Handreiking

Informatiebeveiliging voor eerstelijnsinformatiesystemen

DEEL 2 TOEGANGSLOG

Betere gezondheid door betere informatie Nictiz

Datum: januari 2017
Versie: 1.1
Status: definitief

nhg nederlands huisartsen genootschap
LHV Landelijke Huisartsen Vereniging
ineen ORGANISEERT DE EERSTE LIJN
KNMP

Optimale toepassing van eHealth en ICT in de zorg kan niet zonder standaardisatie. In nauwe samenwerking met zorgverleners, koepelorganisaties, standaardisatieorganisaties en industrie draagt Nictiz zorg voor de ontwikkeling en beschikbaarheid van de noodzakelijke standaarden. We doen dit door het organiseren van gemeenschappelijke ontwikkelprojecten, kennisoverdracht en kwaliteitstoetsing.

Nictiz
Postbus 19121
2500 CC Den Haag
Oude Middenweg 55
2491 AC Den Haag

T 070 - 317 34 50
@Nictiz
info@nictiz.nl
www.nictiz.nl

Inhoud

H-1 Inleiding

1.1. Aanleiding

Vanuit de maatschappij bestaat de uitdrukkelijke vraag om medische gegevens te beschermen tegen onbevoegde inzage en gebruik. Vigerende wet-, regelgeving , gedragscodes en NEN-normeringen vormen de basis voor de beveiliging van de medische gegevens (maatregelen, controle op toepassing en sancties). Aan de ene kant moeten medische dossiers of dossierdelen goed toegankelijk zijn voor zorgverleners en medewerkers die zorgtaken uitvoeren of voor administratieve voorbereiding of afhandeling. Aan de andere kant dienen medische dossiers zodanig beveiligd te worden dat een zorgverlener of medewerker niet ongezien kan "kijken en muteren" in dossiers waar hij niets te zoeken heeft en moeten ze niet toegankelijk zijn voor derden. De patiënt dient bij de beveiliging zelf een controlerol en de daarvoor noodzakelijke controlemogelijkheden te krijgen.

BEIS is een programma waarin de eerstelijnskoepels NHG, LHV, KNMP en InEen samen met Nictiz een handreiking in de vorm van een pakket van eisen hebben ontwikkeld, voor veilig en controleerbaar gebruik van deze systemen en de daarin opgeslagen medische gegevens.

1.2. Doel

BEIS heeft een tweeledig doel. BEIS heeft als hoofddoel te bevorderen/waarborgen dat de eerstelijns informatiesystemen (gaan) voldoen aan de wet- en regelgeving en NEN-normen, en te zorgen dat gebruikers controle kunnen houden op de beveiliging.
Het tweede doel dat de koepels met BEIS voor ogen hebben is, hun leden en gebruikersverenigingen en –platforms van XISSEN te faciliteren bij het vertalen van wet-, regelgeving en NEN-normen naar implementeerbare en op de zorgpraktijk afgestemde eisen voor de eerstelijnssystemen.

1.3. Aanpak

Authenticatie, autorisatie en logging helpen zorgaanbieders om deze zaken goed te regelen. De beveiliging richt zich op veilige toegangscontrole (hoe mag een gebruiker erin ofwel authenticatie), gecontroleerde toegang tot gegevens (waar heb je toegang tot en wat mag je doen ofwel autorisatie) en controleerbaarheid van die beveiliging (bijhouden van gebruik ofwel logging). De transparantie van de beveiliging wordt onderstreept door de mogelijkheid voor de patiënt om de loggegevens van de toegang tot de eigen medische gegevens te kunnen raadplegen. Gedurende het programma zijn de leveranciers van systemen geïnformeerd over de vorderingen en zijn commentaren en aanpassingen van hun kant verwerkt.

Resultaat

Het resultaat van BEIS is een pakket van eisen te gebruiken als praktische implementatiegids voor leveranciers en gebruikers van eerstelijnssystemen. BEIS beschrijft de eisen die aan systemen moeten worden gesteld op gebied van authenticatie, autorisatie en logging van de toegang. Het biedt de basis voor leveranciers van systemen om deze op het juiste beveiligingsniveau te brengen.
Het voldoen aan deze set van eisen moet ook de patiënten, overheid, toezichthouders en verzekeraars de zekerheid kunnen geven dat de noodzakelijke kwaliteit van de informatiebeveiliging in de eerstelijns is gegarandeerd.

Bestuurlijke bekrachtiging

De besturen van de betrokken koepels bekrachtigen het resultaat van BEIS en bieden de rapporten aan hun leden, de gebruikersverenigingen van XISSEN en betrokken software leveranciers aan.

1.4. Dit document

Dit document bevat:

- de eisen aan de toegangslog;
- de eisen aan de weergave van de toegangslog;
- een specificatie van de gegevens in de toegangslog;
- voorbeelden van de weergave van de toegangslog;
- een begrippenlijst.

1.5. Uitgangspunten en randvoorwaarden

- De eisen zijn zo opgesteld dat ze toetsbaar zijn in een zelftoets of een externe toets.
- De eisen zijn gebaseerd op bestaande documentatie:
    - NEN 7513 – Logging – Vastleggen van acties op elektronische patiëntendossiers, juli 2010
    - Programma van eisen organisatie goed beheerd systeem (GBx), december 2012
    - Gedragscode Elektronische gegevensuitwisseling in de zorg (EGiZ), juli 2013
    - CBP – Toegang tot digitale patiëntendossiers binnen zorginstellingen, juni 2013
    - HIS-referentiemodel, september 2012
    - IHE IT Infrastructure – Audit Trail and Node Authentication (ATNA), september 2013
    - RFC-3881 - Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications, september 2004
- De eisen bestaan uit oplossingsonafhankelijke beschrijvingen, eventueel met voorbeelden.
- In de C*onformiteitstoelichting* (bijlage 3) is beschreven hoe partijen kunnen voldoen aan de eisen.

1.6. Leeswijzer

Dit document geeft een handreiking voor het inrichten van toegangslogging in informatiesystemen in de eerstelijn. Het is bedoeld voor verantwoordelijke bestuurders van zorgaanbieders in de eerstelijn, zorgverleners en leveranciers van informatiesystemen.

Hoofdstuk 2 beschrijft de achtergrond en de relatie tussen logging, authenticatie en autorisatie.
Hoofdstuk 3 beschrijft de concrete eisen aan de toegangslog en aan de weergave ervan aan verantwoordelijken bij de zorgaanbieder en de patiënt.
Bijlage 1 beschrijft begrippen en het gegevensmodel.
Bijlage 2 geeft aan de hand van scenario's voorbeelden van de log.
Bijlage 3 toont de weergave van de log.
Bijlage 4 is de conformiteittoelichting en geeft richting aan implementatie en kwalificatie.
Bijlage 5 beschrijft situaties en vragen die aanleiding kunnen geven tot discussie en tevens de keuzes die daarin zijn gemaakt.

H-2 Achtergrond

2.1. Authenticatie , autorisatie en toegangslogging

Authenticatie betreft het identificeren van de gebruiker die toegang wenst tot het systeem en vervolgens het zeker stellen dat die gebruiker ook werkelijk is wie hij zegt dat hij is. Hiervoor wordt gebruik gemaakt van zogenaamde 2-factor authenticatie. De 2 factoren zijn te kenschetsen als iets wat men heeft en iets wat men weet. Gebruikersnaam en wachtwoord zijn dus geen 2 factoren, dat zijn 2 zaken die men weet.
Iets wat men heeft kan een pas zijn, maar ook een telefoon of een lichamelijke eigenschap (vingerafdruk, iris). Om zeker te zijn dat hetgeen men heeft ook toebehoort aan degene die zich wil authenticeren, is het afgifteproces van belang. Men moet zich persoonlijk identificeren met bijv. een paspoort om het middel te verkrijgen. Iets wat men weet is meestal een wachtwoord.
Zodra de gebruiker is geauthentiseerd, kan worden vastgesteld welke functie deze gebruiker binnen het systeem bekleedt. Dit volgt direct uit bijv. de personeelslijst met namen, functies en verantwoordelijkheden.
Betrouwbare authenticatie is een onmisbaar deel van een goede toegangsbeheersing

Autorisatie betreft het gecontroleerd vaststellen van de rechten die aan de gebruiker moeten worden toegekend op basis van de functie die wordt bekleed en eventuele speciale verantwoordelijkheden. Deze rechten bepalen of de gebruiker toegang krijgt tot delen van het systeem, waaronder de medische gegevens van patiënten. Deze rechten worden in een administratief proces, vooraf, gekoppeld aan de gebruiker. De gebruiker is bijvoorbeeld huisarts in een HAP en krijgt daarmee de rol huisarts. Hij heeft op basis van die functie toegang tot de medische gegevens, maar niet tot beheertaken of financiële gegevens. Als de gebruiker naast zijn functie nog extra taken heeft, bijvoorbeeld controle van de toegangslog, worden deze rechten via een additionele rol, toegangslogverantwoordelijke, toegekend.
Naast de rollen zijn er nog wettelijk gereguleerde toegangscontroles, de behandelrelatie en in sommige situaties de toestemming van de patiënt. Alleen als er sprake is van een behandelrelatie mag de gebruiker toegang krijgen tot de medische gegevens van een patiënt. Daarnaast kan de patiënt in het dossier bepaalde gegevens laten afschermen voor anderen dan zijn eigen zorgverlener.
Voor noodsituaties is een noodknop bedacht. In acute situaties waarbij kennis van de medische gegevens van groot belang kan zijn voor de juiste behandeling, kan een noodknop gebruikt worden om toegang te kunnen krijgen tot gegevens waar men volgens de voorgaande controles geen recht toe heeft.
Gestandaardiseerde autorisatie maakt toegang veel beter beheersbaar.

Toegangslogging betreft het vastleggen van activiteiten waarbij toegang tot medische gegevens is verkregen. Het doel is achteraf te kunnen vaststellen welke inzage in dossiers er is geweest en door wie dat is gedaan. Het bijhouden van een toegangslog maakt het mogelijk om onterechte en ongewenste inzage aantoonbaar te maken en daar, weliswaar achteraf, actie op te ondernemen.
De controle vooraf kan niet helemaal waterdicht zijn (behandelrelatie, noodknop) en controle achteraf wordt gezien als het beste middel in ongewenste inzage te voorkomen. Het is daarbij wel een vereiste deze controle met regelmaat uit te voeren.
Daarnaast is de controlemogelijkheid voor de patiënt van groot belang. Deze moet toegang hebben tot de logregels die de toegang tot zijn gegevens hebben vastgelegd. Deze mogelijkheid laat zien hoe de gegevens worden gebruikt en verhoogt het vertrouwen in kwaliteit en veiligheid.

Het loggen van toegang wordt gezien als het sterkste middel voor het voorkomen van ongewenste inzage. De recente historie laat een tendens zien om ongewenste inzage op te volgen met ontslag op staande voet.

N.B*. De logging is specifiek gericht op het vastleggen van de toegang tot medische gegevens., opdat kan worden achterhaald of de privacy van de patiënt is geschonden. Hier wordt niet de volledige logging van het systeem beschreven.*
N.B. *De presentatie van de logging is enerzijds gericht op de beheerder en anderzijds op de patiënt die inzicht moet kunnen krijgen. Met het oog hierop zijn keuzes gemaakt om de overzichtelijkheid en daarmee controleerbaarheid van de log te verbeteren.*

2.2. Informatiedomein

Het is belangrijk voor een organisatie om de vraag te beantwoorden op welke applicaties en bestanden de logging, authenticatie en autorisatie betrekking hebben. Een combinatie van applicaties en bestanden met hetzelfde regime noemen we - in navolging van de NEN7513 - een informatiedomein. Er doen zich in sommige situaties ook meerdere goede keuzes voor.

Een informatiedomein zoals beschreven in de NEN is *Een gebied waarbinnen het beleid en de verantwoordelijkheden ten aanzien van de informatievoorziening gemeenschappelijk zijn en de naamgeving van personen, systemen en andere objecten uniek is*.
Een belangrijke consequentie van de afbakening is: gegevens die het informatiedomein verlaten, moeten worden gelogd als 'export'. Als het daarbij gaat om niet-geanonimiseerde gegevens, kan dit leiden tot veel logregels. Dit pleit ervoor om het informatiedomein niet te smal te kiezen.
De keerzijde lijkt dat alle toegang tot gegevens binnen dat bredere informatiedomein moet worden gelogd, maar dat moest toch al. Alleen gaat het vaak om een andere leverancier. Wat wel mag is werken met meerdere logbestanden en meerdere autorisatietabellen, maar alle overzichten gelden voor het gehele informatiedomein en moeten alle logbestanden omvatten.

Een ander aspect waarover binnen het informatiedomein moet worden nagedacht is de te hanteren toegangsprotocollen. Het gaat dan om het protocol voor autorisatie, het protocol voor het controleren van toestemming, het protocol voor het controleren van de behandelrelatie en het protocol voor het gebruik van de noodknop. Die gelden voor het gehele informatiedomein.

Het is mogelijk om twee informatiedomeinen te combineren tot een *samengesteld informatiedomeinen.* In dat geval gelden dezelfde naamgeving et cetera, maar - verdergaand dan de norm - kunnen verschillende protocollen gelden. In alle gevallen moeten de oid's in de logregel verwijzen naar de gehanteerde protocollen die golden bij de betreffende toegangspoging.

