordelijke:    |                                      |
| •     zorgaanbieder-id        | verplicht, niet wijzigbaar           |
| •     zorgverlener-id         | verplicht, wijzigbaar                |
| •     zorgverlener-functie    | verplicht, wijzigbaar                |
| • inhoudverantwoordelijke:    |                                      |
| •     zorgaanbieder-id        | verplicht, niet wijzigbaar           |
| •     zorgverlener-id         | verplicht, wijzigbaar                |
| •     zorgverlener-functie    | verplicht, wijzigbaar                |
| • gegevenssoort               | verplicht, slechts te verbijzonderen |
| • patiëntgegevens-id          | verplicht, niet wijzigbaar (sleutel) |
| • actualiteit, bestaande uit: | optioneel, wijzigbaar                |
| •     begintijd               |                                      |
| •     eindtijd                |                                      |
| • foutenteller                | niet wijzigbaar (verborgen)          |
| • {toekomst} status           |                                      |

waarbij is aangegeven welke attributen verplicht zijn bij aanmelden en welke wijzigbaar zijn bij heraanmelden, zie verder bijlage C.

**VWI · b02** Er wordt nadrukkelijk niet gekozen voor het mechanisme van een zogenaamde Master Patiënt Index (MPI), waarbij de verwijfsindex ook het interne patiëntnummer in dat dossier bevat.

**VWI · b03** Patiëntdossiers moeten een nieuwe verwijfsing binnen 1 kwartier aanmelden aan de verwijfsindex, en van iedere bestaande verwijfsing de actualiteit met een resolutie van een dag bijwerken in de verwijfsindex door heraanmelden.

**VWI · b04** {toekomst} Als gevolg van architectuurbeslissing [ovg.b03] zal de verwijfsindex alle wijzigingen zodanig moeten loggen in de toegangsllog, dat de inhoud van de verwijfsindex op een bepaald moment in het verleden gereconstrueerd kan worden.

**VWI · b05** De verwijfsindex mag geen verwijfsingen bevatten voor patiënten/cliënten die bezwaar hebben gemaakt tegen elektronische uitwisseling van hun patiëntgegevens.

**VWI·b06** De verwijfsindex zal het aantal mislukte opvragingen als gevolg van een foute verwijfsing, moeten bijhouden in een foutenteller per verwijfsing.

De verwijfsindex dient de volgende *operaties* te kunnen afhandelen op verzoek van een schakelpunt:

- het opvragen van een verwijfsing,
- het toevoegen van een verwijfsing (aanmelden),
- het wijzigen van attributen van een verwijfsing (heraanmelden),
- het verwijderen van een verwijfsing (afmelden),
- het ophogen van de foutenteller voor een mislukte verwijfsing.

Opmerkingen:

- let op het verschil tussen de *inhoud*verantwoordelijke en de *beheer*verantwoordelijke. De eerste is verantwoordelijk is voor de juistheid van de medische inhoud van de patiëntgegevens. De tweede is verantwoordelijk is voor het bewaren van bepaalde patiëntgegevens en het zonodig ter beschikking stellen daarvan aan anderen. Meestal gaat het om dezelfde zorgaanbieder, behalve na overdracht van patiëntgegevens. Vaak gaat het ook om dezelfde zorgverlener, tenzij collega-zorgverleners regelmatig de behandeling van elkaars patiënten/cliënten overnemen. Zie verder bijlage C.
- de *inhoud*verantwoordelijke als de *beheer*verantwoordelijke verwijfsen naar zowel de verantwoordelijke zorgverlener als de zorgaanbieder onder wiens verantwoordelijkheid hij op dat moment werkt. In de praktijk is het meestal niet de zorgverlener maar een gemandateerde medewerker die de feitelijke handeling uitvoert. De mandaterende zorgverlener geldt dan als verantwoordelijke. Zie ook [Bedrijfsarchitectuur] paragraaf 5.3 en 7.3.
- Per zorgtoepassing moet bepaald worden in hoeverre de optionele attributen in de verwijfsindex moeten worden ingevuld bij de aanmelding. Per gegevenssoort moet bepaald worden of de patiëntgegevens categoriaal of atomair moeten worden aangemeld.

Openstaande punten:

- Architectuurbeslissing [VWI·b05] heeft als nadeel dat, als een patiënt/cliënt later alsnog akkoord gaat met landelijke uitwisseling van patiëntgegevens, de verwijfsindex aanvankelijk leeg is. Dit betekent dat alle zorgaanbieders met patiëntgegevens van hem moeten worden bewogen tot aanmelding daarvan, alvorens die patiëntgegevens landelijk kunnen worden opgevraagd. Hiervoor is (nog) geen technische voorziening, dus moet die patiënt/cliënt zelf langs al zijn zorgaanbieders met het verzoek om alsnog aan te melden, zie verder bijlage C.

## 5.4 Gegevenssoortentabel (GGS)

De gegevenssoortentabel vertelt het schakelpunt welke gegevenssoorten in aanmerking komen voor iedere soort opvraag. Deze tabel is nodig omdat op basis van een bepaalde HL7-interactie-id niet automatisch kan worden afgeleid welke aanmeldbare gegevenssoort wordt opgevraagd. De oorzaak daarvan ligt in het feit dat patiëntstukken en hun gegevenssoorten niet allemaal hetzelfde aggregatieniveau hebben, zie ook paragraaf 5.1.

Bijvoorbeeld, als een huisarts een *eerstelijnsdossier* als gegevenssoort aanmeldt bij de verwijzindex, komt dit dossier in principe in aanmerking voor opvraag van de volgende gegevenssoorten:

- professionele samenvatting voor DWH,
- professionele samenvatting voor SEH,
- medicatievoorschriften.

Gewoonlijk is er een eenvoudige 1-op-1 relatie. Bijvoorbeeld, als een apotheek medicatieverstrekkingen aanmeldt bij de verwijzindex, komt diens dossier alleen in aanmerking voor opvraag van medicatieverstrekkingen.

De gegevenssoortentabel zal bestaan uit een lijst met regels die ieder bevatten:

- een gegevenssoort-id als *aanmeldbare* gegevenssoort,
- een HL7-interaction-id als *opleverbare* gegevenssoort.

Daarin kan iedere HL7-interactie en iedere gegevenssoort meer malen voorkomen. Op deze wijze kan één HL7-interactie gebonden worden aan meerdere *opleverbare* gegevenssoorten en andersom.

De onderstaande figuur geeft een voorbeeld (met suggestieve tekst in plaats van onbegrijpelijke codes) van deze tabel voor de zorgtoepassingen EMD en WDH.

Gegevenssoort	HL7-interaction
Index	opvragenIndex
Medicatievoorschrift	opvragenMedicatievooschriften
Medicatieverstrekking	opvragenMedicatieverstrekkingen
Eerstelijnsdossier	opvragenSamenvattingVoorDWH
Eerstelijnsdossier	opvragenSamenvattingVoorSEH

## 5.5 Autorisatieprotocol (APT)

Het autorisatieprotocol is een door koepelverenigingen gedefinieerde autorisatietabel die bepaalt *welke* soorten patiëntgegevens voor *welke* functies van zorgaanbieders toegankelijk zijn. Het autorisatieprotocol is bedoeld voor gebruik door het schakelpunt, maar kunnen eventueel ook door zorgaanbieders worden gebruikt voor de interne autorisatie of voor inzage door zorgverleners.

Uit oogpunt van *vertrouwelijkheid* zijn er geen beperkingen: iedereen mag het autorisatieprotocol inzien en vrij kopiëren.

Uit oogpunt van *integriteit* is het belangrijk te kunnen achterhalen wie het autorisatieprotocol heeft aangepast, bijv. door middel van een autorisatielog.

Uit oogpunt van *beheerbaarheid* is het wenselijk het autorisatieprotocol centraal te onderhouden.

Architectuurbeslissingen:

**APT·b01** Er komt één centraal beheerd autorisatieprotocol t.b.v. landelijke uitwisseling van patiëntgegevens via het schakelpunt.

**APT·b02** {toekomst} Zorgaanbieders kunnen een lokale kopie van dit autorisatieprotocol maken t.b.v. inzage of autorisatie van de interne uitwisseling van patiëntgegevens.

**APT·b03** {toekomst} Als gevolg van architectuurbeslissing [ovg·b03] zal het autorisatieprotocol de historie van wijzigingen moeten bijhouden tot aan de afgesproken reconstructiehorizon.

Het autorisatieprotocol zal bestaan uit:

- een algemeen autorisatieprotocol, dat bestaat uit een aantal autorisatieregels met:
  - opvragende zorgpartij
  - opleverende zorgpartij
  - de gegevensklasse
  - de bevoegde algemene gebruikersinteractie, zie [Technische Architectuur] paragraaf 5.1,
  - autorisatieniveau: voorlopig alleen de indicatie wél of géén toegang
  - vereiste logging: wel, niet
  - vereiste vertrouwensniveau: laag, midden, hoog
  - ingangsdatum van wijziging
  - identiteit van de beheerder die de regel heeft vastgelegdbehalve voor de combinatie *zorgaanbieder/zorgaanbieder/medisch*, want daarvoor geldt het *medische* autorisatieprotocol.
- een medisch autorisatieprotocol, dat bestaat uit een aantal autorisatieregels met:
  - de functie van de opvragende zorgverlener
  - de betrokkenheid van de opvragende zorgverlener
  - de bevoegde medische gebruikersinteractie, zie [Technische Architectuur] paragraaf 5.1,

- autorisatieniveau: voorlopig alleen de indicatie wél of géén toegang
  - vereiste vertrouwensniveau: laag, midden, hoog
  - ingangsdatum van wijziging
  - identiteit van de beheerder die de regel heeft vastgelegd
- een autorisatielog bestaande uit alle historische wijzigingen met telkens:
    - datum en tijd dat de wijziging is doorgevoerd
    - identiteit van de beheerder of {toekomst} patiënt/cliënt die de wijziging heeft doorgevoerd.

Autorisatieregels die worden overschreven door een nieuwe autorisatieregels, zijn daarna alleen nog interessant voor auditdoeleinden en de reconstructie van een historische opvraag door de toezichthouder. Aldus kunnen overschreven autorisatieregels worden opgeborgen in een *autorisatielog*, die kan worden gearchiveerd naar een off-line opslagmedium.

## 5.6 Autorisatieprofiel (APF)

Het autorisatieprofiel bestaat uit een groot aantal individuele profielen, één voor iedere patiënt/cliënt die ooit heeft aangegeven al of niet akkoord te gaan met elektronische uitwisseling van zijn patiëntgegevens.

Uit oogpunt van *vertrouwelijkheid* mogen zorgverleners geen autorisatieprofielen inzien. Immers, als een patiënt/cliënt zijn buurman wil uitsluiten, die toevallig als apotheker in een ziekenhuis werkt, mag die apotheker niet in dat autorisatieprofiel kunnen zien dat hij is uitgesloten door zijn buurman.

Uit oogpunt van *integriteit* is het belangrijk te kunnen achterhalen wie de autorisatieprofielen heeft aangepast, bijv. door middel van een autorisatielog.

Uit oogpunt van *schaalbaarheid* zijn kopieën van alle (potentieel 16 miljoen) autorisatieprofielen lastig te distribueren over de vele zorgaanbieders. Het zou ook niet doelmatig zijn, als men bedenkt dat een patiënt/cliënt slechts enkele zorgaanbieders bezoekt. In het genoemde voorbeeld m.b.t. vertrouwelijkheid, kan de patiënt/cliënt beter kiezen om dat ziekenhuis te vermijden óf dat ziekenhuis te vragen een intern autorisatieprofiel in te stellen t.b.v. hun interne uitwisseling van patiëntgegevens.

Uit oogpunt van *beheerbaarheid* is het wenselijk de centrale autorisatieprofielen te laten onderhouden door een autorisatiebeheerder, die op verzoek van patiënten/cliënten aanpassingen doorvoert. In de toekomst is aanpassing door de patiënt/cliënt zelf via Internet mogelijk.

Uit oogpunt van *actualiteit* kan een aanpassing van een centraal of lokaal autorisatieprofiel onmiddellijk ingaan. Frequente wijzigingen worden pas verwacht als de patiënt/cliënt zelf toegang via Internet krijgt.

Architectuurbeslissingen:

**APF·b01** Er komt per patiënt één centraal beheerd autorisatieprofiel t.b.v. landelijke uitwisseling van patiëntgegevens via het schakelpunt.

**APF·b02** Zorgaanbieders kunnen per patiënt een eigen, intern autorisatieprofiel onderhouden t.b.v. interne uitwisseling van patiëntgegevens.

**APF·b03** {toekomst} Als gevolg van architectuurbeslissing [ovg·b03] zal het autorisatieprofiel de historie van wijzigingen moeten bijhouden tot aan de afgesproken reconstructiehorizon.

Een centraal autorisatieprofiel van een patiënt/cliënt bestaat uit:

- een akkoordprofiel met afzonderlijke indicaties van de patiënt/cliënt of hij wel/niet akkoord gaat met:
  - elektronische uitwisseling van zijn patiëntgegevens,
  - {toekomst} elektronisch inkijken in de toegangslog door hemzelf,
  - {toekomst} elektronisch inkijken in zijn autorisatieprofiel door hemzelf,
  - {toekomst} elektronisch wijzigen van zijn autorisatieprofiel door hemzelf, met voor iedere indicatie

- {toekomst} vereiste vertrouwensniveau
- nul of meer autorisatieregels, die ieder bestaan uit:
  - opvragende zorgpartij, eventueel uitgedrukt in functie of identiteit
  - de gegevensklasse,
  - een indicatie met de waarde:
    - altijd
    - alleen in noodsituatie
    - na expliciete toestemming
    - nooit
  - eventueel de persoon van wie de expliciete toestemming wordt verlangd
  - vereiste vertrouwensniveau
- een autorisatielog bestaande uit alle historische wijzigingen met telkens:
  - datum en tijd dat de wijziging is doorgevoerd
  - identiteit van de beheerder of {toekomst} patiënt/cliënt die de wijziging heeft doorgevoerd.

Naast alle patiënt/cliënt-specifieke autorisatieprofielen is er een generieke tabel met verstekwaarden voor de akkoordprofielen. Voor autorisatieregels zijn geen verstekwaarden nodig, want nul autorisatieregels betekent op grond van BAF·b02: géén inperking van de bevoegdheden zoals bepaald in het autorisatieprotocol.

Een intern autorisatieprofiel van een patiënt/cliënt bestaat slechts uit nul of meer autorisatieregels zoals hierboven beschreven.



## 5.7 Identificatie & authenticatie-module (I &A)

De identificatie & authenticatie-module wordt hier gedefinieerd als de eenheid die ten behoeve van het schakelpunt:

- zorgverleners en {toekomst} patiënten/cliënten identificeert en authenticceert aan de hand van hun persoonsgebonden vertrouwensmiddel wanneer zij inloggen op het schakelpunt,
- patiëntdossiers en zorgaanbiederpostbussen identificeert en authenticceert aan de hand van hun systeemgebonden vertrouwensmiddel wanneer zij worden aangesproken door het schakelpunt,
- zichzelf identificeert en authenticceert bij inloggende zorgverleners en {toekomst} patiënten/cliënten en aangesproken patiëntdossiers en zorgaanbiederpostbussen.

Gegeven de keuze voor PKIO, zie het document [Technische Architectuur], zal de identificatie & authenticatie-module ook zelf een systeemgebonden vertrouwensmiddel bevatten.

Uit oogpunt van *authenticiteit* van het schakelpunt, dient het vertrouwensmiddel fysiek te zijn beschermd tegen kopiëren of ongeautoriseerd verwijderen.

Uit oogpunt van *schaalbaarheid* kan ieder schakelpunt zijn eigen identificatie & authenticatie-module hebben, maar kunnen schakelpunten ook een gezamenlijke module hebben.

Uit oogpunt van *actualiteit* is het noodzakelijk dat deze module geregeld de lijst met ingetrokken vertrouwensmiddelen ophaalt van de CA van het zorgverlenerregister.

De identificatie & authenticatie-module dient de volgende *operaties* te kunnen afhandelen op verzoek van een schakelpunt:

- het identificeren en authenticeren van zorgverleners en {toekomst} patiënten/cliënten, patiëntdossiers en zorgaanbiederpostbussen op basis van hun vertrouwensmiddelen,
- het opzetten van beveiligde sessies met de applicaties die deze zorgverleners en {toekomst} patiënten/cliënten gebruiken of de applicaties die deze patiëntdossiers en zorgaanbiederpostbussen ontsluiten.

## 5.8 Toegangslog (LOG)

De toegangslog dient om de toezichthouder, zorgaanbieders en patiënten/cliënten te kunnen laten achterhalen welke patiëntgegevens ooit landelijk (en eventueel intramuraal) zijn uitgewisseld, zie paragraaf 4.14.

Ten behoeve van de toezichthouder, die een bewijs wil kunnen vinden dat een zorgaanbieder bepaalde patiëntgegevens heeft ingezien, zou er een centraal beheerde log moeten zijn, waarin alle landelijk uitgewisselde patiëntgegevens inhoudelijk worden gelogd. Maar daarmee zou een nieuwe, centrale vastlegging van patiëntgegevens ontstaan, hetgeen niet beantwoordt aan het doel van de toegangslog. Daarom moet een centrale log alleen de metagegevens (waaronder de uitgevoerde gebruikersinteractie) bevatten, onder verwijzing naar de plaats waar de inhoud gelogd is, of anderszins terug te vinden is.

Ten behoeve van de beheerverantwoordelijke zorgaanbieder, die moet kunnen achterhalen wie zijn patiëntdossiers heeft ingezien, moet er toch al een lokale log worden bijgehouden. Deze lokale log hoeft de (berichten met) uitgewisselde patiëntstukken niet per sé inhoudelijk te bevatten, indien de afkomstige zorgapplicatie die patiëntstukken kan reconstrueren als gevolg van architectuurbeslissing [OPV·b03], of indien het afkomstige patiëntdossier alle afzonderlijke versies van patiëntstukken bewaart als gevolg van architectuurbeslissing [PDO·b01].

Ten behoeve van de toezichthouder, die wil kunnen achterhalen wat een zorgaanbieder precies heeft gezien na het opvragen van een index van beschikbare gegevenssoorten, zouden de ontvangen indexregels inhoudelijk moeten worden gelogd. In plaats daarvan kan de inhoud van de verwijzindex op een bepaald tijdstip ook worden gereconstrueerd. Als gevolg van architectuurbeslissing [OPV·b03] moet dit toch al, dus verdient deze variant de voorkeur. Dat betekent wel dat alle interacties van een zorgaanbieder met het schakelpunt centraal moeten worden gelogd.