Ten slotte ook uit de NEN7513: *In samenwerkingsverbanden en complexere organisaties zijn veel informatiesystemen aanwezig. Dan kan een enkel informatiedomein worden gevormd wanneer voor een gemeenschappelijk regime wordt gekozen. Een bijzonder informatiedomein vormt het landelijk (virtueel) EPD van AORTA met het landelijk schakelpunt als centraal systeem. Beleid, verantwoordelijkheden en naamgeving zijn hiervoor op nationaal niveau bepaald. Aan het andere eind van het spectrum vormt het persoonlijk zorgdossier van een patiënt een privé informatiedomein.*

2.3. Deel 2: logging van toegang

Dit eerste deel geeft de regels voor logging van gepleegde toegang. We gaan hier wat dieper op in en bekijken de risico's die we willen verminderen, en hoe we voorstellen dat te doen.

Welke type risico is in scope?
Het is belangrijk dat we ons realiseren dat we het hier hebben over risico's binnen de rechtenstructuur, en dus niet over risico's door in het systeem in te breken; die moet de organisatie op andere manieren afdekken. En dat we het hebben over een expliciet afgebakend informatiesysteem ('systeem') waarvoor we de logging willen inrichten. Hiermee wordt bedoeld een geheel van 1 of meer systemen die onder de verantwoordelijkheid van één zorgaanbieder vallen.
Het gaat dan om alle toegang tot dossiers gezocht door de eigen medewerkers via de reguliere toegangsroutes van het systeem. Dat kunnen dossiers zijn die in het systeem zijn opgeslagen, maar ook dossiers elders die de medewerker via het systeem kan opvragen. De scope omvat ook de toegang tot het systeem vanuit een andere organisatie (vooruitlopend: in de autorisatiestructuur krijgt deze externe raadpleger ook een rol). Ook binnen de scope valt de toegang tot dossiers vanuit een applicatie die bijvoorbeeld op gezette tijden dossiers selecteert om te exporteren uit het systeem (vooruitlopend: in de autorisatiestructuur krijgt deze applicatie ook een rol). Samenvattend: het risico dat we willen verminderen betreft dat rond elke vorm van geautoriseerde toegang tot dossiers.

Wat zijn de risico's: rechtmatig gebruik versus onrechtmatig gebruik:
We lopen een aantal rollen langs en bekijken het risico dat vanuit die rol onrechtmatige inzage optreedt. Achtereenvolgens kunnen rechten hebben (nadere gradaties zijn mogelijk, rollen zijn gegeven als voorbeeld maar beslaan wel het gehele spectrum):
- de patiënt (rol: patiënt)
- de arts of medewerker (rol: zorgverlener)
- de organisatie/zorgverlener op afstand (rol: externe organisatie)
- een koppeling of exportfunctie (rol: koppeling/export)

De rol patiënt:
- mag alles zien van zijn eigen dossier
- wat bij zijn rol is toegestaan (autorisatieschema)
- op elk moment, hoeft geen extra toestemming te hebben

Ad risico rol patiënt: Lijkt weinig risico, behoudens dat iemand met zijn toegangsmiddelen toegang zoekt. Dus een mantelzorger, een hulpverlener, die een pasje of wachtwoord in handen krijgt en gaat neuzen terwijl de patiënt dat niet wil.

Hulpmiddel: Om dat te kunnen opsporen lijkt een overzicht voor de patiënt afdoende. Hierop ziet hij wie wanneer in zijn dossier is geweest, en onder wiens verantwoordelijkheid.

De rol zorgverlener:
- mag dossier zien wat bij zijn rol is toegestaan (autorisatieschema)
- mits de patiënt dit niet heeft ingeperkt (toestemmingsschema)
- er behandelrelatie bestaat (behandelrelatie)
- en er ook een actie nodig is

daarnaast mag hij ook query's uitvoeren bijvoorbeeld in het kader van preventie, en managementtaken uitvoeren.

Ad risico rol medewerker: Een honderd procent sluitende toegangscontrole die voorkomt dat een medewerker inziet terwijl het niet mag, is niet voorhanden en waarschijnlijk ook niet mogelijk. Voorstelbare scenario's zijn: de nieuwsgierige medewerker, de boze medewerker, de frauduleuze medewerker, de pestende medewerker. Los daarvan is het ook voorstelbaar dat inloggegevens van een medewerker zijn ontfutseld en door een ander worden gebruikt. Ook aan query's kleven risico's: met een gerichte eenmalige query kan een medewerker achterhalen of een patiënt in de selectie voor een bepaald kenmerk valt.

Hulpmiddel: De organisatie zal zelf haar medewerkers willen controleren. Om de ongewenste inzage te kunnen opsporen is een dagelijks overzicht voor de verantwoordelijke nodig. Dit overzicht moet snel inzicht geven in het gedrag, dus per medewerker het aantal raadplegingen binnen en buiten de organisatie inclusief afgewezen pogingen en gebruik van de noodknop. Daarnaast moet er de mogelijkheid zijn een detailoverzicht te maken per medewerker, dat alleen nodig is als steekproefcontrole of bij vermoed misbruik. Het overzicht voor de patiënt dient als extra waarborg, de patiënt kijkt op een andere manier en zal zeker zijn bekenden gemakkelijker signaleren.

De rol organisatie/zorgverlener op afstand:
Hier bedoelen we mee de zorgverlener die vanuit een andere organisatie een dossier of een deel daarvan opvraagt

- mits er een afspraak is tussen de organisaties
- mag de zorgverlener dossier zien wat bij zijn rol en voor die organisatie is toegestaan
- er een behandelrelatie bestaat (behandelrelatie)
- mits de patiënt dit niet heeft ingeperkt (toestemmingsschema)
- en er ook een actie nodig was

Ad risico organisatie/zorgverlener op afstand: Lijkt in opzet niet anders dan hierboven aangegeven voor de medewerker van de eigen organisatie.

Hulpmiddel: Wat is dan nodig om misbruik te kunnen opsporen: ligt die taak bij de vragende organisatie, bij de verstrekkende of bij beide?

- Het is duidelijk dat de *verstrekkend organisatie* maar deels kan controleren of een inzage van buitenaf terecht is. Hij kan controleren of de vragende partij valt onder de lopende afspraken, en hij kan controleren welke inperkingen van de patiënt gelden. Een logregel is daarmee nodig. Verder moet hij kunnen vertrouwen op afspraken die weer moeten waarborgen dat de *vragende zorgaanbieder zelf* een werkende toegangsstructuur heeft en haar medewerkers controleert.
- De *bevragende* zorgaanbieder kan wel alles controleren, maar dat is eigenlijk niet veel anders dan een interne raadpleging. Ook deze partij schrijft een logregel.

De inzage komt dus bij beide organisaties op het overzicht. Bij de vragende organisatie om de medewerker te kunnen controleren, bij de geraadpleegde om te kunnen zien dat het dossier is geraadpleegd door een externe partij. De patiënt kan de raadpleging dubbel terugvinden: zowel bij de organisatie waar zijn dossier is opgevraagd, als bij de partij aan wie de inzage is verleend.

De rol koppeling/export:

- mag dossier zien wat bij zijn rol is toegestaan (de applicatie heeft een eigen rol)
- mits de patiënt dit niet heeft ingeperkt (toestemmingsschema)
- er behandelrelatie bestaat (behandelrelatie) tenzij in geval van geanonimiseerde oplevering ten behoeve van onderzoek en registratie.
- en er ook een actie nodig was

Ad risico rol koppeling/export: Risico is dat een koppeling meer dossiers verstrekt dan nodig en/of vaker dan nodig. Dit risico, dat er onterecht dossiers naar een eigen andere applicatie gaan of zelfs de deur uit, is serieus.
Vanwege dit serieuze risico en vanwege de vereiste transparantie naar de patiënt is het nodig om voor elk dossier dat niet-geanonimiseerd wordt opgenomen in een export een eigen logregel te schrijven.

Om onterechte verstrekking te kunnen opsporen vermeldt het overzicht voor de verantwoordelijke al deze export. Alle niet geanonimiseerde export komt tevens op het overzicht voor de patiënt.

Terug naar het doel: bescherming tegen onbevoegde inzage
Voegen we nu iets toe met de logging van toegang?

Jazeker: De organisatie kan met de overzichten ongewenste toegang door de eigen medewerkers op het spoor komen, houdt zicht op alle exports, en kan aantijgingen van misbruik snel couperen. Dat samen is een enorme winst.

Een andere winst is dat de patiënt zelf kan toezien op inzage. Wellicht stimuleert dat patiënten tot het geven van toestemming van uitwisseling. In het volgende PvE, autorisatie, zullen we de rol patiënt uitwerken. Eerst wellicht in de praktijk / post / apotheek et cetera maar op termijn zou hij ook op afstand moeten kunnen inzien wie zijn dossier raadpleegt.

Een niet te vergeten waarde van de logoverzichten is die voor het finetunen van de autorisatie. Veelvuldig gebruik van de noodknop zal bijvoorbeeld aanleiding zijn om nog eens naar de autorisatiestructuur te kijken.

H-3 Toegangslogging

3.1. Inleiding

Dit hoofdstuk is een handreiking in de vorm van een set van eisen waaraan de toegangslog moet voldoen, om tegemoet te komen aan wettelijke regels, normen en richtlijnen voor toegangslogging.
In de 'toelichting conformiteit' (bijlage 4) is beschreven hoe partijen kunnen voldoen aan de eisen.

3.2. Eisen aan de Toegangslog

1. Elke toegang of poging tot toegang, op elk moment, in elke situatie, tot patiëntgegevens opgeslagen in het Informatiesysteem moet worden vastgelegd in de Toegangslog, daarbij tevens de toegang tot de Toegangslog zelf.

2. Toegang tot gegevens door een medewerker van de zorgaanbieder ten behoeve van administratieve activiteiten, zoals maken van een query, agendabeheer, verwerken van post, behoeven niet specifiek per patiënt te worden gelogd mits er geen inzage in medische gegevens aan te pas komt.

3. Het Informatiesysteem mag niet toegankelijk zijn indien aan eis 1 geen gevolg kan worden gegeven.

4. De Toegangslog is specifiek voor dit doel ingericht en mag niet zijn geïntegreerd met logging voor andere doelen zoals systeembeheer of herstel.

5. De Toegangslog moet volledig zijn afgeschermd van elke mogelijkheid tot wijziging, aanvulling of verminking, inclusief die van systeembeheer. Als in verband met systeemfouten toch regels uit de toegangslog moeten worden geschrapt, worden deze niet verwijderd, maar op inactief worden gezet ('geannuleerd'). Ook dit moet worden gelogd.

6. Een toegangslogregel blijft beschikbaar gedurende een periode van ten minste 2 jaar na het schrijven van de regel en ten hoogste zo lang als de bewaartermijn van de gegevenscategorie waarop de toegangslogregel betrekking heeft. Het verwijderen van toegangslogregels na overschrijden van de bewaartermijn wordt niet gelogd in de toegangslog.

7. De toegangslog moet worden vastgelegd in een gestandaardiseerd formaat dat de volgende velden bevat:

1.1	Toegangslogregel.inzageactie.id
1.2	Toegangslogregel.registratiedatumtijd
1.3	Toegangslogregel.geannuleerd
2.1	Patiëntgegeven.patient.id
2.2	Patiëntgegeven.zorgaanbieder.id
2.3	Patiëntgegeven.dossier.id
2.4	Patiëntgegeven.gegevenscategorie
3.1	Actie.type
3.2	Actie.resultaat
3.3	Actie.beschrijving
5.1	Actor.Zorgaanbieder.id
6.1	Actor.Verantwoordelijke.medewerker.id

6.2	Actor.Verantwoordelijke.medewerker.rol
7A.1 of 7B.1	Actor.Medewerker.id of Actor.Applicatie.id
7A.2 of 7B.2	Actor.Medewerker.rol of Actor.Applicatie.rol
8.1	Geadresseerde organisatie.id
9.1	Controle.autorisatie[1]
9.2	Controle.behandelrelatie[1]
9.3	Controle.toestemming[1]
9.4	Controle.noodknopgebruikt[1]

[1] steeds met verwijzing naar het gehanteerde Protocol
In Bijlage 1 is de uitwerking van deze gegevensset te vinden.

8. Logging vindt plaats op dossierniveau. Dit houdt in dat een toegangslogregel wordt vastgelegd zodra een actie wordt ondernomen in een dossier met patiëntgegevens. Categorieën van patiëntgegevens die worden onderscheiden, zijn:
   - Het 'patiëntendossier' van de patiënt;
   - De 'toegangslog patiënt'
   - Een specifiek onderdeel van het patiëntendossier van de patiënt (dit is afhankelijk van de opbouw en implementatie van het systeem).

   Zie Bijlage 1 tabel 3: gegevenscategorieën.

9. De acties die worden gelogd, zijn:
   - read — Iedere toegang tot patiëntgegevens, ongeacht wat er daarna in of met de patiëntgegevens gedaan wordt. Zodra een dossier met patiëntgegevens wordt geopend, wordt deze actie als een Actie.type 'read' opgeslagen in een toegangslogregel. Ook inzage of raadpleging van buitenaf valt hieronder.
   - export — Zodra een patiëntgegeven elektronisch wordt verzonden naar een andere applicatie, wordt afgedrukt, opgeslagen op een medium dat zich buiten het informatiesysteem bevindt of op andere wijze wordt geëxporteerd, wordt deze actie als een Actie.type 'export' opgeslagen in een toegangslogregel.
   - query — Indien een zoekactie wordt gestart over meerdere patiëntendossiers, wordt deze actie gelogd als Actie.type 'query' in een toegangslogregel.

   Zie ook Bijlage 1 tabel 1.

10. Als meerdere acties worden uitgevoerd door één persoon op één gegevenscategorie, worden hiervoor meerdere logregels geschreven.

11. Het moment van loggen is bij start van de actie en voordat gegevens worden gepresenteerd of geëxporteerd.

12. Ook als een poging tot toegang geweigerd wordt op basis van de controles moet de actie worden gelogd.

13. Bij alle van de volgende situaties wordt een toegangslogregel toegevoegd aan de Toegangslog:

    a. elke poging en/of geslaagde toegang tot elk in het Informatiesysteem opgeslagen patiëntendossier;
       - *Actie.type*: {read;},
       - *Patiëntgegeven.gegevenscategorie*: {patiëntendossier;}

       NB dit houdt in: elke toegang tot het patiëntendossier, ongeacht wat er vervolgens in het dossier aan acties worden uitgevoerd. Zodra een dossier geopend wordt, wordt dit gelogd.
       NB hieronder valt ook inzage in het Informatiesysteem vanuit een andere zorginstelling.
       NB hieronder valt ook inzage door de patiënt

    b. elke 'export' (zoals bedoeld onder 8) van een patiëntendossier of delen daaruit;
       - *Actie.type*: {export;},
       Patiëntgegeven.gegevenscategorie: {patiëntendossier;}

       NB een voorbeeld is een export naar een persoonlijk gezondheidsdossier (PGD).

       In het geval van batchgewijze export, waarbij meerdere (delen van) patiëntendossiers worden geëxporteerd, wordt onderscheid gemaakt tussen geanonimiseerde en niet-geanonimiseerde export:
       - als het bestand niet wordt geanonimiseerd of gepseudonimiseerd, of als dit pas gebeurt na de export, buiten het informatiesysteem, wordt voor ieder Patiëntgegeven.gegevenscategorie een afzonderlijke regel geschreven in de toegangslog.
       - Als het bestand wel binnen het informatiesysteem wordt geanonimiseerd of gepseudonimiseerd, mag worden gelogd per batch. Hierbij wordt gebruik gemaakt van een eigen herkenbare gegevenscategorie (bijv. 'selectie LINH'), waaruit duidelijk wordt naar wie de informatie geëxporteerd is. Het veld patiënt is leeg.

       NB Als de export naar meerdere ontvangers wordt gestuurd, worden deze als afzonderlijke logregels gelogd.
       NB Ook als het bestand wordt geëxporteerd voor facturering of declaratie, wordt gelogd per Patiëntgegeven.gegevenscategorie. Hierbij wordt gebruik gemaakt van een eigen, herkenbare gegevenscategorie (bijv. 'declaratie').

    c. elke poging en/of geslaagde toegang vanuit het Informatiesysteem in patiëntdossiers van andere systemen (applicaties en / of organisaties). Anders gezegd: een medewerker zoekt vanuit het Informatiesysteem toegang tot (een deel van) een dossier dat zich in een ander systeem of bij een andere organisatie bevindt.
       - *Actie.type*: {read;};
       - *Patiëntgegeven.zorgaanbieder.id: {organisatie}*
       - *Patiëntgegeven.gegevenscategorie*: {patiëntendossier;};

    d. elke query op praktijkpopulatieniveau. Anders gezegd: het uitvoeren van een zoekopdracht voor bijvoorbeeld een preventieprogramma waarbij de patiënt wordt geselecteerd.
       - *Actie.type*: {query;};
       - *Patiëntgegeven*: {zoekopdracht;};

       NB De selectie wordt niet vastgelegd op patiëntniveau. Alleen de concrete zoekopdracht wordt gelogd.

e. elke poging en/of geslaagde toegang tot het '*Overzicht inzage in een patiëntendossier*' van de Toegangslog;
   - *Actie.type:* {read;}
   - *Patiëntgegeven.gegevenscategorie*: {toegangslog patiënt}
   -
   NB hieronder valt ook inzage door de patiënt

14. Als een zorgorganisatie overstapt op een ander informatiesysteem en ervoor kiest om de toegangslog mee over te zetten naar het nieuwe informatiesysteem, geldt dit als een actie.type {export;} van de toegangslog uit het oude systeem en als een actie.type {read;} bij import in het nieuwe systeem. Veld patiënt blijft leeg.

3.3. Eisen aan de weergave van de toegangslog

1. Er zijn twee rollen die toegang kunnen krijgen tot de toegangslog:
   - de patiënt
   - de toegangsverantwoordelijke binnen de organisatie.

2. De patiënt heeft toegang tot het 'Overzicht inzage in uw dossier'.

3. Het '*Overzicht inzage in uw dossier*' toont een chronologisch overzicht van wie toegang hebben gekregen tot de patiëntgegevens van de patiënt in het Informatiesysteem. Hierin is te zien:
   a. welke medewerkers van de eigen organisatie toegang hebben gehad tot de gegevens van de patiënt in het Informatiesysteem;
   b. welke medewerkers van de eigen organisatie toegang hebben gehad tot de gegevens van de patiënt bij andere organisaties;
   c. welke organisaties toegang hebben gehad tot de gegevens van de patiënt in het Informatiesysteem;
   d. of de patiënt toegang heeft gehad tot het dossier of de toegangslog van de patiënt in het Informatiesysteem.
   e. wie toegang hebben gehad tot de toegangslog van de patiënt.

   Per inzageactie is te zien wanneer deze heeft plaatsgevonden, door wie (organisatie, persoon, rol, verantwoordelijke), tot welke gegevens deze persoon toegang heeft gehad en welke actie is uitgevoerd.

   Er kan gefilterd worden op de periode waarover de toegangslogregels getoond moeten worden.

   Het is toegestaan om meerdere gelijksoortige regels (waarbij Actor, Patientgegeven en Actie gelijk zijn) die op één dag zijn geregistreerd, op het 'Overzicht inzage in uw dossier' samen te voegen tot één regel met het eerste tijdstip.

4. Alleen de patiënt mag het '*Overzicht inzage in uw dossier*' kunnen inzien.

5. De toegangsverantwoordelijke mag toegang krijgen tot:
   - het '*Dagoverzicht inzage via praktijk'*;
   - het '*Overzicht inzage door een medewerker'*;
   - het '*Overzicht inzage in een patiëntendossier*'.

6. Het '*Dagoverzicht inzage via praktijk*' toont hoeveel inzageacties door interne medewerkers en externe organisaties zijn uitgevoerd.

   Van de inzageacties door interne medewerkers is per persoon te zien welke rol deze persoon heeft, hoeveel verschillende dossiers deze persoon heeft ingezien of geëxporteerd en hoe vaak daarbij de noodknop is gebruikt. Van de inzageacties door externe organisaties is per organisatie te zien hoeveel dossiers met patiëntgegevens vanuit deze organisatie zijn ingezien. Alleen inzageacties met betrekking tot de gegevenscategorie {patiëntendossier;} worden in het dagoverzicht getoond, niet de acties rond de gegevenscategorie {toegangslog patiënt}.

   Er kan gefilterd worden op de periode waarover de acties getoond moeten worden.

7. Het '*Overzicht inzage door een medewerker*' toont een chronologisch overzicht van tot welke patiëntgegevens deze medewerker toegang heeft gehad of andere acties op heeft uitgevoerd.

   Per actie is te zien wanneer deze heeft plaatsgevonden, op welke patiënt het betrekking heeft (naam, BSN), tot welk gegevenscategorie deze persoon toegang heeft gehad, welke actie is uitgevoerd en of daarbij de noodknop is gebruikt. Het overzicht toont ook de rol(len) van de medewerker.

   Er kan gefilterd worden op de periode waarover de acties getoond moeten worden.

   In geval van meerdere gelijksoortige regels (waarbij Actor, Patiëntgegeven en Actie gelijk zijn) op één dag, worden deze allemaal getoond op het 'Overzicht inzage door een medewerker'.

8. Het '*Overzicht inzage in een patiëntendossier*' toont een chronologisch overzicht van wie toegang hebben gekregen tot de patiëntgegevens van de geselecteerde patiënt in het Informatiesysteem. Hierin is te zien:
   a. welke medewerkers van de eigen organisatie toegang hebben gehad tot de gegevens van de patiënt;
   b. welke andere organisaties toegang hebben gehad tot de gegevens van de patiënt in het Informatiesysteem.;
   c. of de patiënt toegang heeft gehad tot de gegevens van de patiënt in het Informatiesysteem.
   d. wie toegang hebben gehad tot de toegangslog van de patiënt.

   Per inzageactie is te zien wanneer deze heeft plaatsgevonden, door wie (organisatie, persoon, rol, verantwoordelijke), tot welk gegevenscategorie deze persoon toegang heeft gehad, welke actie is uitgevoerd en of daarbij de noodknop is gebruikt.

   Er kan gefilterd worden op de periode waarover de acties getoond moeten worden.

   In geval van meerdere gelijksoortige regels (waarbij Actor, Patiëntgegeven en Actie gelijk zijn) op één dag, worden deze allemaal getoond op het 'Overzicht inzage in een patiëntendossier'.

Bijlage 1. Begrippen en gegevensmodel

Begrippen rond toegang

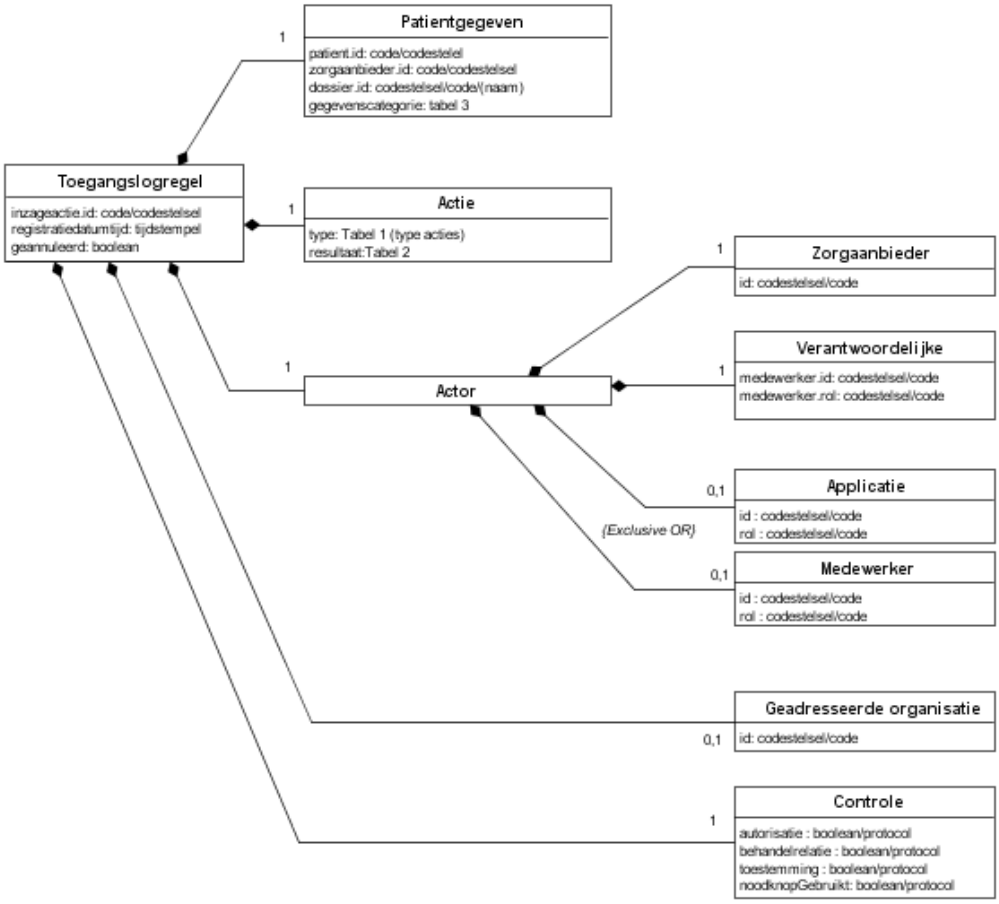
De meeste begrippen zijn beschreven in het gegevensmodel dat hierna volgt. Voor lastigere begrippen wordt hier toegelicht hoe deze in dit document worden gebruikt.

Authenticatie	Zekerstellen dat degene die toegang zoekt ook degene is die hij zegt dat hij is (zie H2.1).
Autorisatie (-protocol, -matrix, -schema, -structuur; zie ook Rol)	Het toekennen aan personen van rechten voor toegang tot gegevens door de verantwoordelijke voor die gegevens. Het autorisatie*protocol* beschrijft het proces van toekennen van rechten tot en met hanteren van deze rechten; autorisatie*matrix*, *-schema* en *structuur* zijn hieraan gerelateerd (zie H2.1). Zie ook *Controle.autorisatie (8.1*) in het gegevensmodel.
Behandelrelatie (-protocol)	De relatie tussen een patiënt en de personen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereen-komst (zoals vastgelegd in de Wet op de geneeskundige behandelingsovereenkomst). Het behandelrelatie*protocol* beschrijft het proces van controleren van de behandelrelatie. Zie ook *Controle.behandelrelatie (8.2)* in het gegevensmodel.
Inzage	zie: Toegang
Noodknop	Een voorziening die inzage mogelijk maakt ondanks negatieve uitkomst van een of meer controles (van autorisatie, behandelrelatie en toestemming). De enige legitieme toepassing van gebruik hiervan is als de autorisatiestructuur kennelijk niet voldoet. Dat de noodknop als functionaliteit wordt genoemd, betekent niet dat het een verplicht aanwezige funtionaliteit is. Zie ook *Controle.noodknopGebruikt (8.4) in het gegevensmodel*.
Rol	Een (verplicht) mechanisme binnen autorisatie om gelijke rechten voor meerdere personen (of applicaties onder hun verantwoordelijkheid) te beheren. NB. In de toegangslog en de overzichten wordt alleen de Primaire Rol vermeld. Zie ook *Verantwoordelijke.medewerker.rol (6.2), Medewerker.medewerker.rol (7A.2), Applicatie.applicatie.rol (7B.2)* in het gegevensmodel.
Systeem (Informatie-)	Het geheel van een of meer systemen die onder de verantwoordelijkheid van één zorgaanbieder vallen en die voor toegang als een geheel worden beschouwd (zie H2.2).
Toegang	Toegang (tot patiëntgegevens) betekent dat een door het systeem gekende gebruiker een al of niet geslaagde poging doet om een patiëntgegeven te raadplegen, wijzigen, aan te vullen dan wel elektronisch te verzenden, printen of op andere wijze te exporteren.
Toegangslog (-regel)	De toegangslog is het geheel van toegangslogregels bij een systeem.