Uit oogpunt van *vertrouwelijkheid* vindt de eventuele inhoudelijke logging plaats bij het patiëntdossier waaruit de uitgewisselde patiëntstukken afkomstig zijn. In geval van gebruikersinteractie *versturen* is dat die van de agerende partij, in geval van *opvragen* is dat de reagerende partij. Op deze wijze wordt onbedoelde proliferatie van patiëntstukken voorkomen.

Uit oogpunt van *integriteit* is het belangrijk dat oude logregels leesbaar blijven, ook als de daarin gebruikte codes en identiteiten zijn vervallen. Dit vereist dat de desbetreffende codetabellen en registers de vervallen codes en identiteiten kan reconstrueren of dat de codes in de logregel worden vervangen.

Uit oogpunt van *volledigheid* is het belangrijk dat ook eventuele pogingen tot uitwisseling van patiëntgegevens worden gelogd van patiënten/cliënten die daartegen bezwaar hebben gemaakt. Dit is belangrijk opdat deze patiënten/cliënten na raadpleging van de toegangslog kunnen vaststellen dat hun bezwaar is ingewilligd en dat dit ook het gewenste resultaat heeft.

Uit oogpunt van *beheerbaarheid* is het wenselijk de centrale toegangslog te laten beheren door een logbeheerder, die op verzoek van patiënten/cliënten de toegangslog doorzoekt.

Uit oogpunt van *schaalbaarheid* is het wenselijk dat patiënten/cliënten zelf de toegangslag doorzoeken. In de toekomst wordt dit via Internet mogelijk.

Uit oogpunt van *doelmatigheid* moet de toegangslag geen redundante identificerende gegevens van agerende en reagerende zorgaanbieders en zorgverleners bevatten, maar alleen hun zorgaanbieder-id resp. zorgverlener-id. Een applicatie die de inhoud van de toegangslag toont, kan deze id's vertalen naar herkenbare gegevens met behulp van de zorgaanbieder*gids*. In afwachting van de zorgaanbieder*gids*, zouden deze herkenbare gegevens tijdelijk alsnog in de toegangslag kunnen worden opgenomen, maar doelmatiger is het gebruik van een aparte zorgaanbieder *tabel*, zie verder paragraaf 5.13.

Architectuurbeslissingen:

**LOG·b01** De toegangslag zal alle gebruikersinteracties loggen:

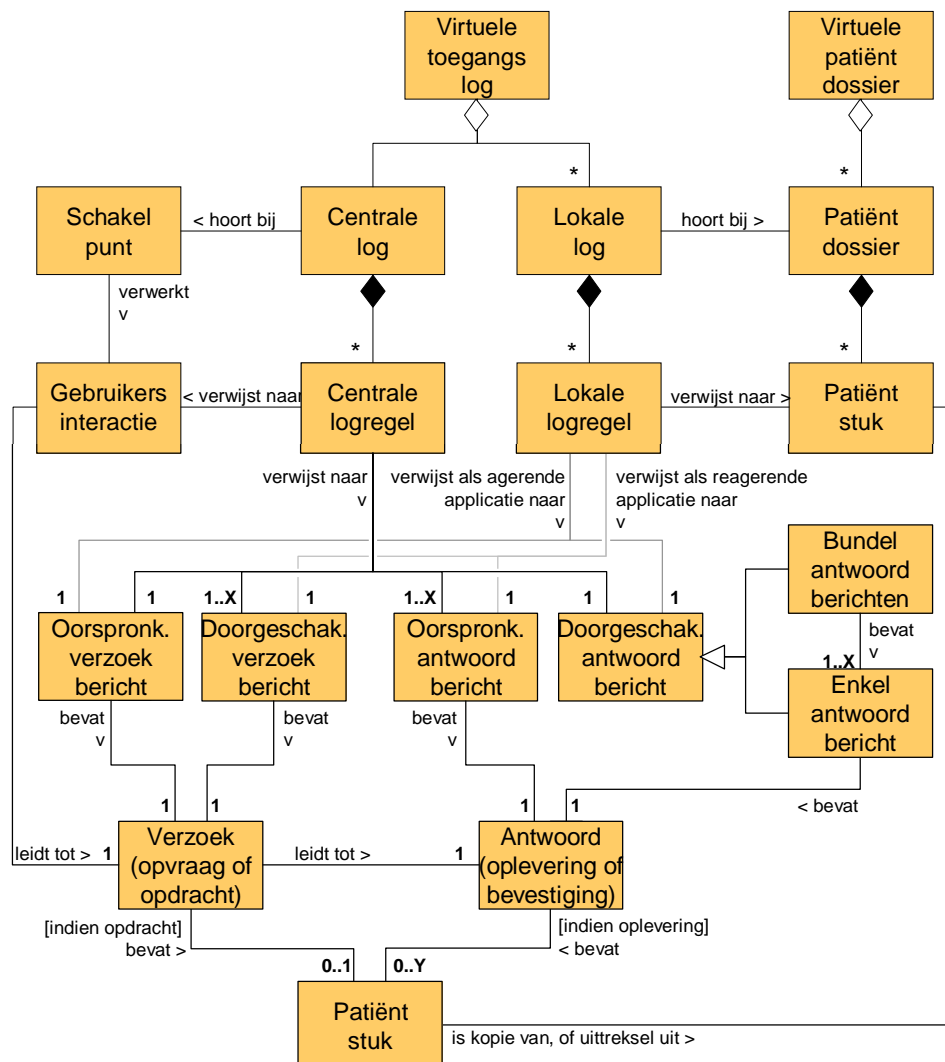
- {toekomst} aansluiten en afsluiten van een applicatie,
  - inloggen en uitloggen van gebruiker,
  - opvragen, versturen van patiëntgegevens,
  - opvragen index van gegevenssoorten,
  - aanmelden en afmelden van gegevenssoorten,
- ongeacht of de patiënt/cliënt bezwaar heeft gemaakt tegen elektronische uitwisseling van zijn patiëntgegevens.

**LOG·b02** {toekomst} De eventuele inhoudelijke logging vindt plaats bij de bron: het patiëntdossier waaruit de uitgewisselde patiëntstukken afkomstig zijn.

**LOG·b03** De toegangslag zal omvatten:

- een centrale log bij ieder schakelpunt, met daarin alle uitgevoerde gebruikersinteracties, met verwijzingen naar de zorgaanbieder van wie ze afkomstig zijn en het patiëntdossier waaruit ze afkomstig zijn.
- een lokale log bij ieder (applicatie met) patiëntdossier, met daarin alle gebruikersinteracties waarbij dit patiëntdossier als bron van de patiëntgegevens fungeerde.

De toegangsllog wordt dus een virtuele log. De onderstaande figuur toont dit, in een UML class diagram, waarbij de logregels zijn uitgewerkt voor de interacties *indirect opvragen* en *indirect versturen* van patiëntgegevens.



Het diagram is gebaseerd op de UML class diagrammen in [Technische Architectuur] paragraaf 5.2 en 5.3. De aldaar genoemde bericht-id's, opvraag-id's, patiëntstuk-id's en gebeurtenis-id's kunnen in de toegangsllog worden gebruikt om de relaties vast te leggen tussen:

- de initiërende gebruikersinteractie (gebeurtenis-id),
- de eventueel daaruit voortkomende opvraagssessie (opvraag-id),
- de uitgewisselde patiëntstukken (patiëntstuk-id),
- de berichten waarin die patiëntstukken zijn uitgewisseld (bericht-id).

Merk verder op dat:

- het schakelpunt alle berichten van iedere gebruikersinteractie logt,
- een (applicatie met) patiëntdossier in principe alleen de berichten logt van:
  - de interactie *indirect opvragen* als reagerende (opleverende) applicatie,
  - de interactie *indirect versturen* als agerende (versturende) applicatie.

Een centrale toegangslag zal aldus bestaan uit een reeks logregels, met voor iedere logregel de volgende attributen:

- het tijdstip: jaar, maand, dag, uur, minuut, seconde, milliseconde,
- het type en het volgnummer van de uitgevoerde gebruikersinteractie,
- indicatie van een eventueel opgetreden foutsituatie m.b.t. het schakelpunt,
- in geval van aansluiten, afsluiten, inloggen of uitloggen:
  - het vertrouwensniveau: hoog, midden, laag,
  - in geval van vertrouwensniveau *laag*:
    - de identiteit van de inloggende zorgaanbieder,
    - een referentie naar het gebruikte UZI-servicescertificaat,
  - in geval van vertrouwensniveau *midden*:
    - de functie en identiteit van de inloggende zorgverlener of medewerker,
    - een referentie naar het certificaat van de gebruikte UZI-pas,
  - het resultaat van de authenticatiecontrole,
- in geval van aanmelden, afmelden, opvragen of versturen:
  - de identiteit van de patiënt/cliënt,
  - de identiteit van de agerende zorgaanbieder,
  - de functie en identiteit van de agerende zorgverlener of medewerker,
  - indien van toepassing: de functie en identiteit van de mandaterende zorgverlener,
  - de identiteit van de agerende applicatie,
  - de gebruikersinteractie,
  - het resultaat van de autorisatiecontrole,
  - {toekomst} de episode waarvoor deze gebruikersinteractie is uitgevoerd,
  - {toekomst} de reden waarom deze gebruikersinteractie is uitgevoerd,
  - een indicatie of een beroep was gedaan op een noodsituatie,
- in geval van *opvragen index*:
  - de bericht-id van het opleverbericht,
  - het aantal retries dat nodig was voor het terugsturen van het opleverbericht, zie het document [Technische Architectuur] onder betrouwbaarheid,
  - een indicatie van een eventueel opgetreden foutsituatie m.b.t. het terugsturen van het opleverbericht,
- in geval van opvragen patiëntgegevens,
  - de bericht-id van het originele opvraagbericht,
  - in geval van een bundel: de bericht-id van de bundel van geconvergeerde opleverberichten,
  - het aantal retries dat nodig was voor het verzenden van het geconvergeerde opleverbericht,
  - een indicatie van een eventueel opgetreden foutsituatie m.b.t. het convergeren van het opleverbericht,

met daarnaast per reagerende (opleverende) applicatie:

- de identiteit van de reagerende zorgaanbieder,
- de functie en eventueel identiteit van de beheerverantwoordelijke zorgverlener,
- de identiteit van de reagerende applicatie, die diens dossiers ontsluit,
- de bericht-id van het gedivergeerde opvraagbericht,
- indicatie van een eventueel opgetreden foutsituatie m.b.t. het divergeren van het opvraagbericht,
- de bericht-id van het originele opleverbericht,
- de bericht-id van het geconvergeerde opleverbericht,
- in geval van versturen patiëntgegevens:
  - de bericht-id van het opdrachtbericht,
  - de identiteit van de reagerende (bestemde) zorgaanbieder,
  - de functie en eventueel identiteit van de bestemde zorgverlener,

- de identiteit van de reagerende applicatie, die diens postbus ontsluit,
- een indicatie van een eventueel opgetreden foutsituatie m.b.t. het doorsturen van het opdrachtbericht,
- de bericht-id van bevestigbericht,
- het aantal retries dat nodig was voor het doorsturen van het bevestigbericht, zie [Technische Architectuur] paragraaf 12.3,
- een indicatie van een eventueel opgetreden foutsituatie m.b.t. het doorsturen van het bevestigbericht.

Een lokale toegangslag zal bestaan uit een reeks logregels, met voor iedere logregel de volgende attributen:

- de identiteit van de patiënt/cliënt,
- indien van toepassing: de functie en identiteit van de mandaterende zorgverlener,
- het tijdstip: jaar, maand, dag, uur, minuut, seconde, milliseconde,
- het type en het volgnummer van de uitgevoerde gebruikersinteractie (tenminste *opvragen* en *versturen patiëntgegevens* vanuit het bijbehorende patiëntdossier),
- indicatie van een eventueel opgetreden foutsituatie mbt het schakelpunt,
- in geval van opvragen patiëntgegevens:
  - de identiteit van de agerende (opvragende) zorgaanbieder,
  - de functie en identiteit van de agerende zorgverlener of medewerker,
  - de bericht-id van het gedivergeerde opvraagbericht,
  - de bericht-id van het originele opleverbericht,
  - indicatie van een eventueel opgetreden foutsituatie m.b.t. het terugsturen van het opleverbericht,
  - de patiëntstuk-id's van in het opleverbericht aanwezige patiëntstukken,
- in geval van versturen patiëntgegevens:
  - de identiteit van de reagerende (bestemde) zorgaanbieder,
  - de functie en identiteit van de reagerende zorgverlener, indien vermeld,
  - de identiteit van de reagerende applicatie, die diens postbus ontsluit,
  - de bericht-id van het opdrachtbericht,
  - de patiëntstuk-id van in het opdrachtbericht aanwezige patiëntstuk,
  - een indicatie van een eventueel opgetreden foutsituatie m.b.t. het versturen van het opdrachtbericht,
  - de bericht-id van het bevestigbericht.

Indien het lokale patiëntdossier niet in staat is de historisch opgeleverde patiëntstukken te reconstrueren, moet de toegangslag ook de inhoud van alle opgeleverde of verstuurd patiëntstukken met hun patiëntstuk-id bevatten.

Opmerkingen:

- In theorie is een lokale toegangslag niet noodzakelijk. Zorgverleners zouden namelijk rechtstreeks kunnen inkijken in hun deel van de centrale toegangslag. Er moeten dan nog wel HL7v3-berichten worden gedefinieerd voor het uitwisselen van logregels. Ook zou de centrale toegangslag dan de patiëntstuk-id's van de uitgewisselde patiëntstukken moeten bevatten. Voordeel van de huidige opzet is dat men niet geheel afhankelijk is van de centrale toegangslag, maar deze zonodig kan verifiëren met de lokale toegangslagen.
- De lokale toegangslag bij een bepaald patiëntdossier dient primair voor het reconstrueren van welke patiëntstukken precies zijn ingezien door een *andere* zorgaanbieder. Daarnaast mag een lokale toegangslag ook bijhouden welke andere gebruikersinteracties hebben plaatsgevonden m.b.t. dat patiëntdossier, zoals het

aanmelden en afmelden van gegevenssoorten. Maar dat voegt inhoudelijk niets toe aan de centrale toegangslog, omdat deze logregels niet naar afzonderlijke patiëntstukken verwijzen.

- Voor het loggen van de eventuele interne uitwisseling van patiëntgegevens kan een lokale log ook logregels bevatten met attributen zoals gespecificeerd voor de centrale log.
- Een gedoseerde opvraag bestaat uit een eerste opvraag van N patiëntstukken en een willekeurig aantal opvragingen voor de volgende N patiëntstukken. Hierbij wordt iedere (vervolg)opvraag als een afzonderlijk te loggen gebruikersinteractie beschouwd.
- De toegangslog heeft geen betrekking op de autorisatietabellen en andere centrale tabellen. Voor het loggen van beheeracties op die tabellen, zie aldaar.

Openstaande punten:

- De waarde van het lokaal loggen van de berichtinhoud bij de bron, zie [LOG·b02], staat nog ter discussie. Als het erom gaat te bepalen welke patiëntgegevens een zorgverlener precies heeft gezien na opvraag, is er geen garantie dat diens gebruikersapplicatie al die berichtinhoud ook heeft getoond aan de zorgverlener. In plaats daarvan zou het loggen van de scherminhoud (*screen dumps*) meer zekerheid geven, maar dat moet dan niet bij de bron, maar bij de bestemming gebeuren, hetgeen in strijd is met paragraaf 4.9 eis [OPV·e11].

## 5.9 Mandateringstabel (MDT)

In een mandateringstabel kan een zorgverlener vastleggen welke andere zorgverleners (als medebehandelaar) en/of medewerkers zijn gemandateerd om namens hem landelijk patiëntgegevens uit te wisselen, zie paragraaf 4.15.

Uit oogpunt van *integriteit* mogen alleen zorgverleners hun eigen mandateringen vastleggen, raadplegen, wijzigen en verwijderen. Dit is belangrijk omdat de mandaterende zorgverlener verantwoordelijk blijft voor de handelingen van de door hem gemandateerde medebehandelaren en medewerkers.

Uit oogpunt van *vertrouwelijkheid* mogen alleen gemandateerde medebehandelaren en medewerkers inzage krijgen in de aan hen toegekende mandateringen. Zij hebben deze inzage nodig alvorens de aan hen gemandateerde bevoegdheden te kunnen uitoefenen.

{toekomst} Uit oogpunt van *doeltreffendheid* is er idealiter één centrale mandateringstabel, zodat het schakelpunt zelfstandig kan verifiëren of een medebehandelaar of medewerker gemandateerd is voor landelijke uitwisseling van patiëntgegevens.

Uit oogpunt van *beheerbaarheid* heeft iedere zorgverlener zijn eigen mandateringstabel binnen handbereik. Dit wringt met de doeltreffendheid, maar voorlopig wordt gekozen voor een lokale tabel, want een centrale tabel zou nieuwe HL7v3-berichten vergen voor de uitwisseling van mandateringen tussen lokale zorgapplicatie en het centrale schakelpunt.

Architectuurbeslissingen:

**MDT·b01** Er komt een lokale mandateringstabel voor iedere zorgverlener die als hoofdbehandelaar kan optreden.

**MDT·b02** {toekomst} Als gevolg van architectuurbeslissing [OPV·b03] zal de mandateringstabel de historie van wijzigingen moeten bijhouden tot aan de afgesproken reconstructiehorizon.

De mandateringstabel bestaat uit een aantal mandateringsregels met ieder:

- de identiteit van de mandaterende zorgverlener,
- de identiteit van de gemandateerde zorgverlener of medewerker,
- de bevoegde medische gebruikersinteractie(s), zie [Technische Architectuur] paragraaf 5.1,
- een ingangsdatum,
- eventueel een verloopdatum.



## 5.10 Patiëntenregister (PAR)

Het patiëntenregister is een tabel met identificerende gegevens van (potentiële) patiënten/cliënten.

Uit oogpunt van *vertrouwelijkheid* mag het patiëntenregister geraadpleegd worden door alle zorgaanbieders en medewerkers voor het opvragen of verifiëren van een patiëntnummer, maar niet voor het opvragen van de bijbehorende identificerende gegevens, zie paragraaf 4.3.

Uit oogpunt van *doeltreffendheid* is er idealiter één landelijk patiëntenregister, waar alle potentiële patiënten/cliënten in te vinden zijn met een landelijk patiëntnummer. In plaats daarvan zou men ook meerdere (bijv. regionale) patiëntenregisters kunnen opzetten, maar groot risico daarvan is dat een patiënt/cliënt niet kan worden gevonden, omdat hij in een ander register staat, en dus een tweede patiëntnummer krijgt toegewezen.

Uit oogpunt van *beschikbaarheid* is het wenselijk dat zorgaanbieders zelf de patiëntnummers met bijbehorende identificerende gegevens en bereikbaarheidsgegevens van zijn patiënten/cliënten opneemt in zijn patiëntdossier of een interne patiëntenindex, mocht de zorgaanbieder afzonderlijke dossiers per afdeling hebben.

Uit oogpunt van *beheerbaarheid* is het wenselijk dat zorgaanbieders worden ingelicht over eventuele wijzigingen van identificerende of bereikbaarheidsgegevens van patiënten/cliënten.

Ontwerpbeslissingen:

**PAR·b01** Er is één landelijk patiëntenregister nodig waar landelijke patiëntnummers kunnen worden opgevraagd en geverifieerd voor tenminste alle Nederlandse ingezetenen.

**PAR·b02** {toekomst} Als gevolg van ontwerpbeslissing [OPV·b03] zal het landelijke patiëntenregister de historie van wijzigingen moeten bijhouden tot aan de afgesproken reconstructiehorizon.

Het landelijke patiëntenregister wordt ingevuld door de BVBSN (beheervoorziening burgerservicenummer), die voor zorgpartijen raadpleegbaar is via de SBV-Z (sectorale berichtenvoorziening in de zorg), zie verder [BSN] en [SBV-Z].

Een intern patiëntenregister, meestal patiëntenindex genoemd, al dan niet als onderdeel van een patiëntdossier, bevat identificerende gegevens van de patiënt/cliënt, waaronder het BSN, zonodig aangevuld met de volgende vlaggen en attributen:

- vlag of het BSN is opgevraagd of geverifieerd en zo ja:
  - bron van het BSN
- vlag of het WID is gecontroleerd op echtheid, geldigheidsdatum en gelijkenis met de patiënt/cliënt en zo ja:
  - aard van het WID
  - nummer van het WID
- vlag dat op andere wijze is vergewist van de identiteit van de patiënt/cliënt,
- vlag of het WID is gecontroleerd op het in omloop mogen zijn en zo ja:
  - aard van het WID

- nummer van het WID
- vlag of de identificerende gegevens zijn bijgewerkt:
- vlag of de patiëntgegevens inhoudelijk zijn gecontroleerd met de patiënt/cliënt.

Bij iedere vlag kan worden vermeld:

- resultaat van de controle
- datum en tijd van de desbetreffende controle
- identificatie van de controlerende zorgverlener/medewerker
- zorgverlenersnummer van de mandaterende zorgverlener, indien van toepassing.

De laatste vlag kan per dossier worden bijgehouden, mocht de zorgaanbieder afzonderlijke dossiers per afdeling hebben. De vlag kan ook per patiëntstuk worden bijgehouden, zie ook een van de opmerkingen bij eis [BIJ.e02] in paragraaf 4.5.

Het landelijke patiëntenregister dient de volgende *operaties* te kunnen afhandelen op verzoek van het schakelpunt:

- het zowel interactief als bestandgewijs opleveren of verifiëren van het BSN van een patiënt/cliënt op basis van een zoekpad van identificerende gegevens.

## 5.11 Zorgaanbiederregister (ZAR)

Het zorgaanbiederregister is een tabel met identificerende gegevens van certificaten van vertrouwensmiddelen aangevraagd door zorgaanbieders en uitgegeven aan zorgverleners, medewerkers en hun zorgsystemen. Ook publiceert het een lijst van ingetrokken vertrouwensmiddelen.

Uit oogpunt van *vertrouwelijkheid* kan het register beperkt geraadpleegd worden door de geregistreerde zorgaanbieders, als toetsingsregister; er kan niet in worden gebladerd, zie paragraaf 4.4.

Uit oogpunt van *doeltreffendheid* is er idealiter één landelijk zorgaanbiederregister, maar in plaats daarvan zou men ook meerdere (bijv. regionale) zorgaanbiederregisters kunnen opzetten.

Uit oogpunt van *integriteit* is het zeer belangrijk te kunnen vertrouwen op de juistheid van de gegevens in het register.

Uit oogpunt van *beheerbaarheid* is het wenselijk het zorgaanbiederregister centraal te onderhouden, maar lokale inschrijving bij een RA mogelijk te maken.

Uit oogpunt van *actualiteit* is het noodzakelijk om de lijst van ingetrokken vertrouwensmiddelen (CRL) regelmatig te publiceren. Tevens moet het mogelijk zijn een vertrouwensmiddel rechtstreeks op geldigheid te laten controleren door het register (OCSP).

Ontwerpbeslissingen:

**ZAR·b01** {toekomst} Als gevolg van ontwerpbeslissing [OPV·b03] zal het zorgaanbiederregister de historie van wijzigingen moeten bijhouden tot aan de afgesproken reconstructiehorizon.

**ZAR·b02** Als gevolg van ontwerpbeslissing [zag·b01] zal het zorgaanbiederregister alle wijzigingen in identificerende gegevens spontaan moeten aanmelden bij de zorgaanbiedergids.

Het zorgaanbiederregister dient de volgende *operaties* te kunnen afhandelen op verzoek van de identificatie&authenticatiemodule:

- het opleveren van naam, plaats en type van een zorgaanbieder voor een opgegeven zorgaanbieder-id,
- het opleveren van alle identificerende gegevens van een zorgverlener, medewerker of systeem voor een opgegeven zorgverlener-id,
- het opleveren van een lijst met ingetrokken vertrouwensmiddelen (CRL),
- het controleren van de geldigheid van de opgegeven vertrouwensmiddel (OCSP),
- het opleveren van (een certificaat met) de publieke sleutel van het opgegeven type voor de opgegeven zorgverlener-id.

Het zorgaanbiederregister dient de volgende *operaties* te kunnen afhandelen ten behoeve van de zorgaanbiedergids:

- het spontaan aanmelden van wijzigingen in identificerende gegevens van zorgverleners, medewerkers of systemen,

- het op verzoek opleveren van alle identificerende gegevens van een zorgverlener, medewerker of systeem voor een opgegeven zorgverlener-id,

Opmerkingen:

- Als zorgaanbiederregister heeft het ministerie van VWS reeds het UZI-register van CIBG aangewezen. Toch beoogt deze paragraaf alsnog eisen te formuleren voor *een* dergelijk zorgaanbiederregister, geredeneerd vanuit de behoefte van het landelijk uitwisselen van patiëntgegevens. Dit is belangrijk om te kunnen toetsen of het gerealiseerde UZI-register voorziet in de behoefte. Sommige zaken kunnen echter geheel aan CIBG worden gelaten, zie ook paragraaf 4.20.
- Het UZI-register is niet zozeer een register van *zorgaanbieders*, maar een register van *zorgverleners*, hun medewerkers en hun systemen aan wie een vertrouwensmiddel is uitgegeven. Het UZI-register registreert voor ieder vertrouwensmiddel door welke abonnee het is aangevraagd. Alleen zorgaanbieders kunnen abonnee worden. Dit betekent dat het UZI-register alsnog kan fungeren als zorgaanbiederregister en het abonnee-nr (URA) kan fungeren als zorgaanbieder-id.
- Vooral het schakelpunt heeft de lijst van ingetrokken vertrouwensmiddelen (CRL) nodig om de UZI-passen van zorgverleners die inloggen op het schakelpunt te controleren op geldigheid. Zolang zorgaanbiederapplicaties uitsluitend via het schakelpunt gegevens uitwisselen, hebben die applicaties zelf niks nodig van het zorgaanbiederregister, behalve als UZI-passen ook worden gebruikt voor het lokaal inloggen, zie het document [Technische Architectuur]. Voor de verificatie van elektronische handtekeningen zullen applicaties straks wel het zorgaanbiederregister moeten raadplegen, vermoedelijk is OCSP dan doelmatiger dan een CRL.

## 5.12 { toekomst } Zorgaanbiedergids (ZAG)

De zorgaanbiedergids is een tabel met bereikbaarheidsgegevens van alle zorgaanbieders, en eventueel de daarbinnen werkende zorgverleners, die actief zijn (geweest).

Uit oogpunt van *vertrouwelijkheid* kan de zorgaanbiedergids geraadpleegd worden door alle zorgaanbieders die hun eigen gegevens hebben gepubliceerd. Ook patiënten/cliënten zouden in de toekomst toegang kunnen krijgen, zie paragraaf 4.4.

Uit oogpunt van *integriteit* wordt de zorgaanbiedergids eerst automatisch en onwijzigbaar gevuld vanuit het UZI-register, en kan pas daarna handmatig worden ingevuld door de zorgaanbieders zelf. De HL7-adressen die daarbij worden ingevuld, moeten worden getoetst op het bestaan ervan bij de GBZ-configuratietabel, zie paragraaf 5.14.

Uit oogpunt van *schaalbaarheid* is er idealiter één landelijk zorgaanbiedergids, maar in plaats daarvan kan men ook meerdere (bijv. regionale) zorgaanbiedergidsen opzetten.

Uit oogpunt van *beschikbaarheid* kunnen zorgaanbieders de bereikbaarheidsgegevens van collega's waar ze veel mee samenwerken, overnemen in hun lokale zorgaanbieder-adresboek.

Uit oogpunt van *beheerbaarheid* is het wenselijk dat zorgaanbieders zelf hun (frequent wijzigende) bereikbaarheidsgegevens onderhouden. Het automatisch propageren van aanpassingen is lastig.

Ontwerpbeslissingen:

**ZAG·b01** Wenselijk is één landelijke zorgaanbiedergids die automatisch consistent wordt gehouden met het zorgaanbiederregister en de configuratietabellen van het schakelpunt.

**ZAG·b02** Het zorgaanbiederregister moet identificerende gegevens aanleveren aan de zorgaanbiedergids.

**ZAG·b03** De GBZ-configuratietabel moet HL7-adressen aanleveren aan de zorgaanbiedergids.

**ZAG·b04** { toekomst } Als gevolg van ontwerpbeslissing [OPV·b03] zal de zorgaanbiedergids de historie van wijzigingen moeten bijhouden tot aan de afgesproken reconstructiehorizon.

De zorgaanbiedergids bestaat uit een groot aantal bereikbaarheidsprofielen, die ieder bestaan uit:

- zorgaanbieder-id of zorgverlener-id
- zorgaanbieder-type of zorgverlener-functie
- aangeboden zorgdiensten
- nul of meer bereikbaarheidsregels, die ieder bestaan uit:
  - adres, dit kan zijn een bezoekadres, fysiek postadres, elektronisch postadres (internet en HL7v3 applicatie-id) en telefoonnummer
  - één of meer beschikbare diensten op dat adres
  - één of meer openingstijden voor iedere dienst op dat adres

De zorgaanbiedergids dient de volgende *operaties* te kunnen afhandelen op verzoek van het schakelpunt:

- het opleveren van identificerende gegevens van zorgaanbieders en eventueel zorgverleners op basis van willekeurige zoekcriteria,
- het opleveren van het elektronische postadres van een zorgaanbieder of eventueel zorgverlener op basis van het opgegeven zorgaanbieder-id resp. zorgverlener-id.

Opmerkingen:

- De Zorgaanbiedergids lijkt dubbelop met het Zorgaanbiederregister, maar in het register kan niet vrij gezocht worden en kunnen ook geen bereikbaarheidsgegevens worden toegevoegd.
- Wanneer een zorgverlener voor meerdere zorginstellingen werkt, krijgt hij weliswaar afzonderlijke UZI-passen, maar houdt hij éénzelfde UZI-nummer. Dit betekent dat het UZI-nummer alleen onvoldoende is om een zorgverlener te selecteren.
- Het elektronische postadres kan zijn:
  - e-mailadres, conform RFC 821 en RFC 822,
  - application-id, conform HL7v3.

## 5.13 Zorgaanbiedertabel (ZAT)

De zorgaanbiedertabel is een tabel met bereikbaarheidsgegevens van zorgaanbieders, en eventueel de daarbinnen werkende zorgverleners, die in de verwijfsindex zijn vermeld. In afwachting van de zorgaanbiedergids is deze tabel nodig als aanvulling op:

- de verwijfsindex,
- de toegangslg.

Wanneer een zorgverlener/medewerker voor een bepaalde patiënt/cliënt de verwijfsindex opvraagt, zie gebruiksscenario [OPV-s01], of de toegangslg raadpleegt, zie gebruiksscenario [RLO-s01], zou zijn applicatie de daarin vermelde zorgaanbieder-id's en zorgverlener-id's willen vertalen naar de volgende herkenbare attributen:

- zorgaanbieder-naam
- zorgaanbieder-type
- zorgaanbieder-bezoeklocatie
- zorgverlener-naam,

want de abstracte zorgaanbieder-id's en zorgverlener-id's zeggen hem weinig.

Voor die vertaling is de zorgaanbiedergids bedoeld, maar zolang die nog niet is gerealiseerd, is een tijdelijke oplossing nodig in de vorm van een niet-direct raadpleegbare zorgaanbiedertabel. Om die tabel te kunnen vullen is het belangrijk dat tijdelijk de bovengenoemde attributen:

- door de zorgaanbieder worden vermeld bij iedere aanmelding en heraanmelding van patiëntgegevens bij de verwijfsindex. Het schakelpunt moet deze vastleggen in zijn zorgaanbiedertabel. Het gaat hier alleen om de attributen van de *beheerverantwoordelijke*,
- door het schakelpunt worden vermeld bij alle opgeleverde verwijfsingen na opvraag van de verwijfsindex door een zorgverlener/medewerker. Het gaat hier om de attributen van zowel de *inhoudverantwoordelijke* als de *beheerverantwoordelijke*,
- door de agerende zorgaanbieder worden vermeld bij het opvragen of versturen van patiëntgegevens bij of naar andere zorgaanbieders. De applicatie van de reagerende zorgaanbieder moet deze vastleggen in zijn zorgaanbiedertabel.

Uit oogpunt van *doelmatigheid* moeten de attributen niet worden opgeslagen in de verwijfsindex of toegangslg, maar in een aparte tabel. Anders zouden de verwijfsindex en toegangslg veel redundante gegevens bevatten. Bijkomend voordeel van een aparte tabel is dat, bijv. bij verhuizing van een zorgaanbieder, een enkele heraanmelding voldoende is om een nieuwe zorgaanbieder-bezoeklocatie vast te leggen.

Uit oogpunt van *integriteit* moet het schakelpunt bij ontvangst van een (her-) aanmelding alleen de attributen van de *beheerverantwoordelijke* zorgaanbieder en zorgverlener opslaan in de tabel en niet die van de *inhoudverantwoordelijke*. Anders zouden zorgaanbieders elkaars attributen kunnen gaan overschrijven, zie ook bijlage C.

De zorgaanbieder*tabel* bestaat aldus uit een aantal regels die ieder bestaan uit:

- zorgaanbieder-id
- zorgaanbieder-naam
- zorgaanbieder-type
- zorgaanbieder-bezoeklocatie

en een aantal regels die ieder bestaan uit:

- zorgverlener-id
- zorgverlener-naam.

Opmerkingen:

- Omdat er nog geen geschikte berichten zijn voor het uitwisselen van de bovenstaande identificerende en bereikbaarheidsgegevens, zal iedere applicatie zijn eigen lokale zorgaanbieder*tabel* moeten hebben, in plaats van een gemeenschappelijke tabel, zoals de zorgaanbieder*gids* was bedoeld.



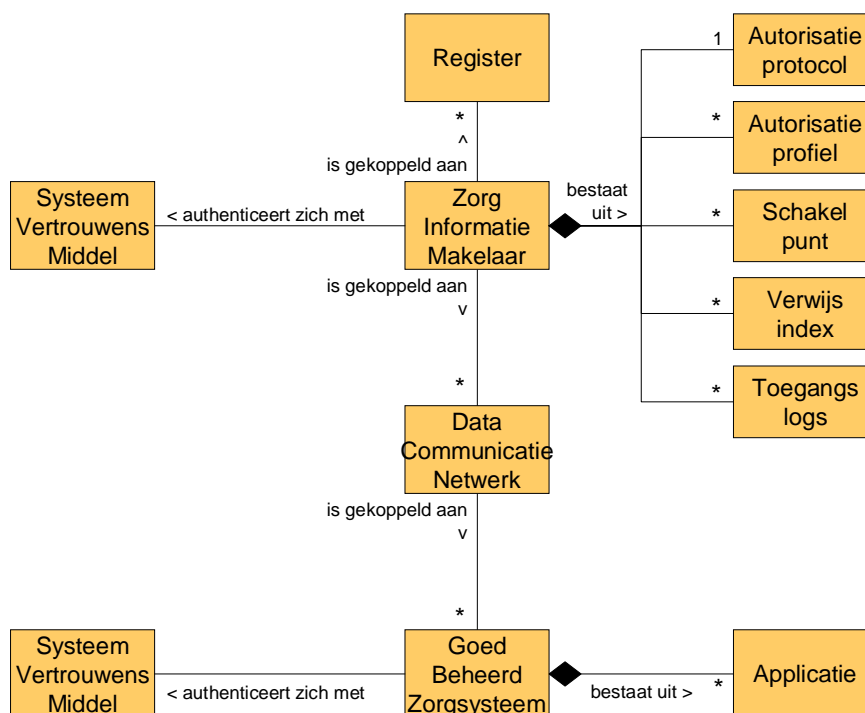
## 5.14 Configuratietabellen (CFT)

De configuratietabellen zijn een verzameling tabellen die bijhouden hoe de ZIM is samengesteld uit verschillende schakelpunten en aangekoppelde beheerobjecten, en op welke manier GBZ'en met hun applicaties via welke DCN daarop zijn aangesloten.

Ruwweg kan onderscheid gemaakt worden tussen:

- ZIM-configuratietablel, met daarin de kenmerken van de operationele, test- en uitwijk-ZIM,
- DCN-configuratietablel, met daarin de kenmerken van ieder aangesloten DCN,
- GBZ-configuratietablel, met daarin de kenmerken van ieder aangesloten GBZ.

De onderstaande figuur toont de relaties tussen alle beheerde objecten, in een UML class diagram.



De in paragraaf 4.18 genoemde HL7-conformancetablel bestaat voor iedere applicatie uit een lijst met de volgende attributen:

- HL7-interactie-id,
- type HTTP/SOAP-binding: enkelvoudig of tweevoudig.