	Een toegangslog*regel* bevat alle informatie over de gevraagde inzage die voldoende wordt geacht om te kunnen nagaan of de toegang rechtmatig of onrechtmatig is geweest. In het gegevensmodel: *Toegangslogregel (1.0)* NB Bij inzage over organisatiegrenzen heen schrijven alle betrokken organisaties een (of meerdere) logregels.
Toestemming (-protocol, schema)	Door de patiënt aangegeven toestemming voor respectievelijk afscherming van (delen van) zijn patiëntendossier. Het toestemmings*protocol* beschrijft de controle van de toestemming. Toestemming*schema* is hieraan gerelateerd (zie H2.1). Zie ook *Controle.toestemming (8.3)* in het gegevensmodel.
Verantwoordelijke (- voor toegang, -voor gegevens, - voor inzage)	I. Elke zorgaanbieder heeft een verantwoordelijke voor de toegang. Deze regelt de rechten en controleert de toegang aan de hand van de overzichten. Deze verantwoordelijke komt in het gegevensmodel niet voor. II. De verantwoordelijke voor een inzage: een persoon kan dat doen op zijn eigen verantwoordelijkheid en rechten, of op verantwoordelijkheid van een ander, waarbij dan voor die inzage de rechten van die persoon van toepassing zijn. In het gegevensmodel: *Verantwoordelijke (6.0)*. III. De verantwoordelijke voor het patiëntgegeven. In het gegevensmodel: *Patiëntgegeven.zorgaanbieder (2.2)*

Gegevensmodel toegangslogregel

NB. Daar waar gesproken wordt over rol (vb. medewerker.rol) is altijd sprake van de Primaire Rol zoals gedefinieerd in Deel 1 Authenticatie en Autorisatie.



Acties die niet patiënt-specifiek zijn

Bepaalde acties zoals het uitvoeren van query's, een backup of het opleveren van registratieinformatie leiden tot het verzamelen van gegevens uit patientendossiers, maar als actie niet gericht op individuele dossiers. De toegangslogregels van acties op groepsniveau verschillen op de volgende punten:

- patiëntspecifieke kenmerken van de toegangslogregel vervallen. Dit is aangegeven met een '[3]'.
- Een extra kenmerk: 'beschrijving' van de Actie is van toepassing

De tabellen hierna beschrijven de klassen van de toegangslogregel en hun kenmerken.

Beschrijving van klassen

	Klasse	beschrijving	toelichting
1.0	Toegangslogregel	Beschrijft wie (de Actor) wanneer een (inzage)Actie heeft uitgevoerd op welk Patiëntgegeven.	
2.0	Patiëntgegeven[1]	Het patiëntgegeven waarop de (inzage)Actie is gedaan.	
3.0	Actie [1]	Duidt de (inzage)Actie die is uitgevoerd met welk resultaat.	Het maakt niet uit of de inzage is gelukt of niet: vanaf het moment dat een medewerker een inzagepoging doet op een specifiek dossier is er sprake van een inzageactie. NB Waar gesproken wordt van actie of inzageactie wordt ook bedoeld export.
4.0	Actor [1]	De Medewerker dan wel de Applicatie van een Zorgaanbieder die onder de verantwoordelijkheid van een Verantwoordelijke medewerker de actie heeft uitgevoerd.	
5.0	Zorgaanbieder [1]	De (zorg)organisatie onder wiens verantwoordelijkheid de Actie is uitgevoerd.	
6.0	Verantwoordelijke [1]	De persoon, werkzaam als zorgverlener bij de Zorgaanbieder, onder wiens eindverantwoordelijkheid de Actie is uitgevoerd.	
7.0A	Medewerker [0..1][1]	De persoon, werkzaam bij de Zorgaanbieder, die de Actie heeft uitgevoerd.	
7.0B	Applicatie [0..1][1]	De Applicatie, horende bij de Zorgaanbieder, die de Actie heeft uitgevoerd.	
8.0	Geadresseerde organisatie [0,1]	De organisatie waarnaar het patiëntgegeven is verstuurd.	Verplicht bij een export naar een andere organisatie.
9.0	Controle [1]	Het geheel van uitgevoerde controles over de rechtmatigheid van de Actie en de resultaten van die controles.	

[1]Ofwel een Medewerker of Applicatie heeft de actie uitgevoerd en wordt in de toegangslogregel vastgelegd.

Toegangslogregel
Toegangslogregel kent de volgende attributen:

	Attribuut	**beschrijving**	**toelichting**	**waarden**
1.1	inzageactie.id [1]	De unieke identificatie van een inzage actie.	Wordt toegekend door de organisatie die de inzageactie start. Indien inzage wordt gevraagd door een andere organisatie, dan wordt de id van de initiator overgenomen.	
1.2	registratiedatumtijd [1]	Het moment waarop de inzage actie werd gestart. *Indien mogelijk dient gesynchroni-seerde tijd gebruikt te worden.*	Dit betreft een tijdstip zo snel mogelijk na het initiatief van de medewerker voor de inzage, maar zeker vóór de daadwerkelijke inzage.	
1.3	geannuleerd [1]	Geeft aan of de toegangslogregel geldig is.	Omwille van audittrail mag een toegangslogregel niet fysiek geschrapt worden. Als blijkt dat de regel ten onrechte is vastgelegd wordt de regel 'geannuleerd'.	TRUE of NIL

Patiëntgegeven
Patiëntgegeven kent de volgende attributen:

	Attribuut	**beschrijving**	**toelichting**	**waarden**
2.1	patiënt.id [1][3]	De unieke identificatie van de patiënt.	Gaat dus om wiens dossier wordt ingezien of verstrekt.	Codestelsel: {BSN}
2.2	zorgaanbieder.id [1][3]	De zorgaanbieder die verantwoordelijk is voor het patiëntgegeven en daarmee ook voor de toegang tot dat gegeven.	Let op: het gaat hier om de zorgaanbieder die *het geraadpleegde dossier onder verantwoordelijkheid heeft* c.q. bewaart of laat bewaren.	Codestelsel: {URA, AGB}
2.3	dossier.id [0..1][3]	Een aanvullende aanduiding van het dossier waarop de inzageactie wordt gedaan.	Om onderscheid te kunnen maken tussen bijvoorbeeld meerdere huisartsenpraktijken en/of apotheken die onder dezelfde zorgaanbieder vallen.	
2.4	Gegevenscategorie [1]			Zie **Tabel 3** NB In fase 3 wordt de tabel verder ingevuld.

Actie
Actie kent de volgende attributen:

	Attribuut	**beschrijving**	**toelichting**	**waarden**
3.1	type [1]	Het type actie	bijvoorbeeld: read, export	Zie **Tabel 1**
3.2	resultaat [1]	Het resultaat van de inzageactie.		Zie **Tabel 2**
3.3	Beschrijving [0][4]	Beschrijving van de query in voor de leek begrijpelijke taal of een verwijzing naar deze beschrijving.		Tekst

Actor
Actor bestaat uitsluitend uit klassen en kent geen eigen attributen.

Zorgaanbieder
Zorgaanbieder kent het volgende attribuut:

	Attribuut	**beschrijving**		
5.1	id [1]	De identificatie van de zorgaanbieder.	Let op: gaat hier om *de zorgaanbieder van de medewerker die de inzage doet*!	Codestelsel: {URA, AGB}

Verantwoordelijke
Verantwoordelijke kent de volgende attributen:

6.1	medewerker.id [1]	De identificatie van de voor de actie verantwoordelijke medewerker		In fase 2 wordt een stelsel afgesproken voor identificatie van medewerkers
6.2	medewerker.rol [1]	De rol van de eindverantwoordelijke medewerker	bijvoorbeeld: huisarts, apotheker	Rol wijst uitsluitend op de primaire rol. In fase 3 wordt een opzet voor rollen afgesproken

Medewerker
Medewerker kent de volgende attributen:

7A.1	id [1]	De identificatie van de medewerker die de actie uitvoert.		In fase 2 wordt een stelsel afgesproken voor identificatie van medewerkers
7A.2	rol [1]	De rol van de medewerker.	bijvoorbeeld: assistente, huisarts, apotheker	Rol wijst uitsluitend op de primaire rol. In fase 3 wordt een opzet voor rollen afgesproken

Applicatie
Applicatie kent de volgende attributen:

7B.1	id [1]	De identificatie van de applicatie die de actie uitvoert.		In fase 2 wordt een stelsel afgesproken voor identificatie van applicaties
7B.2	rol [1]	De rol (in termen van autorisatie) van de applicatie.		Rol wijst uitsluitend op de primaire rol. In fase 3 wordt een opzet voor rollen afgesproken

Geadresseerde organisatie
Geadresseerde organisatie kent het volgende attribuut:

8.1	id [1]	De identificatie van de organisatie waarnaar het patiëntgegevens is verstuurd. Verplicht bij export naar een andere organisatie.	Bijvoorbeeld: een zorgorganisatie, een verzekeraar, LINH.	Codestelsel: {URA, AGB} Mogelijk alternatief volgt in fase 2.

Controle
Controle kent de volgende attributen:

	attribuut	**beschrijving**		
9.1	autorisatie [1][2]	De uitkomst van de controle van de autorisatie: is deze Medewerker of Applicatie met de Verantwoordelijke geautoriseerd voor de gevraagde actie uitvoeren op het Patiëntgegeven?	Anders gezegd: *wat is de rol* van de medewerker en/of van de verantwoordelijke, *en mag die rol* de gevraagde actie doen.	Uitkomst: boolean In fase 3 wordt afgesproken hoe wordt verwezen naar het gehanteerde autorisatieprotocol.
9.2	behandelrelatie [1][2,3]	De uitkomst van het behandelrelatieprotocol: is er sprake van een (in het systeem bekende) behandelrelatie tussen medewerker en/of verantwoordelijke met de patiënt.	Anders gezegd: is er een *behandelrelatie* tussen enerzijds de *medewerker en/of de verantwoordelijke* en anderzijds de *patiënt* waarbij inzage wordt gevraagd.	Uitkomst: boolean In fase 3 wordt afgesproken hoe wordt verwezen naar het gehanteerde protocol voor controle van de behandelrelatie.

9.3	toestemming [1][2,3]	De uitkomst van het toestemmingsprotocol: Heeft de zorgaanbieder een opt-in, die niet is weerlegd door de patiënt voor deze medewerker en/of verantwoordelijke.	Anders gezegd: *mag de inzage ook van de patiënt*?	Uitkomst: boolean In fase 3 wordt afgesproken hoe wordt verwezen naar het gehanteerde protocol voor controle van de toestemming.
9.4	noodknopGebruikt [1][2,3]	De uitkomst van het noodknopprotocol: De uitkomst van het gebruik van de noodknop.	In sommige situaties kan het nodig zijn een voorziening te ondersteunen die inzage mogelijk maakt terwijl de controles (8.1 tot 8.3) een of meerdere nee's opleveren. Dat wordt hier vastgelegd.	Uitkomst: boolean

Noot 2: steeds met verwijzing naar het gehanteerde Protocol
Noot 3: NIET van toepassing bij een logregel op groepsniveau zoals een query of backup
Noot 4: Verplicht en alleen van toepassing bij een logregel op groepsniveau

Tabellen

Tabel 1: Type actie

1	read	Er zijn twee mogelijke betekenissen: 1. De Actor wil het Patiëntgegeven inzien; 2. De Actor (van buitenaf) wil het Patiëntgegeven raadplegen.
2	export	De Actor wil het Patiëntgegeven elektronisch verzenden, printen of op andere wijze exporteren.
3	Query	De Actor voert een query uit over meerdere patiëntendossiers.

Tabel 2: Het resultaat van de (inzage)Actie

1	success	1. De Actor heeft het Patiëntgegeven ingezien 2. Het Patiëntgegeven is aan de Actor opgeleverd. 3. Het patiëntgegeven is verzonden, geprint of op andere wijze geëxporteerd.
2	refused	De actie is geweigerd.
3	error	Er vindt een foutmelding plaats.

Tabel 3: Gegevenscategorieën

1	patiëntendossier	Het gehele patiëntendossier (een nadere detaillering van welke gegevens zijn ingezien wordt niet gegeven)
2	toegangslog patiënt	
Suggesties voor aanvulling gegevenscategorieën op organisatieniveau		
3	Backup	De gegevensset voor externe back-up
4	NIVEL	De gegevensset van NIVEL
5	<Standaardquery A>	Bijvoorbeeld Griepprik selectie
6	<Standaardquery B>	Bijvoorbeeld cervix screening selectie

NB. Hier mag voorlopig een eigen aanvulling op de tabel worden gemaakt, deze wordt herkenbaar gemaakt als lokale variant, bijvoorbeeld met een voorloopletter.

Bijlage 2. Voorbeelden van de toegangslog

Toelichting

Deze bijlage geeft een uitgebreid overzicht van situaties waarin inzage aan de orde is en de mogelijke bijbehorende logregel. We doen dat in de vorm van use-case. In deze use-cases tonen we voorbeelden van hoe de toegangslog eruit ziet in de genoemde situaties. We maken daarbij onderscheid tussen het loggen van toegang op individueel niveau, en bij toegang op bestandsniveau.

Loggen bij toegang op individueel niveau

Voor de motivatie van het loggen op individueel niveau verwijzen we naar hoofdstuk 2. De use-cases 1 t/m 13 zijn voorbeelden van loggen bij toegang op individueel niveau.

Loggen bij toegang op bestandniveau

Bij toegang tot patiëntdossiers via acties op het gehele patiëntenbestand kan men in een aantal situaties volstaan met het vastleggen in het logbestand van de groepsactie. Het gaat om: Back-up, selectie voor geanonimiseerde of gepseudonimiseerde export, en query's. Het maakt daarbij niet uit of de acties zijn geïnitieerd door medewerkers of door geroosterde applicaties.
Hoewel de toegang uiteindelijk individuele patiëntdossiers betreft, lijkt het voor de patiënt in kwestie niet nodig c.q. niet wenselijk om de toegang te kunnen terugvinden. De logregel op bestandniveau is dan uitsluitend bedoeld om de rechtmatigheid van acties door de medewerkers te kunnen beoordelen en afwijkingen gemakkelijk op het spoor te komen.

- bij **back-up**: het spreekt voor zich dat bestanden veilig gesteld moeten worden voor eventualiteiten. Back-ups maken kan op vele manieren, van het stelselmatig trekken van een kopie tot continu spiegelen, zolang de gegevens binnen hetzelfde systeem blijven hoeft dit niet te worden gelogd. Als de gegevens het systeem verlaten neemt het risico van ongewenste inzage toe en moet een logregel worden geschreven per back-up actie. *NB als de gegevens het systeem niet-versleuteld verlaten wordt dit gezien als een verzameling van individuele exports, en wordt dus wel een regel geschreven per dossier!*
- bij **geanonimiseerde of gepseudonimiseerde output**: denk aan regionale of landelijke dataverzameling voor onderzoek. Als de gegevens het systeem verlaten moet een logregel worden geschreven per exportactie. Het risico dat hier bestaat is dat - omdat deze processen op de achtergrond draaien - de praktijkhouder het zicht op het totaal van exports kwijtraakt.
- bij **query's**: in de praktijk zullen vaak patiënten worden geselecteerd voor doelen van preventie et cetera. Het maken van de juiste selectie is soms weinig ambigu door afgesproken selectiecriteria, en er komt één logregel. Echter in sommige gevallen zal de selectie door trial and error worden verkregen. In dat geval moet steeds een logregel worden geschreven. Het risico dat hier bestaat is dat een medewerker via een gerichte zoekactie (bijv. Hiv-positieve labuitslag + mannen 40-50) vrij gemakkelijk privacygevoelige zaken van een kennis kan achterhalen. Met de logregels zal zo'n actie niet gemakkelijk onopgemerkt blijven.

De use-cases 14, 15 en 16 hebben betrekking op loggen bij toegang op bestandsniveau. Let op: in bijlage 1 is door middel van voetnoten aangegeven welke delen van het gegevensmodel in deze situatie van toepassing zijn.

identificatie logregel			patiëntdossier/gegeven				actie			zorgaanb	verantwoordelijke		medewerker/ applicatie		geadres seerde	controles			
1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
inzage.id.	datumtijd	geannul.	patientid	z.aanb.id	dossierid	geg.categ.	type	resultaat	beschrijving	id	mw.id	mw.rol	mw.id/ appl.id	mw.rol/ appl.rol	org.id	controle autorisatie	controle behandelrel	controle toestemming	gebruik noodknop
Logregel-id logt dat op **tijdstip**			van **patiënt** bij **org** in **deelsysteem** het **volledige dossier**				is **ingezien** (met **succes**)			onder verantw van **org**	en onder verantw van **mw** zijnde **arts**		door **mw/appl** zjinde **ass/**		evt: aan **org**	controles vooraf leverden op autorisatie **TRUE,** behandelrelatie **TRUE,** toestemming **TRUE,** noodknop **FALSE**			

use case 1 - enkelvoudige inzage bij eigen organisatie

Doktersassistente **mwaa** van huisartspraktijk **orgA** leest onder verantwoordelijkheid van huisarts **artsA** de **alg. gegevens** in het eigen **hisA** in van de eigen patient **pat.**

In praktijk **orgA** leidt dit tot de volgende logregel:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.1	201...	FALSE	patA	orgA	hisA	pat.dossier[1]	R	read	-	orgA	artsA	ha	mwaa	ass	-	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

TOELICHTING use case 1:

A00.1 logt dat op **20141105;140012**	van **patA** bij **orgA** in **hisA** het **patiënten dossier** is	**ingezien**	onder verantw van **orgA**	en onder verantw van **artsA** zijnde **arts**	door **mwaa** zjinde **ass**	-	controles vooraf leverden op autorisatie **TRUE,** behandelrelatie **TRUE,** toestemming **TRUE,** noodknop **FALSE**

1in de voorbeelden is nog niet opgenomen dat van een 'patiëntendossier' een specifiek deel kan zijn ingezien, vandaar dat in de voorbeelden wordt gesproken van 'patientendossier' (naast 'toegangslog patiënt')

use case 2 - enkelvoudige inzage bij eigen organisatie

Vervolgens leest zij de **medicatiegegevens** in het eigen **hisA**.

In praktijk **orgA** leidt dit niet tot een logregel omdat de praktijk geen onderscheid maakt in gegevenscategorie.

use case 3 - enkelvoudige inzage bij andere organisatie

Vervolgens haalt zij via haar HIS bij apotheek **orgB** in **aisB** op de **verstrekkinggegevens**.

In huisartspraktijk **orgA** leidt dit tot de volgende logregel:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.2	201...	FALSE	patA	orgB	aisB	pat.dossier[1]	R	read	-	orgA	artsA	ha	mwaa	ass	-	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

In apotheek **orgB** leidt dit tot de volgende logregel:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.2	201...	FALSE	patA	orgB	aisB	pat.dossier[1]	R	read	-	orgA	orgA	ha-pr	orgA	ha-pr	-	oid-a/TRUE	-	oid-t/TRUE	-

TOELICHTING use case 3:

OrgA: geef inzage-id mee bij inzage, orgB: neem dat over.	OrgA: Inzage is altijd voorgeprogrammeerd, leg bij ontwerp van de inzage bij orgB vast met welke waarden je de rubrieken vult.		orgA: het gaat hier om de eigen medewerker; orgB: het gaat hier om de organisatie die de inzage vraagt, de rol is huisartspraktijk!		orgB: controles vinden plaats of orgA is geautoriseerd, en of de toestemming akkoord is. Geen controle behandelrelatie.

use case 4 - verwijsbrief

Arts **artsA** van huisartspraktijk **orgA** stuurt voor patient **patA** een verwijsbrief naar artsB in ketenorganisatie **orgC,** en drukt de brief af voor de patA.

In praktijk **orgA** leidt dit tot de volgende logregel:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.4	201...	FALSE	patA	orgA	hisA	pat.dossier[1]	E	exported		orgA	artsA	ha	artsA	ha	orgC	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
A00.5	201...	FALSE	patA	orgA	hisA	pat.dossier[1]	E	exported		orgA	artsA	ha	artsA	ha	patA	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

Ontvangst zonder integratie in een dossier en zonder inzage leidt niet tot een logregel bij orgC.

De verwijsbrief wordt in **orgC** in het systeem **kisA** geintegreerd door de secretaresse **mwbb** van **artsB**

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.4	201...	FALSE	patA	orgC	kisA	pat.dossier[1]	R	read	-	orgC	artsB	internist	mwbb	secr	-	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

TOELICHTING use case 5:

Bij een Export neemt de ontvangende organisatie id over.							E staat voor export gezien vanuit orgA; in orgB is het een R.								orgC is de geadres-seerde				

use case 5 - geautomatiseerde meervoudige read bij andere organisatie

Applicatie **appA** (verantwoordelijke: **artsC**) van huisartspraktijk **orgA** haalt (voor het spreekuur) op **verstrekkinggegevens** van **patA** en **patB** in het **aisB** bij apotheek **orgB.**

In huisartspraktijk **orgA** leidt dit tot de volgende logregels:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.5	201...	FALSE	patA	orgB	aisB	pat.dossier[1]	R	read	-	orgA	artsC	ha	appA	app	-	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
A00.6	201...	FALSE	patB	orgB	aisB	pat.dossier[1]	R	read	-	orgA	artsC	ha	appA	app	-	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

In apotheek **orgB** leidt dit tot de volgende logregels:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.5	201...	FALSE	patA	orgB	aisB	pat.dossier[1]	R	read	-	orgA	-	-	-	-	-	oid-a/TRUE	-	oid-t/TRUE	-
A00.6	201...	FALSE	patB	orgB	aisB	pat.dossier[1]	R	read	-	orgA	-	-	-	-	-	oid-a/TRUE	-	oid-t/TRUE	-

TOELICHTING use case 6:

											hier niet een medewerker die de inzage initieert maar een applicatie								

use case 6 - aanmelding bij LSP

Applicatie **appA** (verantwoordelijke: **artsC**) van huisartspraktijk **orgA** verstuurt aan LSP **orgC** dat **gegevens** beschikbaar zijn van **patA**

In praktijk **orgA** leidt dit tot de volgende logregel:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.4	201...	FALSE	patA	orgA	hisA	med.dossier[1]	E	exported	-	orgA	artsC	ha	appA	app	orgC	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

In LSP **orgC** leidt dit niet noodzakelijk tot een logregel, omdat de gegevens niet worden ingezien.

use case 7 - visite-uitdraai

Doktersassistente **mwaa** van huisartspraktijk **orgA** maakt in opdracht voor huisarts **artsA** een **visite-uitdraai** voor **patA, patB, patC en patD**

In praktijk **orgA** leidt dit tot de volgende logregel:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.9	201...	FALSE	patA	orgA	hisA	pat.dossier[1]	E	exported	-	orgA	artsA	ha	mwaa	ass	orgA	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
A00.0	201...	FALSE	patB	orgA	hisA	pat.dossier[1]	E	exported	-	orgA	artsA	ha	mwaa	ass	orgA	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
A00.1	201...	FALSE	patC	orgA	hisA	pat.dossier[1]	E	exported	-	orgA	artsA	ha	mwaa	ass	orgA	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
A00.2	201...	FALSE	patD	orgA	hisA	pat.dossier[1]	E	exported	-	orgA	artsA	ha	mwaa	ass	orgA	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

TOELICHTING use case 8:

							de visiteuitdraai wordt geprint, E staat daarbij voor export												

use case 8 - inzage logging door patiënt

Patient **patA** van huisartspraktijk **orgA** ziet via een patientportaal of in het HIS zelf zijn eigen dossier in van de huisartspraktijk, en vervolgens de logging.

In praktijk **orgA** leidt dit tot de volgende logregel:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.2	201...	FALSE	patA	orgA	hisA	pat.dossier[1]	R	read		orgA	patA	patient	patA	patient	-	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
A00.3	201...	FALSE	patA	orgA	hisA	logging	R	read		orgA	patA	patient	patA	patient	-	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

TOELICHTING use case 9:

											de patiënt is zowel de verantwoordelijke als degene die de inzage doet								

use case - 9 assistentie op afstand door helpdesk

Helpdeskmedewerker **helpA** van leverancier **levE** helpt huisarts **artsA** huisartspraktijk **orgA** aan de aan de hand van dossier van patA, echter alle persoonlijke velden zijn netjes onleesbaar gemaakt. Er hoeft geen logregel te worden geschreven bij de organisatie van de helpdesk.

In praktijk **orgA** leidt dit tot de volgende logregel:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.2	201...	FALSE	patA	orgA	hisA	pat.dossier[1]	R	read	-	orgA	artsA	ha	artsA	ha	-	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

use case 10 - export facturen en declaraties

Assistente **mwaa** van praktijk **orgA** maakt facturen aan, voor **patA** en **patD** betreft het een factuur, voor **patC** en **patD** declaraties naar verzekeraar **orgV** en **orgW**:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.1	201...	FALSE	patA	orgA	hisA	pat.dossier[1]	E	exported	-	orgA	artsA	ha	mwaa	ass	patA	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
A00.2	201...	FALSE	patB	orgA	hisA	pat.dossier[1]	E	exported	-	orgA	artsA	ha	mwaa	ass	orgV	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
A00.3	201...	FALSE	patC	orgA	hisA	pat.dossier[1]	E	exported	-	orgA	artsA	ha	mwaa	ass	orgW	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
A00.4	201...	FALSE	patD	orgA	hisA	pat.dossier[1]	E	exported	-	orgA	artsA	ha	mwaa	ass	patD	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

TOELICHTING use case 11:

factureren kan niet anoniem, dus een regel per factuur																			

use case 11 - export baxteropdracht

Applicatie appB (verantwoordelijke: apoD) van apotheek orgB stuurt naar bedrijf apoF baxteropdrachten voor patA en patB. Productiemedewerker mwcc onder verantw van direkteur mwdd van apoF retourneert vanuit systeem baxA baxters met naamstickers.

In apotheek **orgB** leidt dit tot de volgende logregels:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
B00.4	201...	FALSE	patA	orgB	aisA	pat.dossier[1]	E	exported	-	orgB	apoD	apo	appB	app	apoF	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
B00.5	201...	FALSE	patB	orgB	aisA	pat.dossier[1]	E	exported	-	orgB	apoD	apo	appB	app	apoF	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

Bij baxteraar apoF leidt dit tot de volgende logregels bij inlezen respectievelijk bij aanmaken baxter:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
B00.4	201...	FALSE	patA	apoF	baxA	pat.dossier[1]	R	read	-	apoF	mwdd	dir	mwcc	prod	-	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
B00.5	201...	FALSE	patB	apoF	baxA	pat.dossier[1]	R	read	-	apoF	mwdd	dir	mwcc	prod	-	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
F00.1	201...	FALSE	patA	apoF	baxA	pat.dossier[1]	E	exported	-	apoF	mwdd	dir	mwcc	prod	orgB	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE
F00.2	201...	FALSE	patB	apoF	baxA	pat.dossier[1]	E	exported	-	apoF	mwdd	dir	mwcc	prod	orgB	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

TOELICHTING use case 13:

per opdracht een read (id van orgB) en een print (id van apoF)						toestemming moet zijn geregeld via apotheek, behandelrelatie moet zijn geregeld door apotheek

use case 12 - inzage mislukt want er is geen behandelrelatie

Doktersassistente **mwaa** van huisartspraktijk **orgA** wil onder verantwoordelijkheid van huisarts **artsA** de **alg. gegevens** in het eigen **hisA** in van een patient **patA** lezen die toestemming daarvoor niet heeft gegeven.