Versienummers zijn in de HL7-conformancetablel niet nodig, omdat nieuwe versies van HL7-berichten leiden tot nieuwe HL7-interactie-id's.

De in paragraaf 4.18 genoemde parametertabel bevat de volgende parameters:

<i>Parameter</i>	<i>Verklaring</i>	<i>Initiële waarde</i>
gebruiker-oplever-time-out	tijdsinterval na opvraag van gebruiker waarbinnen moet worden opgeleverd aan gebruiker	20 sec
GBZ-oplever-time-out	tijdsinterval na HL7-opvraag van GBZ aan ZIM waarbinnen HL7-oplevering moet zijn ontvangen	10 sec
GBZ-opvraag-retry	aantal keren dat mislukte opvraag van GBZ aan ZIM wordt herhaald	1
ZIM-oplever-time-out	tijdsinterval na HL7-opvraag van ZIM aan GBZ waarbinnen HL7-oplevering moet zijn ontvangen	5 sec
ZIM-opvraag-retry	aantal keren dat mislukte opvraag van ZIM aan GBZ wordt herhaald	2
gebruiker-bevestig-time-out	tijdsinterval na opdracht van gebruiker waarbinnen moet worden bevestigd aan gebruiker	10 sec
GBZ-bevestig-time-out	tijdsinterval na HL7-opdracht van GBZ aan ZIM waarbinnen HL7-bevestiging moet zijn ontvangen	5 sec
GBZ-opdracht-retry	aantal keren dat mislukte opdracht van GBZ aan ZIM wordt herhaald	1
ZIM-bevestig-time-out	tijdsinterval na HL7-opdracht van ZIM aan GBZ waarbinnen HL7-bevestiging moet zijn ontvangen	2 sec
ZIM-opdracht-retry	aantal keren dat mislukte opdracht van ZIM aan GBZ wordt herhaald	2
gebruiker-max-kaart-uit	maximum duur dat vertrouwensmiddel van werkplek verwijderd mag zijn, voordat sessie wordt beëindigd	5 minuten
gebruiker-max-sleutel-duur	maximum duur dat tijdelijke SSL/TLS-sleutel gebruikt mag worden, waarna deze ververs moet worden	5 minuten
gebruiker-max-sessie-duur	maximum duur van SSL/TLS-sessie tussen gebruiker en ZIM, voordat sessie wordt beëindigd	8 uur
gebruiker-max-sessie-onbruik	maximum duur dat een SSL/TLS-sessie tussen gebruiker en ZIM niet gebruikt wordt, voordat sessie wordt beëindigd	30 minuten
gebruiker-max-applicatie-onbruik	maximum duur dat applicatie door gebruiker niet gebruikt wordt, voordat sessie wordt beëindigd	15 minuten
systeem-max-sleutel-duur	maximum duur dat een tijdelijke SSL/TLS-sleutel gebruikt mag worden, waarna deze ververs moet worden	5 minuten
systeem-max-sessie-duur	maximum duur van een SSL/TLS-sessie tussen dossier/postbus en ZIM, voordat de sessie wordt beëindigd	8 uur
systeem-max-sessie-onbruik	maximum duur dat een SSL/TLS-sessie tussen dossier/postbus en ZIM niet gebruikt wordt, voordat de sessie wordt beëindigd	15 minuten
ZIM-max-sessie-aantal	Maximum aantal SSL-sessies dat een ZIM mag opzetten met een GBZ	3

Opmerkingen:

- Objectmodellen worden gewoonlijk top-down afgeleid uit de voorgaande paragrafen. Dit objectmodel is echter deels bottom-up afgeleid uit document [Technische architectuur]. Zo toont het objectmodel dat een ZIM kan bestaan uit verscheidene schakelpunten en verwijzindices, terwijl dat pas in het volgende hoofdstuk wordt onderbouwd. Voor een goed begrip van het bovenstaande model is lezing van document [Technische architectuur] noodzakelijk.
- Evenzo komt de tijdsparametertabel voort uit document [Technische architectuur].

## 6 Interacties

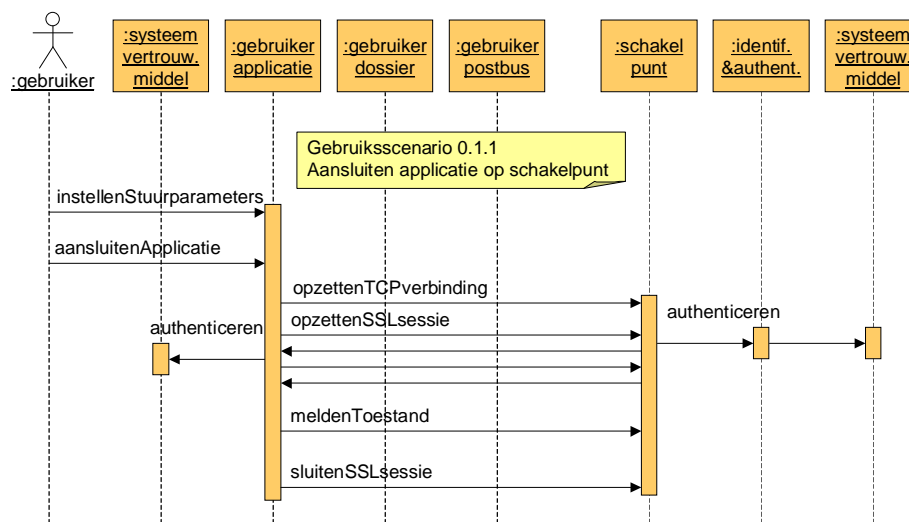
Dit hoofdstuk beschrijft de interacties tussen objecten uit hoofdstuk 5 voor elk van de gebruiksscenario's beschreven in hoofdstuk 4.

Merk op dat de diagrammen voor de gebruiksscenario's 0.1 tot en met 0.4 enkele generieke objecten tonen die altijd één van de onderstaande specifieke objecten moeten zijn:

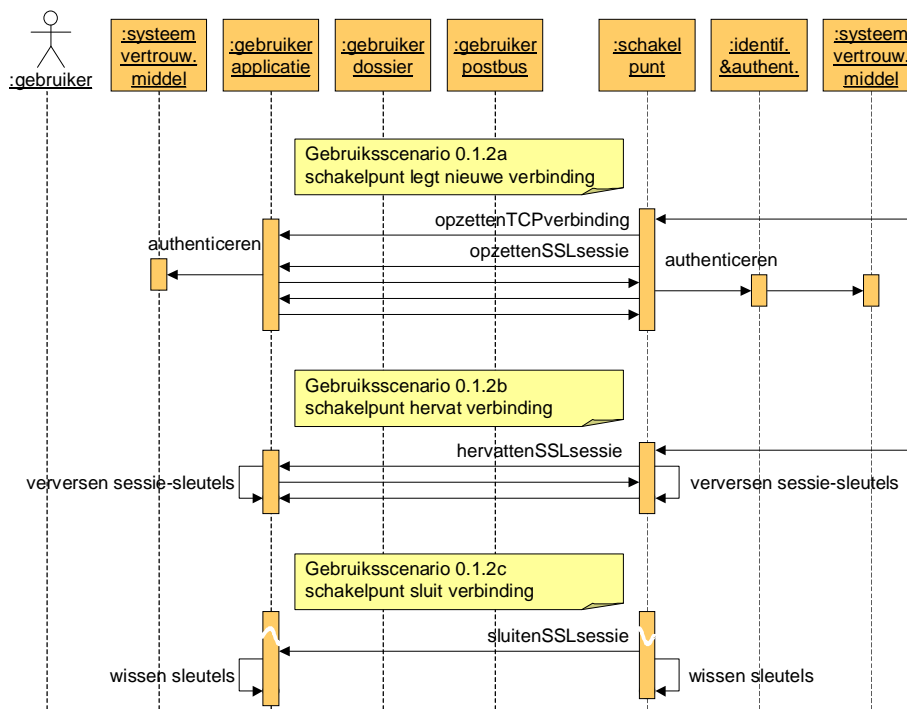
<i>gebruiker</i>	<i>gebruikerApplicatie</i>	<i>gebruikerRegister</i>
patiënt/cliënt	patiëntApplicatie	patiëntRegister
zorgverlener, zorgmedewerker	zorgaanbiederApplicatie	zorgaanbiederRegister
beheerder	beheerApplicatie	beheerdersRegister

### 6.1 Aan-/afsluiten applicatie op schakelpunt

Onderstaande UML sequence diagram toont welke interacties plaatsvinden tussen de bovengenoemde objecten, als gevolg van gebruiksscenario [ASL], zie verder paragraaf 4.16 en het hoofdstuk "Beveiliging" van document [Technische Architectuur].



De figuur toont bij gebruiksscenario [ASL.s01] hoe een beheerder op basis van het systeemvertrouwensmiddel een verbinding opzet met het schakelpunt om een bericht te sturen met een nieuwe beschikbaarheidstoestand.



De figuur toont bij gebruiksscenario [ASL.s02a] hoe de SSL-sessie wordt opgezet door het schakelpunt.

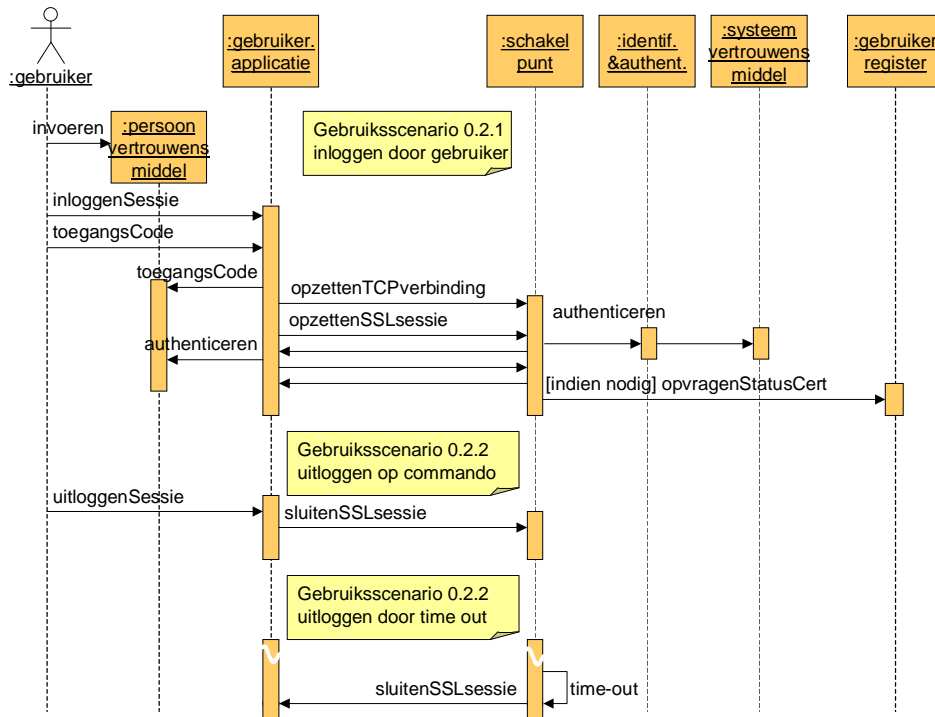
De figuur toont bij gebruiksscenario [ASL.s01b] hoe het schakelpunt een SSL-sessie na verloop van het tijdsinterval *stysteem-max-sessie-sleutel* kan hervatten zonder de tijdrovende authenticatie.

De figuur toont bij gebruiksscenario [ASL.s01c] hoe het schakelpunt een SSL-sessie definitief zal sluiten als:

- het tijdsinterval *stysteem-max-sessie-onbruik* is verlopen sinds het laatste bericht over de SSL-verbinding,
- het tijdsinterval *stysteem-max-sessie-duur* is verlopen sinds de laatste authenticatie.

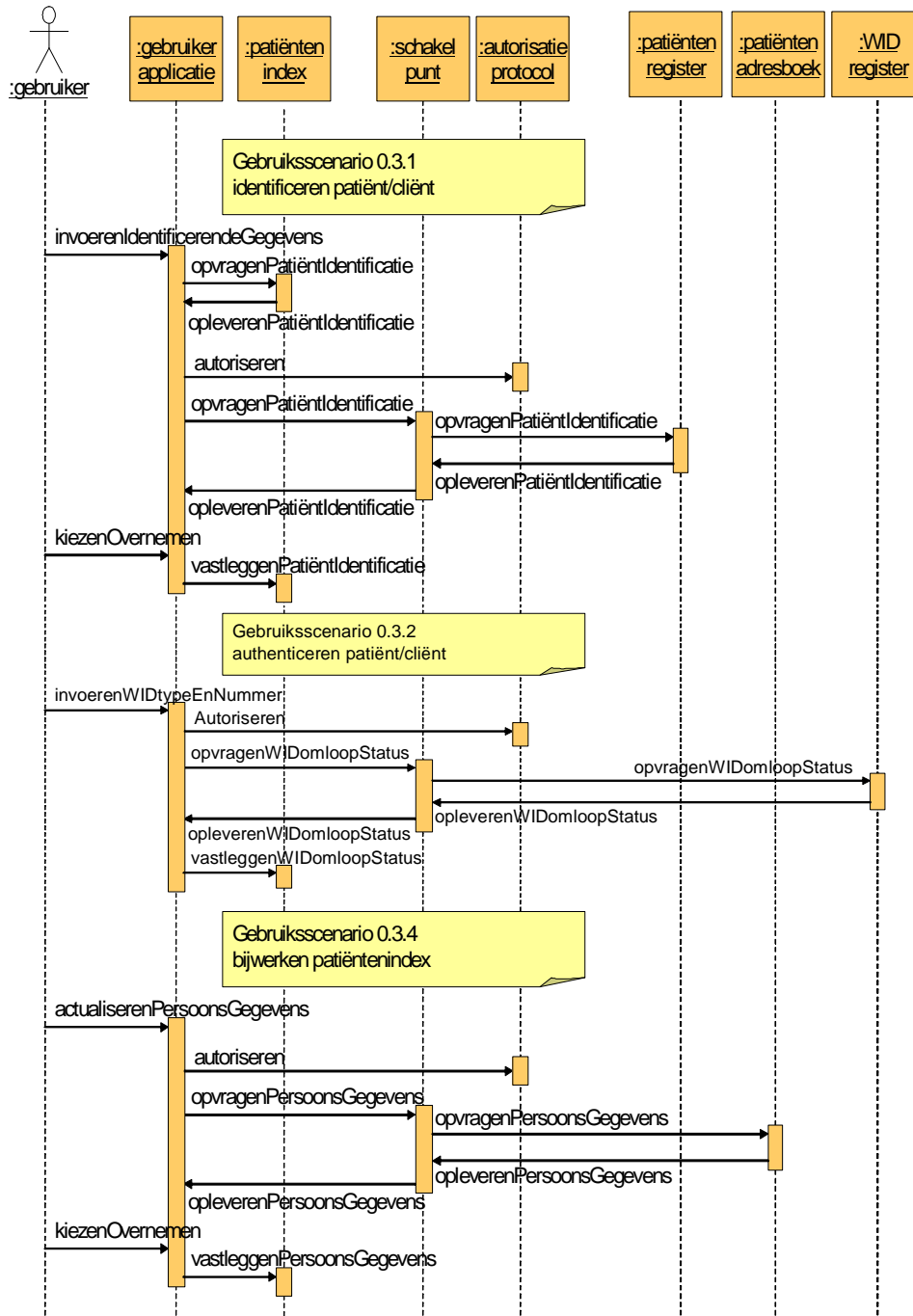
## 6.2 In/uitloggen gebruiker

Onderstaande UML sequence diagram toont welke interacties plaatsvinden tussen de bovengenoemde objecten, als gevolg van gebruiksscenario [INL], zie verder paragraaf 4.2.



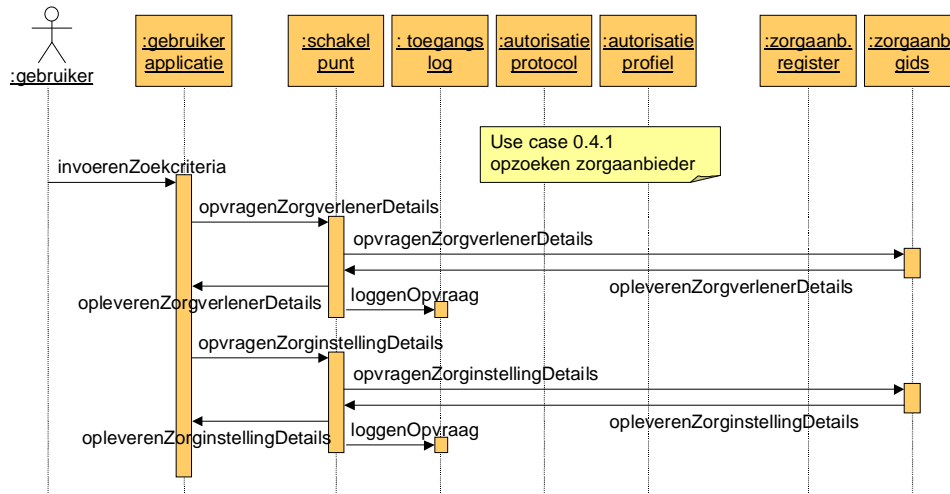
## 6.3 Selecteren patiënt/cliënt

Onderstaande UML sequence diagram toont welke interacties plaatsvinden tussen de bovengenoemde objecten, als gevolg van gebruiksscenario [SPA], zie verder paragraaf 4.3.



## 6.4 Selecteren zorgaanbieder

Onderstaande UML sequence diagram toont, welke interacties plaatsvinden tussen de bovengenoemde objecten, als gevolg van gebruiksscenario [SZA], zie verder paragraaf 4.4.