In praktijk **orgA** leidt dit tot de volgende logregel:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.2	201...	FALSE	patA	orgA	hisA	pat.dossier[1]	R	read		orgA	artsA	ha	mwaa	ass		oid-a/TRUE	oid-b/TRUE	oid-t/FALSE	FALSE

use case 13 - inzage zonder toestemming met de noodknop

Arts **artsA** van huisartspraktijk **orgA** wil een dossier inzien van een patiënt van zijn collega die hem niet heeft ingesloten. Hij gebruikt de **noodknop.**

In praktijk **orgA** leidt dit tot de volgende logregel:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.2	201...	FALSE	patA	orgA	hisA	pat.dossier[1]	R	read		orgA	artsA	ha	artsA	ha		oid-a/TRUE	oid-b/FALSE	oid-t/TRUE	TRUE

use case 14 - export LINH

Applicatie **appA** (verantwoordelijke: **artsC**) van huisartspraktijk **orgA** exporteert wekelijks naar **LINH,** in het praktijksysteem vindt al pseudonimisering plaats.

In huisartspraktijk **orgA** leidt dit tot de volgende logregels:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.2	201...	FALSE		orgA	hisA	batchlinH	E	exported	-	orgA	artsC	ha	appA	app	LINH	oid-a/TRUE	oid-b/TRUE	oid-t/TRUE	FALSE

TOELICHTING use case 12:

één record voor een heel bestand omdat pseudonimisering al in het praktijksysteem plaatsvindt			2.1 patientid is niet van toepassing; 2.4 batchLINH verduidelijkt om welke logische selectie het gaat;				3.3 dient een beschrijving van de actie te bevatten met eventueel een verwijzing naar de specifieke actie.											

use case 15 - back-up

Applicatie **appC** (verantwoordelijke: **artsC**) van huisartspraktijk **orgA** maakt dagelijks een backup.

In huisartspraktijk **orgA** leidt dit tot de volgende logregels:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.2	201...	FALSE		orgA	hisA	back-up	E	exported	-	orgA	artsC	ha	appC	app	orgA	-	-	-	-

TOELICHTING use case 14:

één record voor een heel bestand back-up is uitzondering omdat 1)wordt niet gelezen 2) blijft binnen het logisch systeem			2.1 patientid is niet van toepassing; 2.4 back-up verduidelijkt dat het om een back-up gaat;				3.3 dient een beschrijving van de actie te bevatten met eventueel een verwijzing naar de specifieke actie.				NB waar de back-up plaatsvindt maakt niet uit, gebeurt onder verantwoordelijkheid van artsC.				geen controles aan de orde			

use case 16 - zoekopdracht

Arts **artsA** van huisartspraktijk **orgA** maakt een overzicht van patienten die voldoen aan bepaalde selectiecriteria. Hij vergist zich en maakt een nieuwe query.

In praktijk **orgA** leidt dit tot de volgende logregels:

1.1	1.2	1.3	2.1	2.2	2.3	2.4	3.1	3.2	3.3	5.1	6.1	6.2	7.1	7.2	8.1	9.1	9.2	9.3	9.4
A00.2	201...	FALSE		orgA	hisA	query	R	TRUE	-	orgA	artsA	ha	artsA	ha	orgA	oid-b/TRUE	oid-b/TRUE	oid-b/TRUE	FALSE
A00.3	201...	FALSE		orgA	hisA	query	R	TRUE	-	orgA	artsA	ha	artsA	ha	orgA	oid-b/TRUE	oid-b/TRUE	oid-b/TRUE	FALSE
A00.4	201...	FALSE		orgA	hisA	query	R	TRUE	-	orgA	artsA	ha	artsA	ha	orgA	oid-b/TRUE	oid-b/TRUE	oid-b/TRUE	FALSE

TOELICHTING use case 17:

			2.1 patientid is niet van toepassing; 2.4 query verduidelijkt dat het om een query gaat;				3.3 dient een beschrijving van de actie te bevatten met eventueel een verwijzing naar de specifieke actie.											

Bijlage 3. Voorbeelden van overzichten

Deze bijlage bespreekt hoe de toegangslog in vier overzichten getoond worden aan de patiënt en de toegangsverantwoordelijke. De overzichten zijn:

Overzicht voor de patiënt:
- Overzicht inzage in uw dossier

Overzichten voor de toegangsverantwoordelijke:
- Dagoverzicht inzage via praktijk
- Overzicht inzage door een medewerker
- Overzicht inzage in een patiëntendossier

We bespreken deze overzichten aan de hand van een fictief scenario:

> *De heer Dekker belt 12 februari 2014 de Huisartsenpost van Groningen. Hij heeft een zeer pijnlijke en mogelijk gebroken teen. Hij bespreekt dit telefonisch met de doktersassistente van de post, mevrouw C. van Dijk, die voor hem een afspraak met de huisarts op de post, dokter Pietersen, maakt. Na aankomst haalt dokter Pietersen de professionele samenvatting op bij de eigen huisarts van de heer Dekker, dokter Hiemstra. De doktersassistente stuurt na het contact de waarneemgegevens naar de vaste huisarts.*

Dit levert 4x een inzageactie op, zie verderop.

Overzicht inzage in uw dossier

Scenario

Het scenario krijgt de volgende wending:

> *De heer Dekker krijgt de indruk dat een bekende van hem, mevrouw Haagsma, medische informatie over hem weet en lekt. Mevrouw Haagsma is een doktersassistente die in de week voor en na zijn bezoek aan de huisartsenpost invalskracht was op de huisartsenpost. Om na te gaan of zij zijn dossier heeft ingezien wil de heer Dekker zijn toegangslog inzien. 21 maart bezoekt hij hiervoor de huisartsenpost.*

Uitleg over het overzicht

De huisartsenpost geeft hem een folder met toelichting over de toegangslog:

> Het overzicht laat zien wie via onze praktijk inzage hebben gehad in uw elektronisch dossier. Dit zijn medewerkers van de huisartsenpost of medewerkers van een andere zorginstelling die op elektronische wijze uw dossier bij de huisartsenpost hebben ingezien.
> Inzage is toegestaan voor zorgverleners die bij uw behandeling betrokken zijn en voor medewerkers die nazorg doen op uw dossier. Ziet u vreemde zaken lees dan eerst de veelgestelde vragen.

Presentatie 'overzicht inzage in uw dossier'

Alleen de patiënt mag het volledige overzicht inzien. Daarom logt hij in met zijn persoonsgegevens. Vervolgens geeft hij de periode aan waarover hij de toegangslog wil inzien: van 1 februari 2014 tot en met 21 maart 2014. Hij ziet het volgende overzicht:

Huisartsenpost Groningen — Gemaakt op 21-03-2014; 12:30:02
Overzicht inzage in uw dossier van 01-02-2014 tot en met 21-03-2014
P. Dekker, BSN 123456789

Datum	Wie				dossier	actie
	organisatie	persoon	rol	verantwoordelijke		
21-03-2014 12:30		P. Dekker	Patiënt		toegangslog HAP Groningen	ingezien
12-02-2014 21:53	Huisartsenpost Groningen	C. van Dijk	doktersassistente	I. Janssen, huisarts	HAP-dossier Groningen	geëxporteerd
12-02-2014 21:34	Huisartsenpost Groningen	J. Pietersen	Waarnemend Huisarts	J. Pietersen, huisarts	Huisartsdossier Hiemstra	ingezien
12-02-2014 21:33	Huisartsenpost Groningen	J. Pietersen	Waarnemend huisarts	J. Pietersen, huisarts	HAP-dossier Groningen	ingezien
12-02-2014 21:23	Huisartsenpost Groningen	C. van Dijk	doktersassistente	I. Janssen, huisarts	HAP-dossier Groningen	ingezien

Het overzicht laat zien wie wanneer welk dossier van de patiënt heeft ingezien. In het voorbeeld zijn er drie dossiers ingezien: het 'HAP-dossier Groningen', 'huisartsdossier Hiemstra' waarvan de gegevens zijn opgehaald en de 'toegangslog HAP Groningen' die op dit moment ingezien wordt. De toegangslog is dus een separaat gegevenscategorie.

De inzage van de toegangslog door de patiënt is ook gelogd. Zo kan de patiënt nagaan of iemand onder zijn naam de toegangslog heeft ingezien.

Veelgestelde vragen

De patiënt stelt de volgende veelgestelde vraag:

> **Wat betekent 'actie'?**
> De actie geeft aan of een dossier is 'ingezien' of 'geëxporteerd'.
> - 'Ingezien': de medewerker heeft het dossier gelezen of bewerkt.

- 'Geëxporteerd': de medewerker heeft gegevens afgedrukt, gekopieerd of verstuurd. De waarneemgegevens worden bijvoorbeeld naar de vaste huisarts verzonden. Een ander voorbeeld is het afdrukken of elektronisch versturen van een recept naar de apotheker.

Dagoverzicht inzage via praktijk

Het 'dagoverzicht inzage via praktijk' toont onder andere hoeveel dossiers door interne en externe personen zijn ingezien.

De toegangsverantwoordelijke ziet geregeld het 'dagoverzicht inzage via praktijk' in. Het is een vertrekpunt om verdachte patronen te kunnen herkennen. Vervolgens kan er op een ingezoomd worden op een medewerker / raadpleger.

> *Huisarts Hiemstra is de toegangsverantwoordelijke van zijn praktijk. Hij heeft een huisarts in dienst, en een doktersassistent. Dat is deze week, I. Haagsma, een invalskracht. Huisarts Hiemstra bekijkt iedere ochtend het 'dagoverzicht inzage via de praktijk' van de vorige dag in.*

Dagoverzicht inzage via de huisartsenpraktijk Hiemstra

De toegangverantwoordelijke 'Hiemstra' ziet het volgende overzicht:

Dagoverzicht inzage via de praktijk **Periode: 12 maart 2014; 0:00 tot 23:59**						**13 maart 2014**
Wie			**Aantal**			**noodknop**
Persoon	**Organisatie**	**Rol**	**ingezien**	**geëxporteerd**	**geraadpleegd**	
I. Haagsma		doktersassistente	60	7	0	0
L. Hiemstra		Huisarts	30	12	16	0
P. Overbeek		Huisarts	28	15	20	1
A. Verschie	Huisartsenpraktijk A	Huisarts	30	n.v.t.	n.v.t.	n.v.t.
B. Toren	Huisartsenpraktijk B	Huisarts	4	n.v.t.	n.v.t.	n.v.t.
C. de Bie	Huisartsenpraktijk C	Huisarts	1	n.v.t.	n.v.t.	n.v.t.
D. Kuijt	Huisartsenpraktijk D	Huisarts	1	n.v.t.	n.v.t.	n.v.t.
A. Groen	Apotheek A	Apotheker	1	n.v.t.	n.v.t.	n.v.t.
B. de Groot	Apotheek B	Apotheker	1	n.v.t.	n.v.t.	n.v.t.
C. Hoop	Apotheek C	Apotheker	1	n.v.t.	n.v.t.	n.v.t.

Wat betekenen de kolommen?

- De 'persoon' kan een medewerker zijn van de praktijk of een medewerker van een andere organisatie die het dossier van de huisarts raadpleegt. In geval van een externe organisatie wordt hier de verantwoordelijke getoond.
- De 'rol' geeft de rol weer die de medewerker heeft tijdens het inzien. Wanneer de medewerker twee rollen heeft gedurende de dag komt de medewerker twee maal terug in het overzicht.
- Het 'aantal ingezien' geeft aan hoeveel (unieke) dossiers zijn ingezien door de persoon.
- Het 'aantal geëxporteerd' geeft aan hoe vaak een medewerker medische informatie uit een patiëntendossier heeft geprint, verstuurd of gekopieerd.
- Het 'aantal geraadpleegd' is het aantal dossiers bij andere organisaties die zijn ingezien door de persoon.

- De ‘noodknop’ geeft aan hoe vaak de noodknop is gebruikt. De heer Overbeek heeft een patiënt gezien die zich al had laten uitschrijven naar een andere praktijk. Om toch toegang te krijgen tot het dossier heeft hij de noodknop gebruikt.

Overzicht inzage door een medewerker

Hiemstra wil zien welke dossiers de waarnemend doktersassistente heeft ingezien. Hij selecteert de kolom en opent haar ‘overzicht inzage door een medewerker’. Hij ziet het volgende overzicht:

Overzicht inzage I. Haagsma, doktersassistente.
Verantwoordelijke: L. Hiemstra
Periode: 12 maart 2014

Datum	Patiënt		Wat	Actie	nood knop
	naam	BSN			
12-03-2014 9:51	A. van Dommelen	418238844	huisartsdossier Hiemstra	ingezien	
12-03-2014 9:40	P. Siemens	234215453	huisartsdossier Hiemstra	ingezien	
12-03-2014 9:25	I. Jongelen	231848293	huisartsdossier Hiemstra	geëxporteerd	
12-02-2014 9:05	V. Maarsse	823123828	huisartsdossier Hiemstra	ingezien	
12-03-2014 9:00	P. Dekker	123456789	huisartsdossier Hiemstra	ingezien	
12-03-2014 8:31	S. Dommelen	457483894	huisartsdossier Hiemstra	geëxporteerd	
12-03-2014 8:20	I. Jongelen	231848293	huisartsdossier Hiemstra	ingezien	
12-03-2014 8:13	P. Dekker	123456789	huisartsdossier Hiemstra	ingezien	
12-03-2014 8:01	A. Piek	418238844	huisartsdossier Hiemstra	ingezien	

Scenario

Terugkijkend naar het dagoverzicht vindt Hiemstra de grote hoeveelheid externen die zijn huisarsteninformatiesysteem inzien vreemd; zoveel zijn het er meestal niet.
*Hij wil weten welke dossiers zijn ingezien door de externen. Hij selecteert de eerste ‘***’.*

Overzicht inzage door een persoon

Hij ziet het volgende overzicht:

Overzicht inzage *.**
Periode: 12 maart 2014

Datum	Patiënt		Wat	Actie	nood knop
	naam	BSN			
12-03-2014 9:51	A. Piek	418238844	Huisartsdossier Hiemstra	ingezien	n.v.t.

Hij selecteert het patiëntendossier van A. Piek en opent het ‘Overzicht inzage in een patiëntendossier’

Overzicht inzage in een patiëntendossier

Toegangsverantwoordelijke Hiemstra ziet het volgende overzicht:

Overzicht inzage in patiëntendossier A.Piek, BSN 418238844					Gemaakt op 13-03-2014;	
Huisartsenpraktijk Hiemstra					10:00:00	
Periode: 12-03-2014; 00:00 tot en met 23:59						
Datum	**Wie**				**dossier**	**actie**
	organisatie	**persoon**	**rol**	**verantwoordelijke**		
12-03-2014 23:04	Huisartsenpraktijk F	***	***	F. Joosten	Huisartsdossier Hiemstra	Ingezien
12-03-2014 21:55	Huisartsenpraktijk E	***	***	E. Bongers	Huisartsdossier Hiemstra	Ingezien
12-03-2014 21:51	Huisartsenpraktijk D	***	***	D. Kuijt	Huisartsdossier Hiemstra	Ingezien
12-03-2014 21:45	Huisartsenpraktijk C	***	***	C. de Bie	Huisartsdossier Hiemstra	Ingezien
12-03-2014 21:41	Huisartsenpraktijk B	***	***	B. Toren	Huisartsdossier Hiemstra	Ingezien
12-03-2014 21:30	Huisartsenpraktijk A	***	***	A. Verschie	Huisartsdossier Hiemstra	Ingezien

Het overzicht is vrijwel gelijk aan de ‘overzicht inzage in uw dossier’. Een belangrijk verschil zijn de afgeschermde personen.

Huisarts Hiemstra vindt dit verdacht. Daarbij weet hij dat de heer Piek de vorige dag op de televisie te zien is geweest. Hij neemt contact op met de heer Piek en legt hem de situatie uit. Desgewenst kan de heer Piek het ‘overzicht inzage in uw dossier’ inzien in de praktijk van huisarts Hiemstra.

Bijlage 4. Toelichting conformiteit

De term "conformiteit" gebruiken we om aan te geven of een systeem is ingericht conform de eisen in dit document. Deze toelichting helpt de leverancier om zelf vast te stellen of het systeem in de hoofdlijn voldoet aan de eisen en wijst hiervoor de weg langs de belangrijkste zaken rond toegangslogging.

Maar met een systeem dat voldoet aan de eisen, is de zorgaanbieder nog niet klaar. Voor de zorgaanbieder gaat conformiteit nog een stap verder: zijn systeem voldoet pas als het is ingesteld met de eigen rollen, medewerkers, protocollen en dergelijke. Het goed instellen van deze zaken is een gezamenlijke actie van leverancier en zorgaanbieder. De systeemleverancier helpt de zorgaanbieder, de zorgaanbieder neemt de eindverantwoordelijkheid. Deze toelichting gaat hier verder op in.

Deze toelichting is ten slotte de basis waarop bijv. een externe auditor een toetsing verder kan inrichten, zowel voor het systeem als voor de inrichting ervan bij de zorgaanbieder.

Conformiteit valt zoals gezegd uiteen in twee delen.

1. Conformiteit 'logging van toegang' voor de leverancier

1. **Alle toegang** komt in de toegangslog:
    1) De toegangslog is ingeschakeld voordat een gebruiker toegang kan krijgen en mag pas uit als geen gebruikers toegang meer hebben tot patiëntgegevens;
    2) Er is een testscript om te controleren of alle rollen, gebruikers en exports op een juiste wijze in het bestand komen;
    3) Dit testscript wordt bij elke systeemwijziging uitgevoerd.

2. Het systeem hanteert ten minste een **basale rollenstructuur** (zodat de logregel goed kan worden gevuld):
    1) Elke gebruiker met rechten voor toegang tot patiëntdossiers heeft die rechten vanuit een 'rol';
    2) Bij elke toegang tot een patiëntdossier is er een 'verantwoordelijke' voor deze toegang (dit kan de gebruiker zelf zijn).

3. Het systeem hanteert **actuele protocollen** voor toestemming, autorisatie en behandelrelatie (zodat de logregel goed kan worden gevuld):
    1) Het systeem verwijst naar het geldend toestemmingsprotocol;
    2) Het systeem verwijst naar het geldend autorisatieprotocol;
    3) Het systeem verwijst naar het geldend behandelrelatieprotocol.

4. De leverancier heeft zicht op de manieren waarop data het systeem kunnen verlaten:
    1) De leverancier heeft een overzicht van alle **exports en/of koppelingen** die het systeem biedt en of dit geanonimiseerd/gepseudonimiseerd gebeurt.

5. Het logbestand heeft het **juiste formaat**:
    1) Alle velden zijn conform de specificaties en worden ook gevuld volgens de eisen (zie hoofdstuk 3 en bijlage 1)

6. **Toegang tot de logging** kent de juiste rolverdeling:
    1) De rol 'patiënt' bestaat:
        i. Het systeem biedt de rol 'patiënt' aan waarmee toegang kan worden verkregen tot de logging van één patiënt;

ii. Toegang via de rol ‘patiënt’ wordt altijd in de toegangslog opgenomen;
iii. Het juiste overzicht wordt gepresenteerd (zie bijlage 2).

2) De rol ‘verantwoordelijke voor toegang’ bestaat:
   i. Het systeem biedt de rol ‘verantwoordelijke voor toegang’ aan die toegang geeft tot de logging van de zorginstelling, en tot de logging per medewerker
   ii. De toegang via rol ‘verantwoordelijke’ wordt ook altijd in de toegangslog opgenomen;
   iii. De juiste overzichten wordt gepresenteerd (zie bijlage 2)

3) Afscherming van overzichten:
   i. De overzichten zijn niet anders toegankelijk dan via deze rollen;
   ii. Er zijn geen manieren om de logging te bekijken buiten deze rollen om.

7. Bij overgang door de zorgaanbieder naar een **nieuw systeem** moet het oude systeem in staat zijn de logregels mee te verhuizen naar het nieuwe systeem, het nieuwe systeem moet de regels inlezen. Beide acties leveren een logregel op.

2. Conformiteit ‘logging van toegang’ voor de zorgaanbieder

1. De **leverancier** geeft bij het systeem aan welke onderdelen samen zijn te beschouwen als een informatiedomein. Hij helpt de zorgaanbieder met de keuze van of inbedding in samengestelde informatiedomeinen in diens praktijk. Bijzondere aandacht besteedt hij daarbij eraan dat alle overzichten kunnen worden aangemaakt. De **zorgaanbieder** is verantwoordelijk voor de uiteindelijke keuze van informatiedomein of samengesteld informatiedomein.

2. De **leverancier** of iemand namens deze helpt de zorgaanbieder met het inrichten van een rollenstructuur en met het instellen van de verantwoordelijkheid. De **zorgaanbieder** stelt de rollenstructuur op en vult de verantwoordelijke in (NB Vóór de implementatie!)
   - NB deze eis loopt vooruit op het te verwachten ‘PvE autorisatie’. Een start voor rollen kan zijn: arts - assistente - POH - medewerker - helpdesk. Een start voor verantwoordelijke kan zijn dat het systeem één naam met functie hanteert die formeel verantwoordelijk is voor alle toegangsrechten (bijvoorbeeld X. Janssen – huisarts).

3. De **leverancier** of iemand namens deze helpt de zorgaanbieder met het formuleren van protocollen voor toestemming, autorisatie en behandelrelatie. De **zorgaanbieder** stelt protocollen op voor toestemming, autorisatie en behandelrelatie met een ingangsdatum:
   1) Het toestemmingsprotocol beschrijft hoe bij toegang tot een dossier eventuele afscherming door de patiënt wordt toegepast;
   2) Het autorisatieprotocol beschrijft hoe bij toegang tot een dossier de rechten daartoe worden gecontroleerd;
   3) Het behandelrelatieprotocol beschrijft hoe bij toegang tot een dossier wordt gecontroleerd of er een behandelrelatie bestaat

   - NB deze eis loopt vooruit op het PvE autorisatie. Een start kan zijn dat de organisatie in een document (bijvoorbeeld het praktijkjaarverslag) beschrijft hoe deze zaken zijn geregeld. De leverancier kan hiervoor een basistekst aanleveren.

4. De **leverancier** of iemand namens deze vult voor of met de zorgaanbieder een overzicht van actuele koppelingen en exports in. Hiermee wordt ook het systeem afgebakend: wat hoort er wel bij, wat niet? Het is belangrijk dat dit expliciet gebeurt:

voor alle delen die bij het systeem horen moet de toegang tot patiëntdossiers worden gelogd in het logbestand. De **zorgaanbieder** verifieert met het overzicht van de leverancier of alle bestaande koppelingen en exports wenselijk en legitiem zijn.

5. De **leverancier** of iemand namens deze test of alle toegang in het logbestand komt, met aandacht voor de lokale instellingen. De **zorgaanbieder** keurt het testrapport goed.

6. De **leverancier** of iemand namens deze test of het logbestand correct wordt gevuld.

7. De **leverancier** of iemand namens deze instrueert de zorgaanbieder over de twee rollen voor toegang tot de log en hoe daarmee om te gaan. De **zorgaanbieder** hanteert een procedure voor toegang patiënt en zet deze op de website, en vult de **verantwoordelijke voor toegang** in.
8. Als de zorgverlener overgaat op een nieuw informatiesysteem, moet hij waarborgen dat de toegangslog uit het oude systeem is in te zien gedurende de bewaartermijn.

Bijlage 5. Geparkeerde kwesties

Hieronder kwesties die mogelijk vragen oproepen of tot discussie leiden. Binnen de schrijversgroep hebben we gewikt en gewogen en een oplossing gekozen.

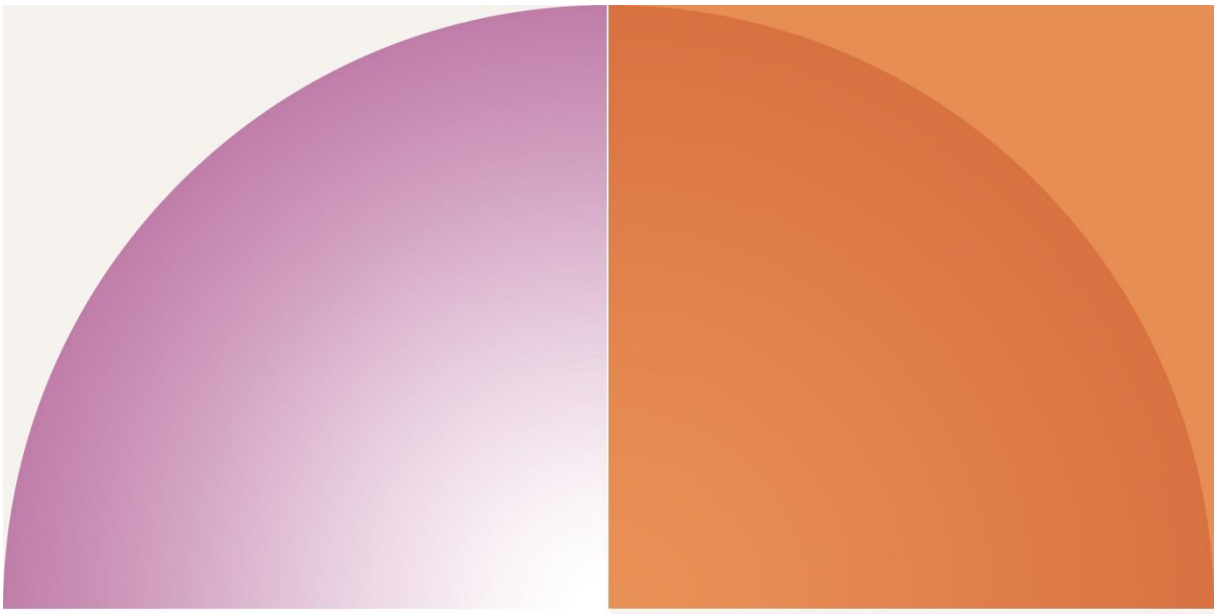
	kwestie	oplossing
1.	**bewaartermijn** *Hoe lang moet/mag je logregels bewaren?* Om die vraag te beantwoorden is gezocht naar een termijn vanuit de wetgeving. Die is vooralsnog niet gevonden, ook niet op een NEN / KNMG bijeenkomst rond deze vraag. Dan is het logisch om te kijken naar het belang van belanghebbers bij bewaren: de patiënt en de zorgaanbieder. De NPCF lijkt namens de patiënt te stellen dat twee jaar bewaren voldoende is. Als we gaan zitten op de stoel van de zorgaanbieder dan lijkt het een afweging tussen wat nodig wordt geacht voor zinnig gebruik (om gedrag van een medewerker te kunnen controleren) en de benodigde opslagcapaciteit. Ook hier lijkt twee jaar een acceptabel compromis. Voor alle partijen is het wenselijk om een harde termijn te stellen zodat iedereen zich daarop kan richten.	**bewaartermijn** Wij stellen de bewaartermijn van logregels op twee jaar. Korter mag niet, langer mag.
2.	**privacy van de medewerkers** *De NEN 7513 stelt dat de patiënt een overzicht moet kunnen krijgen van de inzage door medewerkers. Hoe zit het dan met de privacy van de medewerker?* Het gaat dan om privacy van de medewerker tegenover controle op door de patiënt op diens eigen privacy. Dat laatste weegt zwaarder denken wij.	**privacy van de medewerkers** Wij stellen hier geen specificaties voor op.
3.	**patiënt schrijft over naar een andere praktijk** *Wat moet gebeuren met de logregels als een patiënt overschrijft naar een andere praktijk? Immers het dossier verhuist mee met de patiënt.* Voor de 'oude' praktijk is het duidelijk: die kan de log nodig hebben om de medewerkers te kunnen controleren. De nieuwe praktijk heeft die log niet nodig. Voor de patiënt gaat het ook om inzage in de oude praktijk. Duidelijk dus: logbestand blijft bij de oude praktijk. Een vraag kan nog zijn: wat is de waarde van een 'losstaande' logregel, dus zonder dossier waar die aan refereert. Maar logregels staan altijd los van de geraadpleegde gegevens.	**patiënt schrijft over naar een andere praktijk** Een logbestand blijft bij de organisatie waar de inzage heeft plaatsgevonden. In de praktijk zal de logging bewaard worden tot precies 2 jaar na overdracht van het dossier.