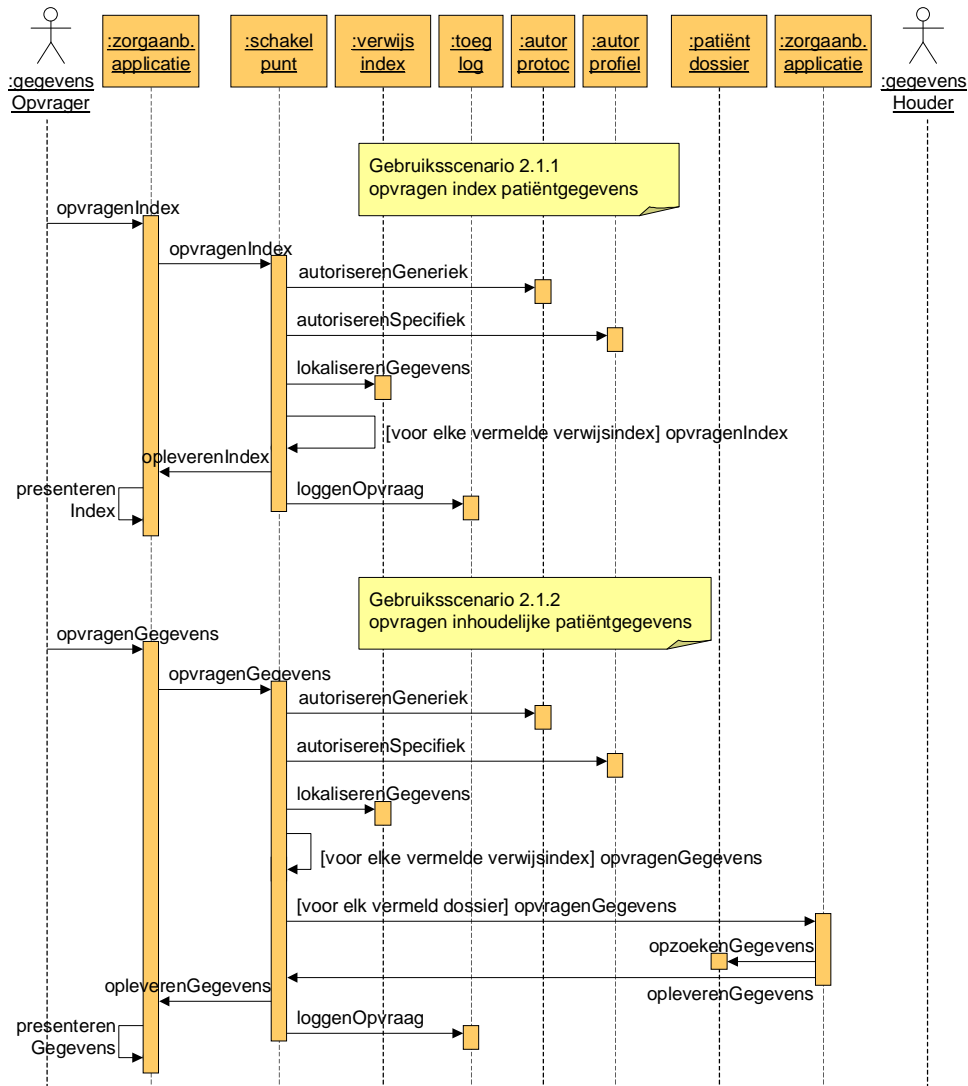


Gebruiksscenario [SZA-s02] heeft met de huidige HL7v3-berichten dezelfde interacties als gebruiksscenario [SZA-s01].



## 6.5 Opvragen patiëntgegevens

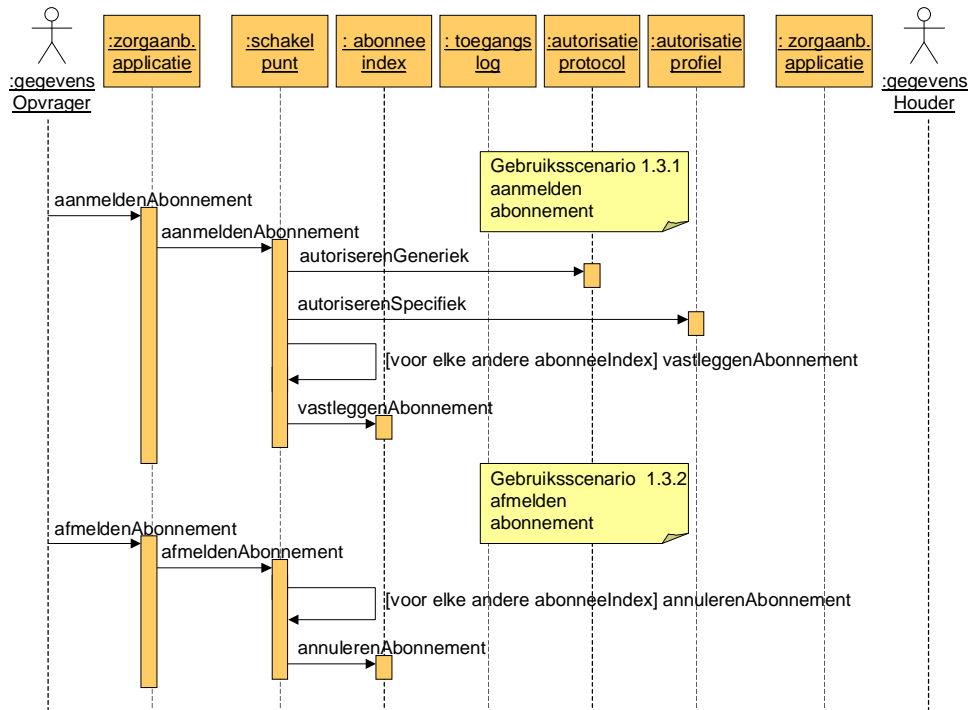
Onderstaande UML sequence diagram toont welke interacties plaatsvinden tussen de bovengenoemde objecten, als gevolg van gebruiksscenario [OPV], zie verder paragraaf 4.9.



Merk op dat de figuur rekening houdt met eventuele meerdere schakelpunten en verwijsindices.

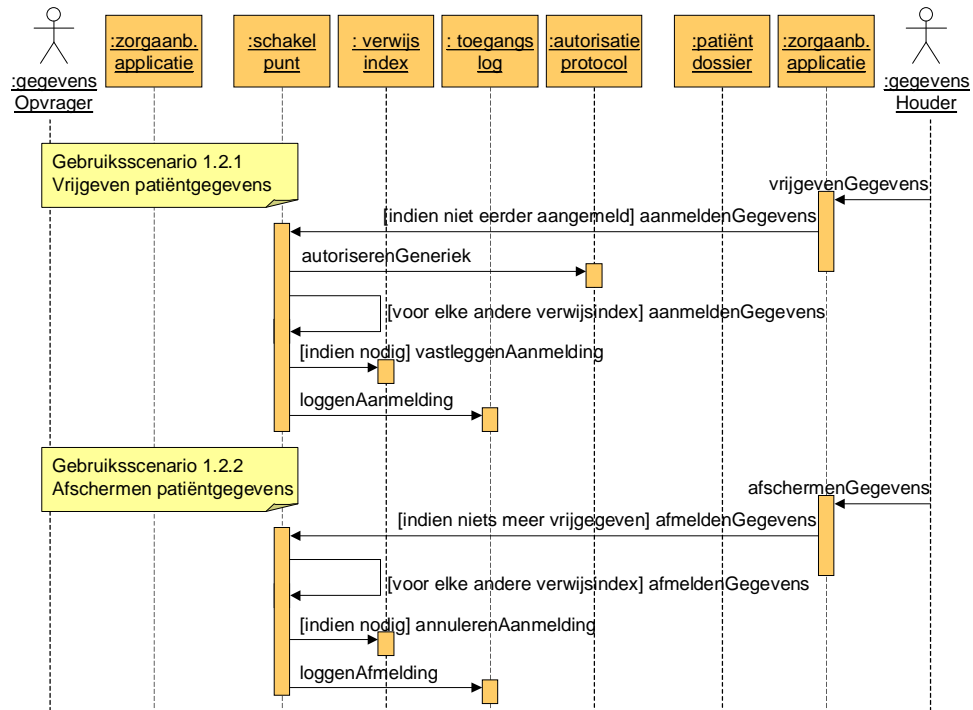
## 6.6 {toekomst} Abonneren patiëntgegevens

Onderstaande UML sequence diagram toont welke interacties plaatsvinden tussen de bovengenoemde objecten, als gevolg van gebruiksscenario [ABO], zie verder paragraaf 4.7.



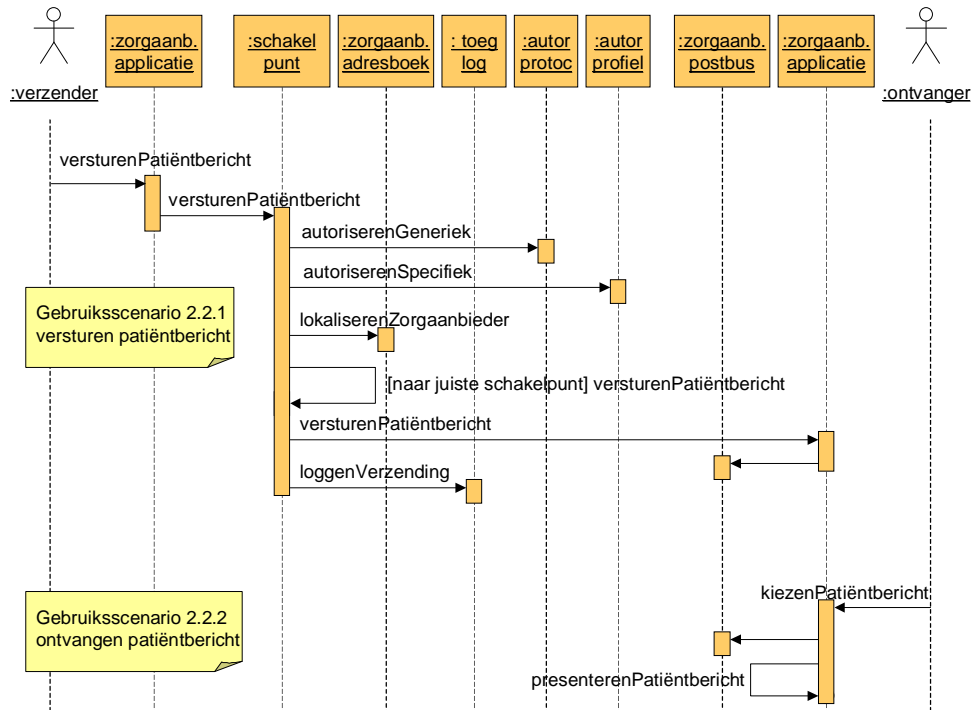
## 6.7 Publiceren patiëntgegevens

Onderstaande UML sequence diagram toont welke interacties plaatsvinden tussen de bovengenoemde objecten, als gevolg van gebruiksscenario [PUB], zie verder paragraaf 4.6.



## 6.8 Versturen patiëntbericht

Onderstaande UML sequence diagram toont welke interacties plaatsvinden tussen de bovengenoemde objecten, als gevolg van gebruiksscenario [STU], zie verder paragraaf 4.10.



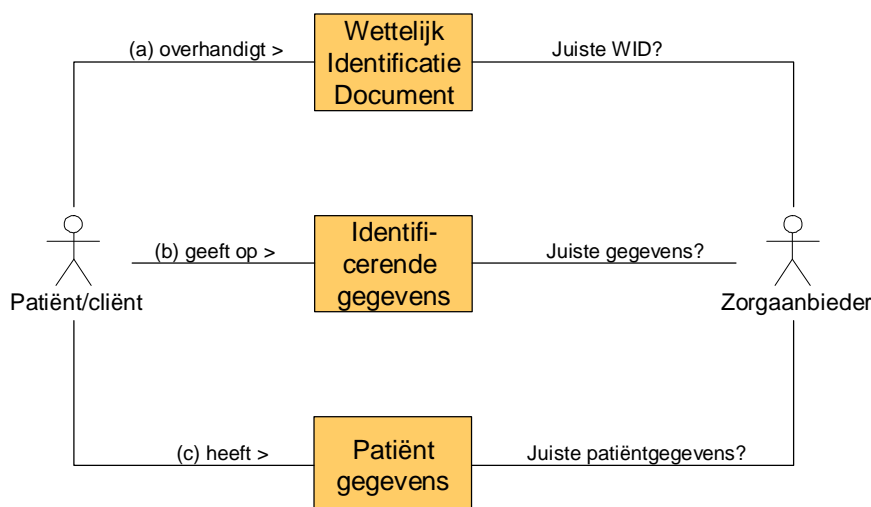
Voor gebruiksscenario [STU·s03] en [STU·s04], zie bijlage B.



# Bijlage A - Invoering burgerservicenummer

## A.1 Inleiding

De invoering en het gebruik van het burgerservicenummer (BSN) in de zorg wordt geregeld in een nieuwe "Wet gebruik burgerservicenummer in de zorg", afgekort Wbsn-z en het "Besluit gebruik burgerservicenummer in de zorg", afgekort Bbsn-z.



De bovenstaande figuur toont de onzekerheden waarmee een zorgaanbieder kan worden geconfronteerd:

- de patiënt/cliënt overhandigt een WID, maar is dit wel echt een WID? En behoort dit WID toe aan deze patiënt/cliënt? En is dit WID niet over de uiterste geldigheidsdatum? En is dit WID misschien gestolen?
- de patiënt/cliënt geeft anders identificerende gegevens op, maar zijn die gegevens wel van deze persoon? En wat is diens BSN (indien niet opgegeven)? Of is het BSN wel juist (indien wel opgegeven)?
- de patiënt/cliënt heeft een dossier met patiëntgegevens bij de zorgaanbieder, maar horen al de patiëntgegevens wel bij deze patiënt/cliënt?

In de volgende paragrafen wordt uitgewerkt op welke wijze een zorgaanbieder deze onzekerheden moet oplossen. Daarbij worden de volgende gevallen onderscheiden:

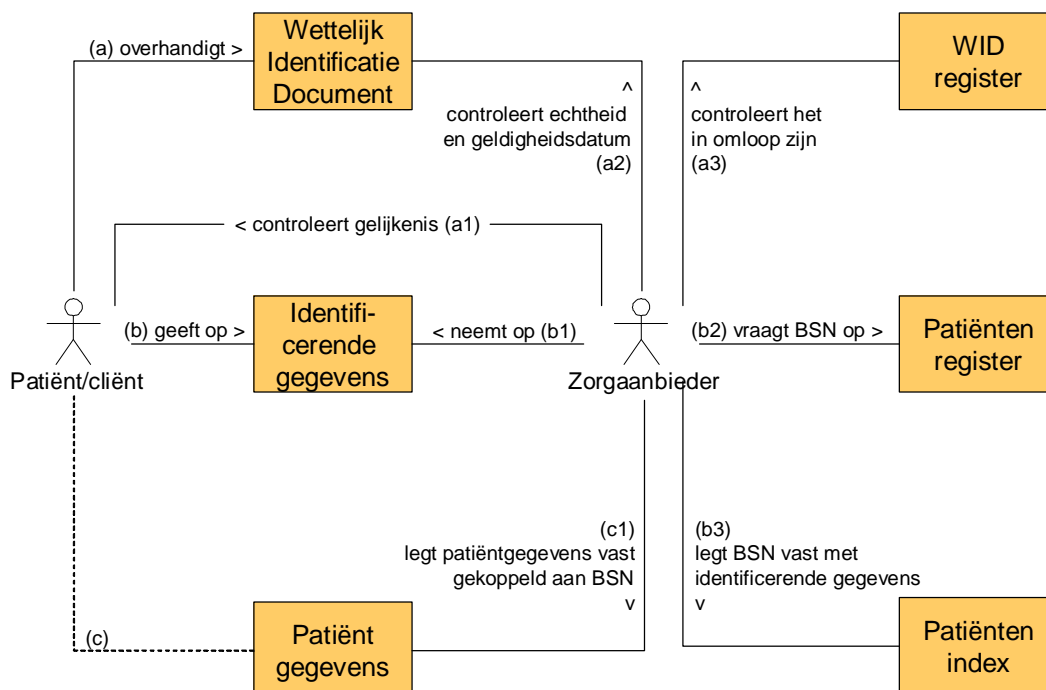
- Eerste contact met nieuwe patiënt/cliënt,
- Eerste contact met ingeschreven patiënt/cliënt,
- Initiële koppeling patiëntgegevens,
- Eerste contact met initieel gekoppelde patiënt/cliënt,
- Vervolg contact met patiënt/cliënt,
- Ontvangst patiëntgegevens.

Daarbij wordt het landelijk *patiëntenregister* genoemd. Dit zal doorgaans de BVBSN zijn die toegankelijk is via de SBV-Z, maar ook het GBA kan als zodanig dienen. Ook wordt een *WID-register* genoemd. Dat zal ook via de SBV-Z toegankelijk gemaakt worden.

De laatste paragraaf beschrijft de consequenties voor het landelijk uitwisselen van patiëntgegevens.

## A.2 Eerste contact met nieuwe patiënt/cliënt

Vanaf de inwerkingtreding van de Wbsn-z moeten zorgaanbieders van alle *nieuwe* patiënten/cliënten bij het eerste contact het BSN vaststellen aan de hand van het WID.



De bovenstaande figuur toont de werkwijze in een UML collaboration diagram:

- (a) de patiënt/cliënt overhandigt desgevraagd een WID, waarna de zorgaanbieder:
1. het WID op gelijkenis met de patiënt/cliënt controleert,
  2. het WID op echtheid en geldigheidsdatum controleert,
  3. zonodig het in omloop zijn van het WID controleert door raadpleging van een WID-register.
- (b) de patiënt/cliënt geeft identificerende gegevens op, impliciet aan de hand van het overhandigde WID, waarop de zorgaanbieder:
1. die identificerende gegevens opneemt uit het WID,
  2. op basis daarvan het BSN opvraagt bij het landelijke patiëntenregister,
  3. het BSN met de identificerende gegevens vastlegt in de lokale patiëntenindex.

- (c) de patiënt/cliënt heeft nog geen patiëntgegevens bij deze zorgaanbieder, maar de zorgaanbieder:
1. kan vanaf het begin patiëntgegevens vastleggen, *definitief* gekoppeld aan het BSN.

Hierbij kunnen bijzondere situaties optreden:

- Ad (a) een WID kan in de volgende gevallen niet worden overhandigd:
  - de patiënt/cliënt is niet aanwezig (bijv. telefonisch consult)
  - de patiënt/cliënt heeft geen WID bij zich (bijv. vergeten)
  - de patiënt/cliënt heeft geen WID (bijv. minderjarig)In het eerste geval mogen patiëntgegevens *voorlopig* worden gekoppeld aan het opgevraagde BSN. In de andere gevallen mogen bij (c) geen patiëntgegevens worden gekoppeld aan het opgevraagde BSN.
- Ad (b2) een BSN kan in de volgende gevallen niet worden opgevraagd of geverifieerd:
  - het patiëntenregister is tijdelijk niet beschikbaar (bijv. storing)
  - de patiënt/cliënt heeft geen BSN (bijv. toerist)
  - de patiënt/cliënt heeft nog geen BSN (bijv. pasgeborene)In het eerste geval moet de zorgaanbieder het later alsnog proberen. Niet-ingezetenen kunnen erop gewezen worden dat zij mogelijk in aanmerking komen voor inschrijving in het RNI, waardoor zij alsnog een BSN kunnen verwerven. Voor pasgeborenen moet de ouder of voogd alsnog een BSN komen opgeven.
- Ad (b3) mocht hier blijken dat de patiënt/cliënt toch reeds was ingeschreven in de lokale patiëntenindex, dan moet de procedure worden voortgezet zoals beschreven in de volgende paragraaf.