4.	**de dokter/apotheker als bewaker van dossiers?** *Moet de dokter of toegangsverantwoordelijke namens de patiënt controleren wie bij diens dossier wil of is geweest?* Dat een zorgorganisatie moet waken over het gedrag van de eigen medewerkers staat vast. Maar namens de patiënt bewaker spelen dat stelt geen enkele partij en lijkt ook weer niet wenselijk vanuit privacyoogpunt. Met de gewenste insteek rond privacy is de patiënt de aangewezen persoon om te waken over toegang tot zijn eigen dossier. De rol 'patiënt' in de autorisatiestructuur is verplicht in elk systeem. In de praktijk is ontstaan dat sommige zorgverleners wél de toegang controleren. De voors en tegens dienen nader afgewogen. Niet in dit PvE maar wel daarbuiten moeten systemen toewerken naar toegang voor de patiënt op afstand.	**waken over dossiers** De patiënt zelf wordt gezien als bewaker van de toegang tot het eigen dossier. De rol 'patiënt' in de autorisatiestructuur is verplicht in elk systeem. De dokter heeft deze rol dus niet standaard namens de patiënt! In de periode tot een definitieve afspraak kan de zorgverlener gebruik maken van de rol patiënt om diens logging tot in detail te zien. Dit wordt wel gelogd.
5.	**hoe krijgt de patiënt inzicht in de inzage** *Toegang gaat vaak over organisatiegrenzen heen. Kan de patiënt dan wel goed inzicht krijgen in de inzage?* Stel de patiënt vermoedt dat er onterecht inzage is geweest in het medicatiedossier. In de apotheek kan hij een overzicht krijgen van toegang. Eventueel moet hij naar aanleiding daarvan ook bij andere zorgaanbieders een dergelijk overzicht gaan ophalen. Een oplossing leek het aanvankelijk om in de logregel van zorgaanbieder A informatie op te slaan van de *persoon* die vanuit zorgaanbieder B de raadpleger is, maar daaraan kleven grote nadelen: een veel groter logbestand doordat die informatie integraal moet worden opgenomen. Er is daarom gekozen voor het opnemen in de logregel van de *raadplegende organisatie* plus *identificerende gegevens* om de raadpleging op termijn voor de patiënt integraal te kunnen presenteren. Wat kan voor postpakketten kan ook voor inzage.	**inzicht in de inzage voor de patiënt** In de eerste instantie krijgt de patiënt alleen inzicht in de medewerker achter een raadpleging via de organisatie waar de medewerker werkzaam is. De logregel bevat wel gegevens om te worden gelinkt aan gerelateerde logregels elders voor integrale presentatie. Integrale presentatie voor de patiënt is daarmee in de toekomst mogelijk.
6.	**granulariteit** *In de logregel moet vastgelegd welk dossier of deel daarvan is geraadpleegd, verstuurd et cetera. Welke granulariteit (detaillering) is daarin vereist?* Voor de hand ligt dat de granulariteit in de logregel aansluit bij die in de autorisatiestructuur. Dus als er voor toegang onderscheid wordt gemaakt in financiële, administratieve, algemeen medisch inhoudelijk en specifiek medisch inhoudelijke gegevens dan is dat ook het niveau voor de logregel.	**granulariteit** De granulariteit in de logregel sluit aan bij die in de autorisatiestructuur.

7.	**nadere toelichting actie** *Geeft de combinatie van Actie en Dossiergegeven de patiënt voldoende duidelijkheid geven over de gepleegde toegang?* Voor het beoordelen van de impact van toegang is het voldoende om aan te geven of een actie een read betrof, dan wel een export. De impact van een export is over het algemeen groter omdat gegevens daarmee de organisatie verlaten. De vraag doet zich voor of de combinatie van Actie en Dossiergegeven de patiënt voldoende duidelijkheid geven, of dat nog een extra veld nodig is om de precieze actie te duiden.	**nadere toelichting actie** Een extra, toelichtend veld binnen Actie wordt onderzocht, uitwerking in fase 3.
8.	**Hoe is de log logica bij opvragen via het LSP?** *Krijgt de patiënt wel inzicht als de bevraging via het LSP loopt?* Voorbeeld LSP. Huisartsenpraktijk A vraagt medicatiegegevens op via het LSP, waarop het LSP met een geconsolideerd antwoord komt. De patiënt ziet alleen dat het antwoord via het LSP is verkregen en zal via het LSP moeten nagaan waar de gegevens hun oorsprong hebben	**wie logt bij bevraging via LSP** vrager, LSP 1x, alle organisaties waarvan gegevens worden ingezien
9.	**gegevens aanmelden bij LSP op logging** *Moet het aanmelden van gegevens bij het LSP op de logging?* Het aanmelden van gegevens bij het LSP is een privacygevoelig gegeven en wordt daarom gelogd. Actie is 'export', type gegeven is 'aanmelden gegevens'.	**gegevens aanmelden bij LSP op logging** ja
10	**is het nodig te loggen via welke applicatie gegevens zijn verkregen?** *Stel gegevens worden opgevraagd door een groot ziekenhuis. Kan de patiënt dan achterhalen wie die gegevens heeft opgevraagd? Moet daarvoor 'applicatie-id. in het bevraagde systeem' in de logregel op te nemen?* Stel de oogarts in ziekenhuis B ziet gegevens in bij huisartspraktijk A. Op zijn overzicht bij de huisarts leest de patiënt dat gegevens zijn opgehaald door ziekenhuis B, verder niets. Hij moet dus naar B als hij wil weten wie daar dan heeft ingezien. Dat klinkt logisch. Het ziekenhuis weet dat het de centrale logging moet betreffen, en geeft de patiënt daarin alle inzage, dus ook die van de oogarts op die dag. Stel dat de oogafdeling een eigen systeem met eigen toegangsmogelijkheden zou onderhouden, dan leest de patiënt dat al bij de huisarts: Oogheelkunde van B. De patiënt moet dan rechtstreeks bij de oogheelkunde gaan inzien. Antwoord is dus: nee de applicatie is niet relevant. Wel de organisatie die inzage heeft gevraagd.	**is het nodig te loggen via welke applicatie gegevens zijn verkregen?** nee de applicatie is niet relevant. Wel de organisatie die inzage heeft gevraagd.

11	**controle behandelrelatie, autorisatie, toestemming** *Hoe controleer je of er een behandelrelatie is, of de medewerker de juiste rechten heeft en of er toestemming is?* Deze vragen zullen worden beantwoord in het eind 2014 verwachte PvE rond autorisatie.	**controle behandelrelatie, autorisatie, toestemming** Wordt beschreven in het 2015 verwachte PvE rond autorisatie.
12	**wijzigingen autorisatiematrix loggen** *De norm 7513 stelt dat wijzigingen in de autorisatie moeten worden gelogd. Hoe moet dat?* Wijzigingen in autorisatiestructuur moeten worden gelogd. Echter die wijzigingen kennen een andere datastructuur dan de logging van toegang. Hoe die datastructuur eruit ziet komt aan de orde in PvE autorisatie	**wijzigingen autorisatiematrix loggen** Wordt beschreven in het 2015 verwachte PvE rond autorisatie.
13	**over hoeveel systemen gaat de logging** *Waar log je als je meerdere systemen hebt?* Verdeeld over de stad heeft Zorggroep Almere 23 gezondheidscentra. Alles werkt met Medicom. Hoe log je dan inzage van een arts van praktijk A in een dossier van een passant in praktijk B? Het ligt hier voor de hand om autorisatie en logging centraal te regelen. Naast de rol huisarts is er de rol 'waarnemend huisarts'. Dossiers zijn afzonderlijk benoemd in de autorisatiematrix: dossier bij huisarts A, dossier bij huisarts B. Een logregel is dan gemakkelijk op te stellen. En de patiënt kan bij zijn huisarts alle inzage zien. Stel dat Almere toch kiest voor autorisatiematrix en logbestand per huisarts. Dan komen er in het voorbeeld twee logregels, een bij A en een bij B. De patiënt ziet dan bij praktijk B dat praktijk A heeft ingezien, niet wie dat is geweest.	**over hoeveel systemen gaat de logging** Het is vrij om de systeemgrenzen te kiezen. Het lijkt aantrekkelijk om logging zoveel mogelijk te centraliseren. Echter autorisatie moet dan ook gecentraliseerd zijn.
14	**noodknop nodig?** *Waarom is de 'noodknop' opgenomen?* De 'noodknop' is bedoeld om autorisatieregels in noodgevallen te kunnen omzeilen. Een leverancier bouwt die voor de situatie dat een gebruiker op grond van autorisatie - behandelrelatiecontrole - toestemmingcontrole geen toegang krijgt en meent dat er voldoende reden is om deze uitslag te overrulen. Dit gebruik wordt vastgelegd in de logregel. In de praktijk zal een organisatie waar de noodknop herhaaldelijk wordt gebruikt daarop de autorisatie beter gaan inrichten. In het PvE autorisatie zal de noodknop worden beschreven. Dat de noodknop als functionaliteit wordt genoemd, betekent niet dat het een verplicht aanwezige functionaliteit is.	**noodknop** De 'noodknop' is bedoeld om autorisatieregels in noodgevallen te kunnen omzeilen. Gebruik moet opgenomen in de logregel. In het PvE autorisatie zal de noodknop worden beschreven.

15	Voor de zorg is het vaak nodig om de meest actuele gegevens in een ander systeem op te halen. Normaal gesproken wordt dit gedaan door een read op dat systeem voorafgaand of tijdens het patiëntcontact. Dat resulteert dan in een logregel per bevraagd systeem. Het kan zijn dat in de praktijk is ingeslopen dat op gezette tijden meerdere dossiers (tot vele of alle) tegelijk worden 'gesynchroniseerd' zonder dat er altijd een patiëntcontact aan de orde is. Dat leidt dan tot evenzovele logregels, maar is nogmaals, ongewenst.	**Synchroniseren** Ophalen van de meest actuele gegevens in een ander systeem gebeurt gerelateerd aan het patiënt contact en per dossier.
16	**Problemen die we nu nog niet overzien** *Invoeren van logging is nieuw. Wat te doen met nieuwe problemen?* NHG en Nictiz zijn gedurende gehele traject beschikbaar om antwoord te geven op nieuwe problemen.	**Overige kwesties** NHG en Nictiz zijn gedurende gehele traject beschikbaar om antwoord te geven op nieuwe problemen.
17	**Logging van Back-up** Back-up creëert een bestand waarmee een nieuw systeem mogelijk kan worden gevuld. Het is daarmee een kopie van het gegevensbestand en verdient daarom logging. De activiteit vindt echter vaak plaats buiten de zorgverlenersapplicaties en is een systeemactie.	Back-up wordt niet opgenomen in de toegangslog. Back-up activiteit moet wel gelogd worden.
18	**Toegang van helpdeskmedewerkers van een XIS-leveranciers tot medische gegevens** Deze toegang is op basis van wet- en regelgeving niet toegestaan. Het is met het oog op probleemoplossing voorstelbaar dat zich situaties voordoen waarbij helpdeskmedewerkers zicht hebben op medische gegevens.	Zicht op medische gegevens vindt altijd plaats onder verantwoordelijkheid van de zorgverlener en wordt als zodanig gelogd. Helpdesktoegang is in directe zin niet mogelijk en wordt derhalve niet gelogd.
19	**Verantwoordelijke zorgverlener niet bij behandeling betrokken** Er doen zich situaties voor waarbij de verantwoordelijke arts/zorgverlener niet betrokken is bij de behandeling en daarom strikt genomen geen behandelrelatie heeft en daarom feitelijk geen verantwoordelijk zorgverlener kan zijn.	Hieraan liggen organisatorische oorzaken ten grondslag die buiten de scope liggen van dit document.



Nictiz
Postbus 19121
2500 CC Den Haag
Oude Middenweg 55
2491 AC Den Haag

T 070 - 317 34 50
info@nictiz.nl
www.nictiz.nl