Opdat achterstallige controles niet worden vergeten, zal dit per patiënt/cliënt kunnen worden aangegeven met vlaggen in de patiëntenindex of in ieder patiëntdossier, zodat de zorgaanbieder erop wordt geattendeerd bij een vervolcontact van de patiënt/cliënt. De benodigde vlaggen kunnen zijn:

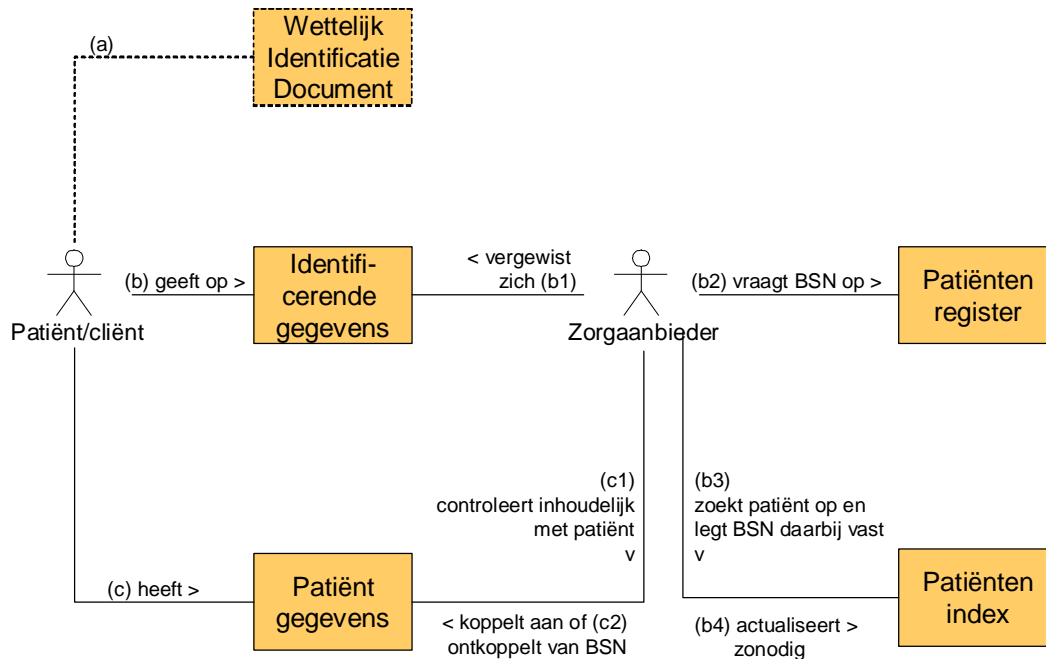
- WID gecontroleerd op gelijkenis met patiënt/cliënt?
- WID gecontroleerd op geldigheidsdatum?
- WID gecontroleerd op echtheid?
- WID gecontroleerd op het in omloop mogen zijn?
- BSN opgevraagd of geverifieerd?
- Dossier inhoudelijk gecontroleerd met patiënt/cliënt?
- Identificerende gegevens geactualiseerd?

Voor zover de WID-controles in één keer worden uitgevoerd, kan worden volstaan met één gecombineerde vlag.

### A.3 Eerste contact met ingeschreven patiënt/cliënt

Vanaf de inwerkingtreding van de Wbsn-z moeten zorgaanbieders van alle *ingeschreven* patiënten/cliënten bij het eerstvolgende contact na de inwerkingtreding het BSN vaststellen.





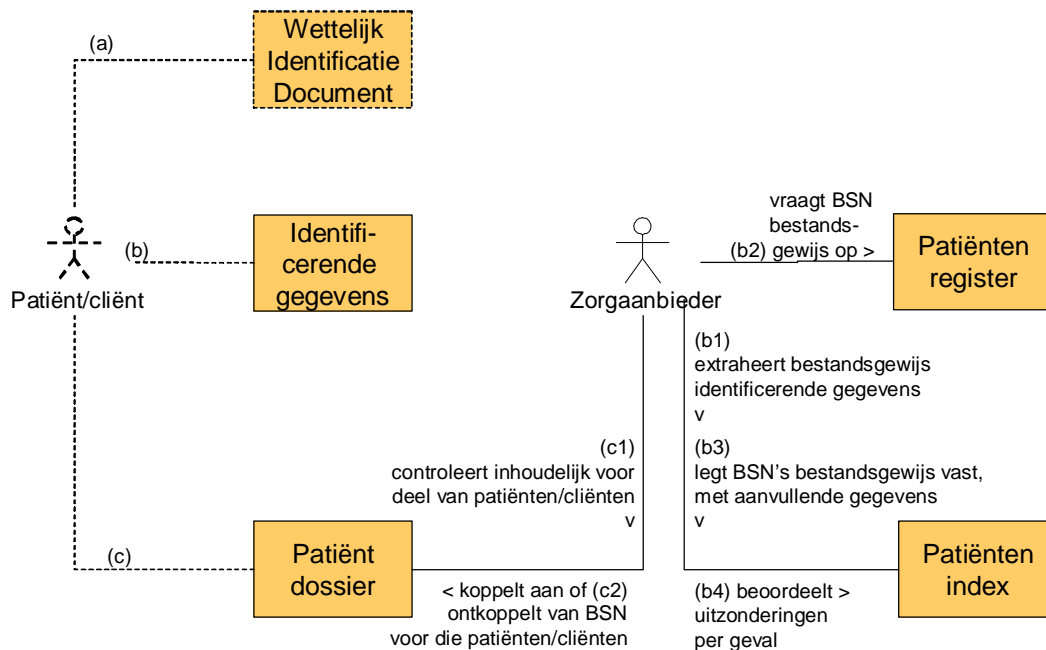
De bovenstaande figuur toont de werkwijze in een UML collaboration diagram:

- (a) de patiënt/cliënt hoeft als reeds ingeschrevene in principe geen WID te overhandigen, tenzij de zorgaanbieder twijfel heeft over de identiteit van deze patiënt/cliënt. In dat geval handelt de zorgaanbieder alsof het gaat om een nieuwe patiënt/cliënt.
- (b) de patiënt/cliënt geeft mondeling identificerende gegevens op, waarna de zorgaanbieder:
  1. zich ervan vergewist dat de identificerende gegevens horen bij die patiënt/cliënt,
  2. op basis daarvan het BSN opvraagt bij het landelijke patiëntenregister,
  3. de patiënt/cliënt opzoekt in de lokale patiëntenindex en het BSN aldaar vastlegt,
  4. zonodig de lokale patiëntenindex actualiseert met aanvullende gegevens uit het landelijke patiëntenregister.
- (c) de patiënt/cliënt heeft reeds patiëntgegevens bij deze zorgaanbieder, waarvan de zorgaanbieder:
  1. controleert of ze inhoudelijk bij deze patiënt/cliënt horen, zonodig samen met de patiënt/cliënt,
  2. zo ja, koppelt de patiëntgegevens *definitief* aan het BSN, zo nee, ontkoppelt de patiëntgegevens van het BSN.

Als bij (b3) blijkt dat de patiënt/cliënt niet kan worden gevonden, was hij toch niet ingeschreven en moet de procedure van de vorige paragraaf vanaf het begin worden gevolgd.

## A.4 Initiële koppeling patiëntgegevens

In plaats van de druppelsgewijze invoering van het BSN, zie vorige paragraaf, kan de zorgaanbieder kiezen voor initiële koppeling door alle ingeschreven, of alleen de actuele, patiënten/cliënten bij de inwerkingtreding van de Wbsn-z bestandsgewijs te koppelen aan een BSN.



De bovenstaande figuur toont de werkwijze in een UML collaboration diagram:

- (a) er zijn géén patiënten/cliënten om een WID te overhandigen, maar dat hoeft ook niet voor reeds ingeschreven patiënten/cliënten.
- (b) er zijn géén patiënten/cliënten om identificerende gegevens op te geven, maar de zorgaanbieder kan:
  1. deze bestandsgewijs extraheren uit de lokale patiëntenindex,
  2. bestandsgewijs BSN's opvragen uit het landelijke patiëntenregister,
  3. de gevonden BSN's bestandsgewijs vastleggen in de lokale patiëntenindex, zonedig samen met aanvullende gegevens uit het landelijke patiëntenregister,
  4. de gevonden uitzonderingen per geval beoordelen, voor zover dat mogelijk is in afwezigheid van de onderhavige patiënt/cliënt. .
- (c) er zijn géén patiënten/cliënten om daarmee de juistheid van de patiëntgegevens inhoudelijk te controleren, maar de zorgaanbieder kan:
  1. voor een deel van de patiënten/cliënten de juistheid vaststellen,
  2. voor die patiënten/cliënten de patiëntgegevens *definitief* aan het BSN koppelen.

Bij stap (b3) worden de patiëntgegevens in eerste instantie *voorlopig* gekoppeld. Nadat (b4) en (c) zijn afgerond kan de koppeling *definitief* worden gemaakt. Echter, bij (b4) kan de zorgaanbieder gaan twijfelen over de identiteit van bepaalde patiënten/cliënten en dus het WID willen inzien. Bij (c) kan de zorgaanbieder gaan twijfelen of alle

patiëntgegevens daadwerkelijk horen bij de gekoppelde patiënten/cliënten en deze samen met hen willen doornemen.

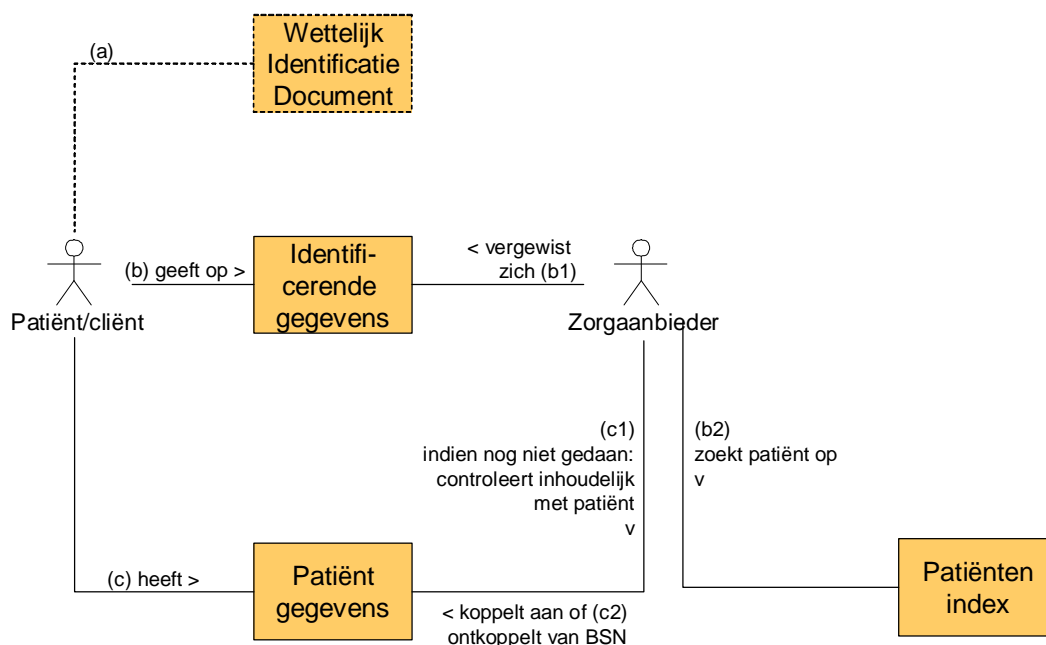
Voor al die patiënten/cliënten zullen (a), (b) en/of (c) in een later stadium alsnog of overnieuw moeten worden gedaan, bijvoorbeeld bij het eerste contact met iedere initieel gekoppelde patiënt/cliënt, zie de volgende paragraaf. Opdat de zorgaanbieder dan erop wordt geattendeerd dat er twijfel is over de identiteit van de patiënt/cliënt en/of dat zijn patiëntgegevens slechts *voorlopig* zijn gekoppeld, zal dit moeten worden aangegeven met vlaggen in de patiëntenindex, dan wel het patiëntdossier.

Reden om initieel te koppelen ligt onder meer in het met terugwerkende kracht kunnen aanmelden van reeds bestaande patiëntgegevens aan de verwijzindex van het LSP. Dit kan voorkomen dat de verwijzindex aanvankelijk erg leeg is, zodat de eerste zorgaanbieders die aansluiten op het LSP lang moeten wachten voordat ze de vruchten van landelijke uitwisseling van patiëntgegevens kunnen plukken.

Omdat de meeste zorgaanbieders pas zullen aansluiten op het LSP na de inwerkingtreding van de Wbsn-z, mag de initiële aanmelding ook worden gedaan bij de eerste aansluiting op het LSP.

## A.5 Eerste contact initieel gekoppelde patiënt/cliënt

Zoals beschreven in de vorige paragraaf, zal de zorgaanbieder bij het eerste contact van een initieel gekoppelde patiënt/cliënt (a) en (c) misschien alsnog of overnieuw moeten doen.



De bovenstaande figuur toont de werkwijze in een UML collaboration diagram:

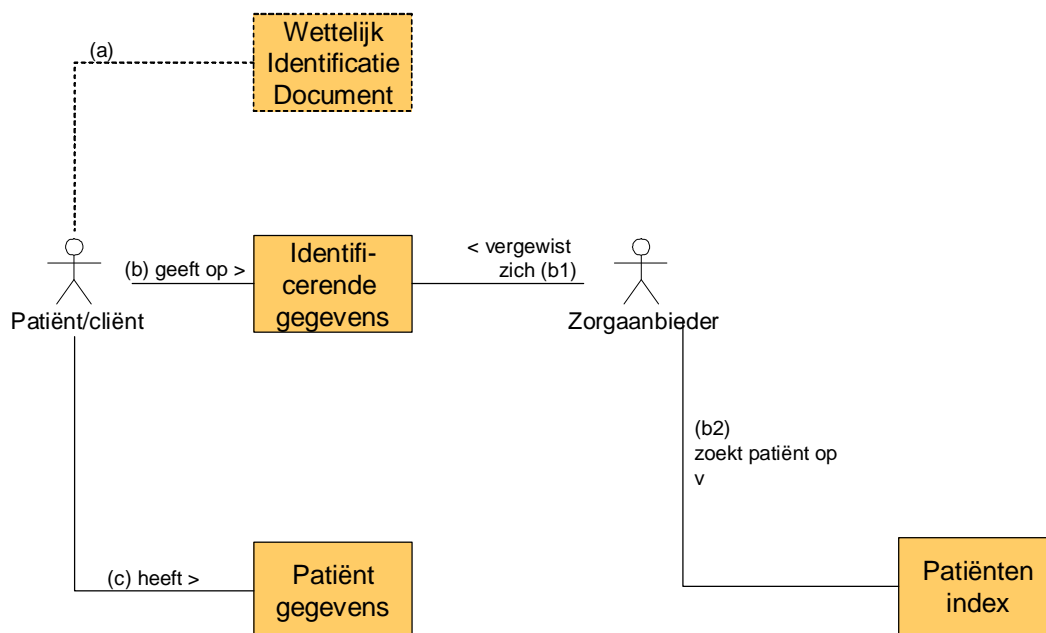
- (a) de patiënt/cliënt hoeft als reeds ingeschrevene in principe geen WID te overhandigen, tenzij de zorgaanbieder twijfel heeft over de identiteit van deze

patiënt/cliënt. In het laatste geval handelt de zorgaanbieder alsof het gaat om een nieuwe patiënt/cliënt.

- (b) de patiënt/cliënt geeft mondeling identificerende gegevens op, waarop de zorgaanbieder:
  1. zich ervan vergewist dat de identificerende gegevens horen bij die patiënt/cliënt,
  2. op basis daarvan de patiënt/cliënt opzoekt in de lokale patiëntenindex,
  3. indien de zorgaanbieder wordt gewaarschuwd dat hij twijfel had over de identiteit van deze patiënt/cliënt, alsnog stap (a) uitvoert.
- (c) indien de zorgaanbieder wordt gewaarschuwd dat de patiënt/cliënt nog *voorlopig* gekoppelde patiëntgegevens heeft, kan de zorgaanbieder:
  1. deze inhoudelijk controleren en zonodig doornemen met bij deze patiënt/cliënt,
  2. deze patiëntgegevens alsnog *definitief* koppelen aan het BSN, of anders ontkoppelen van het BSN.

## A.6 Vervolg contact met patiënt/cliënt

Bij elk volgend contact met een patiënt/cliënt moet de zorgaanbieder hem identificeren aan de hand van gegevens in zijn patiëntenindex, dan wel diens patiëntdossier.



De bovenstaande figuur toont de werkwijze in een UML collaboration diagram:

- (a) de patiënt/cliënt hoeft bij een vervolgcontact geen WID te tonen, tenzij de zorgaanbieder twijfel heeft over de identiteit.
- (b) de patiënt/cliënt geeft identificerende gegevens op, waarop de zorgaanbieder:
  1. zich ervan vergewist dat de identificerende gegevens horen bij die patiënt/cliënt
  2. op basis daarvan de patiënt/cliënt opzoekt in de lokale patiëntenindex.

In de praktijk zal een zorgaanbieder van een verschijnende patiënt/cliënt niet bij voorbaat weten of hij reeds gekoppeld is, zijn WID gecontroleerd is, etc. Dit betekent dat er in de praktijk één procedure moet zijn voor de volgende gevallen:

- Eerste contact met nieuwe patiënt/cliënt,
- Eerste contact met ingeschreven patiënt/cliënt,
- Eerste contact met initeel gekoppelde patiënt/cliënt,
- Vervolg contact met patiënt/cliënt,

waarbij de vlaggen in de patiëntenindex, dan wel diens patiëntdossier bepalen welke stappen worden doorlopen.

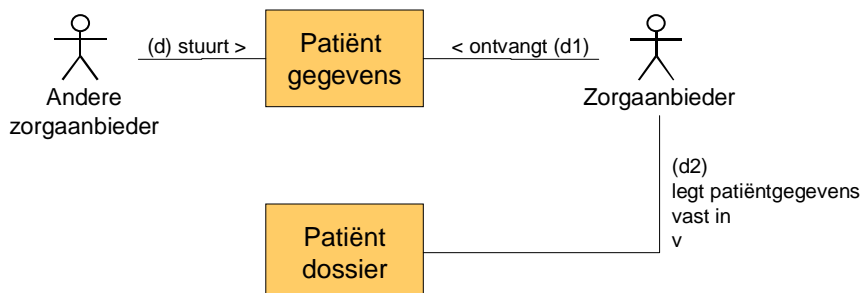
Deze algemene procedure kan als volgt verlopen:

- identificeren patiënt/cliënt:
  - de zorgaanbieder probeert de patiënt/cliënt op te zoeken in de lokale patiëntenindex, dan wel alle patiëntdossiers,
  - als de patiënt/cliënt niet wordt gevonden of als een vlag aangeeft dat het BSN nog niet in het landelijke patiëntenregister is opgevraagd of geverifieerd, moet de zorgaanbieder dat alsnog doen,
- authenticeren patiënt/cliënt:
  - als een vlag aangeeft dat het WID nog niet is gecontroleerd met de patiënt/cliënt, of anderszins van de identiteit is vergewist, moet de zorgaanbieder dat alsnog doen,
- overnemen naar de patiëntenindex, dan wel diens patiëntdossier:
  - als een vlag aangeeft dat de patiëntgegevens nog niet inhoudelijk zijn gecontroleerd met de patiënt/cliënt, moet de zorgaanbieder dat alsnog doen,

De gebruiksscenario's in paragraaf 4.3 zijn gebaseerd op deze procedure.

## A.7 Ontvangst patiëntgegevens

Wanneer een zorgaanbieder patiëntgegevens (bijv. medicatievoorschrift) ontvangt van een andere zorgaanbieder, mag hij veronderstellen dat het daarbij vermelde BSN op de juiste wijze is verkregen.



De bovenstaande figuur toont de werkwijze in een UML collaboration diagram:

(d) Een andere zorgaanbieder stuurt patiëntgegevens, waarop de zorgaanbieder:

1. deze patiëntgegevens afhandelt zoals bedoeld, en daarbij wellicht nieuwe patiëntgegevens aanmaakt, uitsluitend gebaseerd op de ontvangen patiëntgegevens,
2. deze nieuwe patiëntgegevens, eventueel tezamen met de ontvangen patiëntgegevens, na afloop toevoegt aan het patiëntdossier met hetzelfde BSN.

De ontvangende zorgaanbieder hoeft dus geen controles uit te voeren, ervan uitgaande dat zijn eigen dossier reeds conform de voorschriften is gekoppeld, etc. Dit alles gaat ervan uit dat de onderhavige patiënt/cliënt niet aanwezig is, of althans niet als bron van nieuwe patiëntgegevens fungeert.

## A.8 Consequenties

Zoals in de vorige paragrafen beschreven, moet een zorgaanbieder voor iedere patiënt/cliënt de stappen (b) en (c) en vaak ook (a) doorlopen, maar zal dat in de praktijk niet altijd geheel lukken. In dergelijke gevallen zal de zorgverlener gewoon moeten doorgaan met het vastleggen van patiëntgegevens in zijn dossier, al dan niet gekoppeld aan een BSN. Maar het landelijk uitwisselen van patiëntgegevens via het LSP, moet alleen onder de volgende voorwaarden mogelijk zijn:

Een zorgaanbieder mag patiëntstukken *publiceren*, *opleveren*, *versturen* en *opvragen* voor een patiënt indien:

- diens patiëntidentiteit is bepaald door:
  - (voor een patiënt die op het moment van invoering van het BSN reeds ingeschreven was) opvragen van het BSN uit de eigen administratie op basis van identificatiegegevens mondeling verstrekt door de patiënt,
  - (andere patiënten) opvragen of verifiëren van het BSN bij de SBV-Z of een andere betrouwbare bron, op basis van identificatiegegevens overgenomen uit diens WID,
- diens patiëntidentiteit is geverifieerd door:
  - (voor een patiënt die op het moment van invoering van het BSN reeds ingeschreven was) zich op enigerlei wijze te vergewissen van diens identiteit,
  - (andere patiënten) controle van diens WID op gelijkenis met de patiënt en op geldigheid (in omloop mogen zijn) bij de SBV-Z,
- de onderhavige patiëntstukken, indien van vóór de invoering van het BSN, eens door de zorgaanbieder inhoudelijk zijn gecontroleerd als behorende bij de patiënt.

In aanvulling op het bovenstaande mag een apothek patiëntstukken ook *publiceren*, *opleveren*, *versturen* en *opvragen* voor een patiënt indien:

- diens patiëntidentiteit door een andere zorgaanbieder is verstrekt in een patiëntstuk (bijv. medicatievoorschrift),
- de inhoud van de onderhavige patiëntstukken (bijv. medicatieverstrekking) uitsluitend is gebaseerd op dat aangeleverde patiëntstuk of eigen patiëntstukken die definitief zijn gekoppeld aan dezelfde patiëntidentiteit.

In noodgevallen mag een zorgaanbieder patiëntstukken ook *opvragen* als:

- diens BSN op enigerlei wijze is bepaald,
- de opgeleverde patiëntgegevens niet worden opgenomen in het eigen dossier,
- de opgeleverde patiëntgegevens niet worden uitgewisseld met andere zorgaanbieders.

Opmerkingen:

- Het bovenstaande is geheel in lijn met Wbsn-z artikel 8 dat een zorgaanbieder bij het verstrekken van persoonsgegevens met betrekking tot de verlening van zorg altijd het BSN moet vermelden en Wbsn-z artikel 5, 6 en 7 dat daarvoor wel het BSN moet zijn vastgesteld en de identiteit geverifieerd. Binnen AORTA spreken we dan over *definitief gekoppelde* patiëntgegevens.
- Daarnaast zegt Bbsn-z artikel 27: als een WID-controle onmogelijk is of onevenredige inspanning kost, doordat de patiënt geen geldig WID bij zich heeft (vergeten, verlopen, vervalst, onwil, etc.), kan de zorgaanbieder in plaats van het BSN een vijftal identificatiegegevens opnemen bij vast te leggen of te verstrekken patiëntgegevens. Binnen AORTA spreken we dan over *niet gekoppelde* patiëntgegevens, maar AORTA staat niet toe om die landelijk uit te wisselen zonder vermelding van BSN.
- Tenslotte zegt Bbsn-z artikel 28 dat het BSN toch mag worden gebruikt door apothekers of bij zorgverlening per telefoon of e-mail, onder voorwaarde van controle van een vijftal identificatiegegevens en vermelding dat geen WID is gecontroleerd. Binnen AORTA spreken we dan over *voorlopig gekoppelde* patiëntgegevens, maar AORTA ondersteunt dat niet, als gevolg van een besluit van VWS-IO om geen onzekerheidsvlaggen te gebruiken in berichten die worden uitgewisseld tussen zorgaanbieders.

# Bijlage B - { toekomst } Ongeadresseerde opdrachten

## B.1 Inleiding

In de praktijk kan het gebeuren dat een huisarts (voorschrijver) niet weet aan wie hij een medicatievoorschrift moet sturen, omdat zijn patiënt nog niet weet bij welke apotheek (verstrekker) hij de medicijnen wil afhalen. Vroeger zou hij een receptbriefje zonder geadresseerde apotheker aan de patiënt hebben meegegeven, maar hoe realiseren wij de elektronische tegenhanger van dit ongeadresseerde medicatievoorschrift?

Deze bijlage doet een voorstel voor een oplossing die voortbordurt op het concept van de verwijsindex, zie ook ontwerpbeslissing [vst-b01]. Uiteraard beschouwen we hier alleen de extramurale situatie.

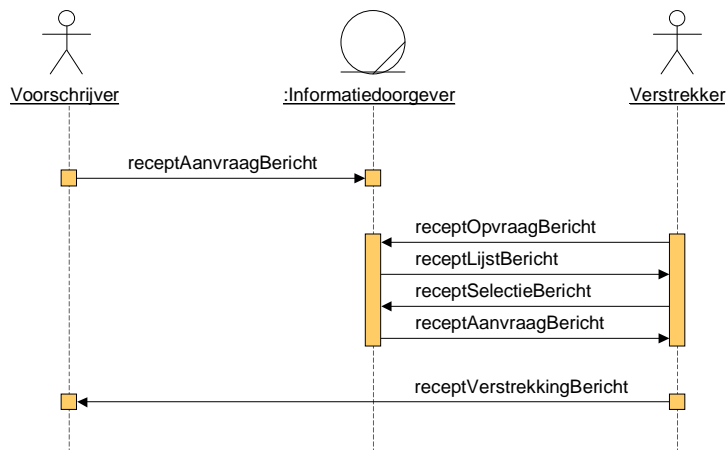


## B.2 Oplossing met informatiedoorgever

De NEN7503 ontwerpnorm beschrijft scenario's voor recept- en verstrekingsberichten. Voor het geval van het ongeadresseerde medicatievoorschrift<sup>1</sup> wordt voorzien in een intermediaire partij (informatiedoorgever), die feitelijk fungeert als een openbare postbus. Het scenario verloopt dan als volgt:

- de voorschrijver stuurt een ongeadresseerd medicatievoorschrift naar de informatiedoorgever,
- de patiënt meldt zich bij een verstrekker,
- de verstrekker vraagt alle ongeadresseerde medicatievoorschriften voor die patiënt op bij de informatiedoorgever
- de verstrekker selecteert het door de patiënt gewenste medicatievoorschrift en meldt dit bij de informatiedoorgever,
- de verstrekker verstrekt het medicijn aan de patiënt,
- etc.

De onderstaande figuur is overgenomen van NEN 7503, waarbij de stopRecept-AanvraagBerichten van de voorschrijver zijn weggelaten.



NEN7503 definieert verder een generiek medicatieAnnuleerBericht, maar beschrijft niet hoe dit in geval van het receptSelectieBericht leidt tot het terugzetten van de receptaanvraag aan de informatiedoorgever.

De *voorschrijver* kan een willekeurige arts zijn. De *verstrekker* is natuurlijk een stadsapotheek of een ziekenhuisapotheek. Blijft de vraag open, wie of wat de rol van *informatiedoorgever* speelt? De ontwerpnorm laat overigens toe dat de rollen van voorschrijver en informatiedoorgever bij éézelfde partij liggen. De NEN7503 ontwerpnorm geeft dus een abstract model dat op verschillende manieren kan worden ingevuld.

<sup>1</sup> Let op: in NEN7503 wordt de volgende terminologie voor een *recept* gehanteerd:

- *medicatieopdracht* voor de intramurale situatie
- *receptaanvraag* voor de extramurale situatie

Hier wordt algemeen de term *medicatievoorschrift* gehanteerd.

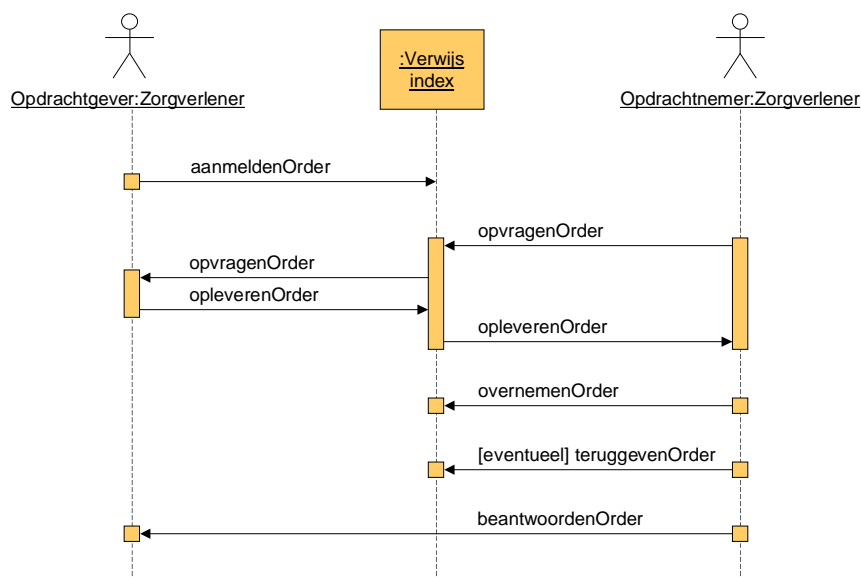
## B.3 Oplossing met verwijfsindex

De basisinfrastructuur gaat uit van het principe dat informatie zoveel mogelijk bij de bron blijft. Aldus blijft een ongeadresseerd medicatievoorschrift gewoon bij de voorschrijver, zolang er nog geen verstrekker is geselecteerd. Als de patiënt eenmaal een verstrekker heeft gekozen, kan deze verstrekker het ongeadresseerde medicatievoorschrift gewoon opvragen bij de voorschrijver.

Om een medicatievoorschrift te kunnen opvragen, moet de voorschrijver dit medicatievoorschrift wel eerst aanmelden bij de verwijfsindex. Gewoonlijk wordt een opdracht niet aangemeld bij de verwijfsindex, want een opdracht is voor niemand interessant anders dan de zorgverlener die deze opdracht toch al ontvangen heeft. Ongeadresseerde opdrachten vormen daarop een uitzondering: ze kunnen worden aangemeld in de verwijfsindex en vervolgens opgevraagd via de verwijfsindex, volgens hetzelfde mechanisme als bij de medische patiëntgegevens.

Daarnaast zijn voor een ongeadresseerd medicatievoorschrift nog extra functies nodig:

- na opvraag moet een verstrekker een medicatievoorschrift kunnen *overnemen*, waarbij het voorschrift uit de verwijfsindex wordt verwijderd. De situatie is dan alsof het voorschrift direct naar deze verstrekker was verstuurd. De verdere afhandeling geschiedt vervolgens op dezelfde wijze als voor directe opdrachten.
- na overname moet een verstrekker het medicatievoorschrift eventueel kunnen *teruggeven*, waarbij het voorschrift in de verwijfsindex wordt teruggezet. De situatie is dan alsof het voorschrift nooit was overgenomen. Zo kan een andere verstrekker het voorschrift overnemen.



De bovenstaande figuur toont het afhandelen van een ongeadresseerde opdracht. Niet getoond is dat de aanvrager ná overname van de opdracht, maar vóór ontvangst van een resultaat, de opdracht nog kan annuleren.

Deze oplossing wijkt nauwelijks af van de NEN7503 ontwerpnorm. Immers de verwijfsindex speelt de rol van *informatiedoorgever*, behalve dat de verwijfsindex niet het ongeadresseerde medicatievoorschrift zelf, maar de verwijfsing daarnaar, bevat.

## B.4 Ontwerpkeuzes

In het bovenstaande voorstel zijn impliciet een aantal keuzes gemaakt die hier worden besproken:

- Iedere medicatie wordt als aparte opdracht aangemeld in de verwijfsindex. Daardoor is het ingewikkelde mechanisme van NEN7503 niet nodig, waarbij bepaalde medicatieregels worden geselecteerd.
- Bij het opvragen van ongeadresseerde opdrachten via de verwijfsindex werkt hetzelfde mechanisme als bij het opvragen van medische patiëntgegevens, dus inclusief autorisatie en logging. Zo kan bijv. worden voorkomen dat andere partijen dan apotheken ongeadresseerde medicatievoorschriften gaan opvragen.
- Bij het overnemen van een ongeadresseerde opdracht wordt de opdrachtgever niet geïnformeerd door de verwijfsindex. Net als bij het plaatsen van een directe opdracht, kan de opdrachtgever ook bij het aanmelden van een ongeadresseerde opdracht aangeven dat hij een expliciete acceptatie van de opdracht verwacht. De opdrachtnemer kan de opdracht dan zelf direct naar de opdrachtgever beantwoorden met een acceptatie, buiten de verwijfsindex om.
- Na het overnemen van een ongeadresseerde opdracht kan blijken dat de opdrachtnemer de opdracht toch niet kan uitvoeren. Bij een directe opdracht kan de opdrachtnemer deze direct naar de opdrachtgever beantwoorden met een afwijzing. Maar dat zou betekenen dat de opdrachtgever de opdracht opnieuw moet aanmelden bij de verwijfsindex. Daarom is hier gekozen voor het teruggeven van de opdracht aan de verwijfsindex, alsof er niks was gebeurd.
- Het teruggeven van een opdracht aan de verwijfsindex komt neer op het opnieuw aanmelden in de verwijfsindex. In afwijking van het normale mechanisme heeft de aanmelding betrekking op gegevens die bij een ander liggen dan degene die de aanmelding doet. Misschien is het beter om de ongeadresseerde opdracht niet eerder uit de verwijfsindex te verwijderen, dan wanneer de opdrachtnemer de opdracht al heeft beantwoord aan de opdrachtgever met een acceptatie. Overigens kent NEN7503 geen bericht voor het teruggeven van een receptaanvraag.
- Als een opdrachtnemer een opdracht al heeft beantwoord aan de opdrachtgever met een acceptatie, kan hij de opdracht niet meer teruggeven aan de verwijfsindex. Net als bij een directe opdracht, kan hij de opdracht alleen nog maar direct afwijzen naar de opdrachtgever. De laatste zal de opdracht opnieuw moeten aanmelden.

# Bijlage C – Bijhouden van de verwijfsindex

## C.1 Inleiding

Zorgaanbieders moeten in principe voor al hun patiënten de verwijfsindex bijhouden, door middel van aanmelden, heraanmelden en afmelden. Paragraaf 5.3 beschrijft dat de verwijfsindex (VWI) per verwijfsing de volgende attributen bevat:

- patiënt-id (BSN)
- applicatie-id
- beheerverantwoordelijke:
  - zorgaanbieder-id
  - zorgverlener-id
  - zorgverlener-functie
- inhoudverantwoordelijke:
  - zorgaanbieder-id
  - zorgverlener-id
  - zorgverlener-functie
- gegevenssoort
- patiëntgegevens-id
- actualiteit, bestaande uit:
  - begintijd
  - eindtijd
- foutenteller
- {toekomst} status

De vraag is welke attributen verplicht zijn bij aanmelden, welke attributen wijzigbaar zijn bij heraanmelden en welke attributen van belang zijn bij afmelden. Ook is de vraag onder welke voorwaarden een aanmelding, heraanmelding of afmelding kan of moet worden gedaan. Tenslotte is de vraag wanneer moet worden aangemeld en hoe vaak moet worden heraanmeld.

## C.2 Sleutel

Iedere verwijfsing in de VWI heeft een *patiëntgegevens-id* als verwijfsing naar de patiëntgegevens waarnaar verwezen wordt. In geval van een atomaire verwijfsing is deze gelijk aan de *patiëntstuk-id* van het desbetreffende patiëntstuk, in geval van een categorale verwijfsing is deze te beschouwen als *categorie-id* van de desbetreffende gegevenssoort. Om deze *patiëntgegevens-id* te kunnen gebruiken als sleutel binnen de VWI, moet deze uniek zijn.

De *patiëntgegevens-id* moet bij aanmelden worden meegegeven door de aanmeldende GBZ-applicatie. De ZIM moet een reeds bekende *patiëntgegevens-id* in een aanmelding weigeren, omdat de *patiëntgegevens-id* uniek moet zijn. Voor de wijze waarop een GBZ-applicatie de uniciteit kan garanderen, zie document [Technische Architectuur] onder Betrouwbaarheid.

Dezelfde GBZ-applicatie moet al zijn *patiëntgegevens-id*'s onthouden zodat deze kunnen worden meegegeven bij het heraanmelden of afmelden van een verwijfsing. De ZIM heeft voor een heraanmelding of afmelding de desbetreffende *patiëntgegevens-id* nodig om te

bepalen om welke verwijzing het gaat. De ZIM moet een niet bekende *patiëntgegevens-id* in een heraanmelding of afmelding weigeren.

Een GBZ-applicatie moet voor iedere *patiëntgegevens-id* onthouden of deze al is aangemeld bij de VWI of niet. Immers, de ZIM weigert een aanmelding voor een reeds bekende *patiëntgegevens-id* en weigert een heraanmelding voor een niet bekende *patiëntgegevens-id*.

### C.3 Beperkingen bij heraanmelden of afmelden

Om te voorkomen dat een zorgaanbieder onbedoeld andermans verwijzingen in de VWI gaat corrumpen of dat een hacker de gehele VWI gaat saboteren, moet de mogelijkheid tot *heraanmelden* en *afmelden* van een verwijzing *tenminste* worden beperkt tot de *zorgaanbieder* die de verwijzing heeft *aangemeld*.

Dit betekent dat de ZIM:

- de *zorgaanbieder-id* (URA) van de aanmelder moet vastleggen als *beheerverantwoordelijke* bij iedere verwijzing in de VWI, zoals te halen uit de ControlAct Wrapper van het aanmeld-bericht en gecontroleerd met die op het gebruikte UZI-certificaat.
- na ontvangst van een heraanmeld-bericht of afmeld-bericht moet controleren of de *zorgaanbieder-id* (URA) van de *beheerverantwoordelijke* zoals vastgelegd in de onderhavige verwijzing in de VWI overeenkomt met die genoemd in de ControlAct Wrapper van het bericht en gecontroleerd met die op het gebruikte UZI-certificaat.

Om te waarborgen dat een zorgverlener zijn eigen verantwoordelijkheid voor verwijzingen in de VWI volledig kan nakomen, zonder dat collega's zijn verwijzingen kunnen bijwerken, zou het in theorie wenselijk zijn om de mogelijkheid tot *heraanmelden* en *afmelden* van een verwijzing *nader* te beperken tot de *zorgverlener* die het heeft *aangemeld*.

Nadeel daarvan is echter dat nauw samenwerkende zorgverleners binnen een zorgaanbieder (denk aan specialisten binnen een ziekenhuis die voor elkaar als medebehandelaar optreden) niet meer zo gemakkelijk één dossier kunnen delen, ook niet als de zorgaanbieder daarvoor alle verantwoordelijkheid wil nemen.

Nog groter nadeel zou zijn dat, als een zorgverlener eenmaal patiëntgegevens voor een patiënt heeft aangemeld bij de VWI en vervolgens uit dienst treedt, zijn opvolger deze niet meer zou kunnen afmelden als dat nodig is, bijv. na afloop van de wettelijke bewaartermijn. Naderhand zou de oorspronkelijke zorgverlener ook niet meer kunnen afmelden, als zijn UZI-pas eenmaal is verlopen of ingetrokken door zijn ex-werkgever. Om dit te vermijden, zouden uittredende zorgverleners op hun laatste werkdag hun beheerverantwoordelijkheid voor alle verwijzingen in de VWI moeten overdragen aan hun opvolger.

Aldus is het praktischer de verantwoordelijkheid voor zorgverleners die elkaars aanmeldingen in de VWI gaan bijwerken, neer te leggen bij de zorgaanbieder. Als een zorgaanbieder dit beslist wil uitsluiten, kan diens GBZ dat zelf afdwingen, in plaats van de ZIM.

## C.4 Verantwoordelijke partij

Het bovenstaande betekent dat onderscheid gemaakt moet worden tussen:

- *Inhoudverantwoordelijke*: degene die verantwoordelijk is voor de juistheid van de medische inhoud van de patiëntgegevens.
- *Beheerverantwoordelijke*: degene die verantwoordelijk is voor het bewaren van bepaalde patiëntgegevens en het zonodig ter beschikking stellen daarvan aan anderen.

Merk op dat de *inhoudverantwoordelijke* zorgaanbieder niet altijd gelijk is aan de *beheerverantwoordelijke* zorgaanbieder. Immers, als een zelfstandige zorgverlener stopt met zijn praktijk, kan een andere praktijk zijn patiëntdossiers overnemen. Daarbij wijzigt de *beheerverantwoordelijke* maar niet de *inhoudsverantwoordelijke*.

Het kan nuttig zijn om beide partijen te hebben vermeld in de VWI want:

- de *beheerverantwoordelijke* kan men dan bellen als er *logistieke* problemen zijn met de aangemelde patiëntstukken. Bijv. als een opvraag niks oplevert ondanks de verwijzing in de VWI.
- de *inhoudverantwoordelijke* kan men dan bellen als er *zorginhoudelijke* vragen zijn over de aangemelde patiëntstukken. Ook kun je dit attribuut gebruiken als selectie-parameter om bij een opvraag te zoeken naar patiëntstukken van één bepaalde zorgverlener.

Beide verwijzen naar zowel de verantwoordelijke zorgverlener als de zorgaanbieder onder wiens verantwoordelijkheid hij op dat moment werkt. In de praktijk is het meestal niet de zorgverlener maar een gemandateerde medewerker die de feitelijke handeling uitvoert. De mandaterende zorgverlener geldt dan als verantwoordelijke. Zie ook [Bedrijfsarchitectuur] paragraaf 5.3 en 7.3.

Uit medisch oogpunt is de vermelde zorgverlener (UZI-nr) zelden interessant. Zeker op landelijke schaal, zal de VWI vooral onbekende zorgverleners bevatten. Bovendien als een zorgverlener wil bellen, heeft hij van de *inhoudverantwoordelijke* zorgaanbieder meestal de dienstdoende arts nodig. Van de *beheerverantwoordelijke* zorgaanbieder heeft hij meestal geen arts maar een medewerker nodig. Vooral zorgverleners van een grote zorginstelling zien het beheer van patiëntgegevens als een taak van de zorginstelling.

Voor een patiënt, daarentegen, die zijn deel van de VWI wil kunnen raadplegen, zijn de zorgverlener wel interessant omdat hij die zal herkennen. Voor het vertrouwen van de patiënt in de VWI is het belangrijk dat hij kan zien dat de beheer van zijn patiëntgegevens in goede handen is. Als hij daaraan twijfelt kan hij aan de hand van de VWI de verschillende verantwoordelijke zorgverleners daarop aanspreken.

## C.5 Verplichte attributen bij aanmelden

Bij het aanmelden van patiëntgegevens bij de VWI zijn de meeste attributen verplicht. Alleen de actualiteit is optioneel.

## C.6 Wijzigbare attributen bij heraanmelden

Het heraanmelden was oorspronkelijk bedoeld voor het actualiseren van het attribuut *actualiteit* in een eerder, categoriaal aangemelde verwijzing in de VWI. Inmiddels blijkt dat er ook de behoefte bestaat om andere attributen te actualiseren en niet alleen voor categorale verwijzingen:

- *Applicatie-id*: een zorgaanbieder zou deze willen actualiseren als zijn oude GBZ-applicatie wordt vervangen door een nieuwe GBZ-applicatie.

In plaats van actualiseren is het ook mogelijk dat de oude GBZ-applicatie alles afmeldt en de nieuwe GBZ-applicatie alles opnieuw aanmeldt. Dat zou eigenlijk in omgekeerde volgorde moeten, want tijdens de migratie heb je liever een dubbele verwijzing dan géén verwijzing.

Afhankelijk van de wijze waarop de migratie wordt gedaan, kan bovenstaande werkwijze lastig zijn. Gemakkelijker kan soms zijn dat een nieuwe GBZ-applicatie gewoon de bestaande verwijzingen opvraagt uit de oude database of opvraagt bij de ZIM en door middel van heraanmelden de *applicatie-id* actualiseert.

Het kunnen wijzigen van een applicatie-id heeft wel het risico dat verschillende GBZ-applicaties elkaars verwijzingen onbedoeld wijzigen. Denk bijv. aan een ziekenhuis waar GBZ-applicaties van verschillende XIS-leveranciers worden geïmplementeerd zonder onderlinge afstemming.

Merk op dat wijzigen van de applicatie-id momenteel impliciet gebeurt omdat de ZIM veronderstelt dat de (her)aanmeldende applicatie gelijk is aan de gegevenshoudende applicatie. In de toekomst zal het mogelijk worden dat applicatie 1 een (her)aanmelding doet met verwijzing naar applicatie 2.

- *beheerverantwoordelijke Zorgverlener-id* en *Zorgverlener-functie*: wanneer een collega-zorgverlener de behandeling van een patiënt overneemt, zou hij na bijwerken van bepaalde patiëntgegevens de desbetreffende verwijzing in de VWI ook willen bijwerken. Alles onder de voorwaarde dat de zorgaanbieder dit wil toestaan.

Het alternatief dat de nieuwe zorgverlener alles nieuw aanmeldt en de oude zorgverlener alles afmeldt, is in de dynamiek van de dagelijkse praktijk erg omslachtig en soms onmogelijk. Misschien is de andere arts niet eens meer beschikbaar.

- *beheerverantwoordelijke Zorgaanbieder-id*: een patiënt zou deze misschien willen laten actualiseren als hij een nieuwe zorgaanbieder heeft gekozen en het patiëntdossier bij de oude zorgaanbieder wil laten overdragen naar de nieuwe.

Hier gaat het om *overdracht* van een dossier, waarbij de ene zorgaanbieder de verantwoordelijkheid overneemt en de andere zorgaanbieder afstand doet. Zoals blijkt uit issue 1108 is voor *overdracht* gekozen voor een speciale reeks van interacties met de VWI als regisseur van de overdracht. Dit betekent dat het attribuut *zorgaanbieder-id* niet wijzigbaar moet zijn.

- *inhoudverantwoordelijke Zorgverlener-id* en *Zorgverlener-functie*: voor categorale verwijzingen zou een ziekenhuis deze misschien willen actualiseren als een nieuwe

arts als hoofdbehandelaar een patiënt heeft overgenomen van een andere arts en zich verantwoordelijk wil verklaren voor de inhoud van het hele dossier.

Ook voor atomaire verwijzingen zijn deze attributen wijzigbaar, bijv. als een nieuwe versie van het document, bijgewerkt door een andere zorgverlener, wordt vrijgegeven. Denk aan een voorlopige labuitslag die definitief wordt gemaakt.

- *inhoudverantwoordelijke Zorgaanbieder-id*: dit attribuut is in principe nooit wijzigbaar. Na overdracht van een patiëntdossier zou een zorgverlener van de nieuwe zorgaanbieder kunnen besluiten alle patiëntgegevens op te nemen in het eigen dossier, maar dan zal de verwijzing naar het oude dossier geheel worden verwijderd uit de VWI.

De attributen *BSN*, *gegevenssoort* en *patiëntgegevens-id* zijn zo wezenlijk voor een verwijzing, dat die nooit gewijzigd mogen worden. Enige toekomstige uitzondering is dat een gegevenssoort eventueel verbijzonderd kan worden, bijv. van *medicatie* naar *medicatieverstrekking*.

## C.7 Voorwaarden voor aanmelden

Om patiëntgegevens beschikbaar te maken voor landelijke opvraag door anderen, moet de beheerverantwoordelijke in principe altijd de patiëntgegevens van al zijn patiënten aanmelden bij de VWI. Zonder verwijzingen in de VWI is landelijke opvraag niet mogelijk.

Een cruciale vraag is: moeten GBZ-applicaties de VWI bijhouden voor patiënten die bezwaar hebben gemaakt tegen landelijke uitwisseling van hun patiëntgegevens? Een dergelijk bezwaar wordt vastgelegd in een autorisatieprofiel van die patiënt in de ZIM, zie paragraaf 4.13.

Reden om dit *niet* te doen is privacy. Als de patiënt bezwaar heeft gemaakt, mag de ZIM diens patiëntgegevens niet uitwisselen. Er is dan geredeneerd vanuit de WBP ook geen noodzaak om in de VWI verwijzingen van zorgaanbieders bij te houden. Bovendien zijn die verwijzingen ook op te vatten als gezondheidsgegevens. Bijv. het feit dat een psychiater voor een patiënt medicatie voorschriften heeft aangemeld, zegt iets over de gezondheidstoestand van die patiënt. Volgens de WBP heeft iedereen het recht bezwaar te maken tegen een dergelijke registratie.

Reden om dit *wel* te doen is doelmatigheid. Als een patiënt in latere instantie zijn bezwaar intrekt, zou de VWI idealiter meteen gevuld zijn met alle verwijzingen. Anders moeten al zijn zorgaanbieders alsnog de patiëntgegevens voor deze patiënt aanmelden. De ZIM zou ervoor kunnen zorgen dat de VWI geheel onzichtbaar blijft, zolang het bezwaar van de patiënt van kracht is.

Omdat privacy zwaarder weegt dan doelmatigheid, is de conclusie: voor patiënten die bezwaar hebben gemaakt tegen elektronische uitwisseling van hun patiëntgegevens moet geen VWI worden bijgehouden, zie [VWI·b05]. Bovendien heeft de patiënt de keuze voor een tussenoplossing: wel akkoord gaan, maar alle zorgaanbieders uitsluiten in het autorisatieprofiel. Deze architectuurbeslissing heeft een aantal consequenties.

Volgens het principe van de veronderstelde toestemming, zie [Bedrijfsarchitectuur] paragraaf 9.2, mag een zorgverlener ervan uitgaan dat voor al zijn patiënten de



patiëntgegevens moeten worden aangemeld. Aldus moet een GBZ-applicatie na het vastleggen en vrijgeven van patiëntgegevens altijd een poging tot (her-) aanmelden doen. Als de ZIM na raadpleging van het autorisatieprofiel constateert dat de patiënt bezwaar heeft gemaakt, moet de ZIM de (her-) aanmelding weigeren en de reden opgeven. De GBZ-applicatie moet de zorgverlener inlichten over het bezwaar, zodat hij de patiënt nog eens kan uitleggen wat de voordelen van landelijke uitwisseling van patiëntgegevens zijn voor de continuïteit van de zorg.

Wanneer de patiënt later doorgeeft aan de autorisatiemanager *alsnog* akkoord te gaan met landelijke uitwisseling van patiëntgegevens, zullen zijn zorgaanbieders de nog niet aangemelde patiëntgegevens *alsnog* moeten aanmelden bij de VWI. Dit betekent dat de patiënt zelf al zijn zorgaanbieders langs moet gaan, met het verzoek om zijn patiëntgegevens *alsnog* aan te melden. De zorgaanbieder moet dan in staat zijn op verzoek van de patiënt alle vrijgegeven patiëntgegevens in één keer aan te melden bij de VWI, zie [PUB-b03]. Dit is geen ideale oplossing, want het kost de patiënt veel inspanning en hij kan er gemakkelijk eentje vergeten. Echter, het alternatief om de ZIM automatisch naar alle aangesloten zorgaanbieders een verzoek te sturen "Gaarne voor patiënt X alle beschikbare gegevenssoorten aanmelden" is (nog) niet mogelijk want dat zou een nieuw HL7v3-bericht moeten worden ontwikkeld.

Wanneer de patiënt nog later doorgeeft *niet langer* akkoord te gaan, zal de ZIM zelf automatisch alle verwijzingen in de VWI wissen, zie paragraaf 4.13. De aangesloten zorgaanbieders worden daarover niet expliciet ingelicht door de ZIM, maar zullen het impliciet vernemen via hun GBZ bij de eerstvolgende mislukte (her-) aanmelding of anderszins uitwisseling van patiëntgegevens voor die patiënt, of expliciet na kennisgeving door de patiënt zelf. Het is belangrijk dat zorgaanbieders zich dan realiseren dat de VWI voor die patiënt is gewist.

Zoals uitgelegd in paragraaf C.2 moet een GBZ-applicatie voor iedere *patiëntgegevens-id* onthouden of deze al is aangemeld bij de VWI of niet. Dit betekent dat een GBZ-applicatie na ontvangst van de foutmelding dat de patiënt bezwaar heeft gemaakt tegen landelijke uitwisseling van zijn patiëntgegevens, moet onthouden dat alle verwijzingen zijn gewist. Vanaf dat moment hoeft de GBZ-applicatie geen aanmeldingen meer te doen, totdat de patiënt langskomt.

## C.8 Conclusie

De VWI bevat in principe verwijzingen voor alle patiëntgegevens van alle patiënten van zorgaanbieders die zijn aangesloten op het LSP, behalve voor patiënten die bezwaar hebben gemaakt tegen elektronische uitwisseling van hun patiëntgegevens.

De VWI bevat per verwijzing de volgende attributen:

- patiënt-id (BSN)                      verplicht, niet wijzigbaar
- applicatie-id                          verplicht, wijzigbaar
- beheerverantwoordelijke:
  - zorgaanbieder-id                      verplicht, niet wijzigbaar
  - zorgverlener-id                        verplicht, wijzigbaar
  - zorgverlener-functie                  verplicht, wijzigbaar
- inhoudverantwoordelijke:
  - zorgaanbieder-id                      verplicht, niet wijzigbaar
  - zorgverlener-id                        verplicht, wijzigbaar
  - zorgverlener-functie                  verplicht, wijzigbaar
- gegevenssoort                        verplicht, niet wijzigbaar, wel te verbijsonderen
- patiëntgegevens-id                    verplicht, niet wijzigbaar (sleutel)
- actualiteit, bestaande uit:
  - begintijd                                optioneel, wijzigbaar
  - eindtijd                                  optioneel, wijzigbaar
- foutenteller                            (verborgen)
- {toekomst} status