Handreiking

Informatiebeveiliging voor eerstelijnsinformatiesystemen

DEEL 1 AUTHENTICATIE EN AUTORISATIE

Betere gezondheid door betere informatie

Nictiz

Datum: januari 2017
Versie: 1.0
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 handreiking 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 authenticatie;
- de eisen aan de autorisatie
- een specificatie van de gegevens in de authenticatie en autorisatie;
- voorbeelden van authenticatie en autorisatie;
- 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:
- De eisen bestaan uit oplossingsonafhankelijke beschrijvingen, eventueel met voorbeelden.
- De eisen zijn gebaseerd op bestaande documentatie:
    - NEN 7512:2015 Medische informatica - Informatiebeveiliging in de zorg - Vertrouwensbasis voor gegevensuitwisseling
    - NEN 7510:2011 nl Medische informatica - Informatiebeveiliging in de zorg
    - 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
    - ISO 27002
    - Wet gebruik burgerservicenummer in de zorg
    - Wet algemene bepalingen burgerservicenummer
    - Gedragscode Elektronische Gegevensuitwisseling in de Zorg - EGiZ (2013)
- In de C*onformiteitstoelichting* (bijlage 4) is beschreven hoe partijen kunnen voldoen aan de eisen.

1.6. Leeswijzer

Dit document geeft een handreiking voor het inrichten van authenticatie en autorisatie 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 van authenticatie en autorisatie.
Hoofdstuk 3 beschrijft de concrete eisen aan de authenticatie en autorisatie.
Bijlage 1 beschrijft begrippen en het gegevensmodel.
Bijlage 2 bevat een overzicht van te gebruiken rollen.
Bijlage 3 beschrijft de matrices voor de autorisatie en de autorisatielog.
Bijlage 4 geeft voorbeeldoverzichten.
Bijlage 5 is de conformiteitstoelichting en geeft richting aan implementatie en kwalificatie.
Bijlage 6 beschrijft situaties en vragen die aanleiding kunnen geven tot discussie en tevens de keuzes die daarin zijn gemaakt.

H-2 Achtergrond authenticatie en autorisatie

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.

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.

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. Authenticatie

Het werkwoord authenticeren betekent 'authentiek, rechtsgeldig maken' of 'de identiteit vaststellen van'.

In dit kader omvat Authenticatie ook Identificatie. Deze twee begrippen zijn als volgt te definiëren:

- Identificatie, *"zeggen wie je bent",* betekent in deze context het identificeren van een gebruiker aan de hand van een uniek kenmerk, zoals een identificerend uniek nummer.
- Authenticatie, *"bewijzen wie je bent",* behelst de controle of de gebruiker daadwerkelijk de persoon of entiteit is die deze beweert te zijn. Dit kan door middel van iets wat een gebruiker weet (bijvoorbeeld een wachtwoord), heeft (zoals een reisdocument) of is (zoals vingerafdrukken).

Zodra is vastgesteld "wie" een gebruiker is (dit kan ook een applicatie of organisatie zijn) zal op basis van een gebruikersmatrix worden vastgesteld wat de functie is van de gebruiker en zal op basis daarvan een primaire rol worden toegekend.

Aangezien het bij de betrokken systemen persoonlijke medische gegevens betreft is een hoog zekerheidsniveau vereist in de Authenticatie. Dit vereist maatregelen zoals weergegeven in tabel 1 en tabel 2(conform NEN 7510:2015 6.3.3 en 6.3.2).

Authenticatiemiddel	**Registratie wijze**	**Aanvullende maatregelen**	**Zekerheidsniveau**
Geen	1		Laag
Geheime kennis (wachtwoord of PIN-code)	1		Laag
	2	Procedures voor veilig initialiseren en geheimhouden conform NEN-EN 12251	Midden
Fysiek kenmerk (biometrie)	3	Gebruiken in combinatie met ander authenticatiemiddel	Hoog
	3		Midden
Fysiek bezit (token)	4	Token conform CWA 14169; Initialiseren en uitreiken via waterdichte procedure; Gebruiken in combinatie met ander authenticatiemiddel	Zeer Hoog
	3	Gebruiken in combinatie met ander authenticatiemiddel	Hoog
	2		Midden
	1		Laag
Toetsbare verklaring (digitaal certificaat)	4	Uitgifte volgens ETSI-norm; Privésleutel alleen met PIN-code of biometrie te gebruiken en niet te kopiëren	Zeer Hoog
	3	Privésleutel alleen te gebruiken in combinatie met ander authenticatiemiddel	Hoog
	2	Privésleutel wel te kopiëren, maar alleen met PIN-code of biometrie te gebruiken	Midden
	1	Privésleutel te kopiëren	Laag

Tabel 1 Zekerheidsniveaus per authenticatiemiddel, registratiewijze en aanvullende maatregelen

Registratie wijze	Identificatieproces	Uitgifte authenticatiemiddel
1	Geen controle van gegevens, eigen opgave; pseudoniem mogelijk, fysieke aanwezigheid niet vereist. en geen toezicht op proces.	Geen toezicht op proces, middel mogelijk in bezit van anderen.
2	Fysieke aanwezigheid niet vereist en geen toezicht op het proces. Verificatie van gegevens die mogelijk niet uitsluitend bij hem/haar bekend zijn, herleidbaar naar een unieke identiteit. Beperkte toetsing van de opgegeven identiteit met gegevens uit erkend register.	Indien van toepassing worden gebruikersnaam en wachtwoord afzonderlijk verstrekt, via verschillende kanalen, en moeten direct worden geactiveerd.
3 fysiek	Directe controle (face-to-face), eenmalig. Verificatie van gegevens die mogelijk niet uitsluitend bij hem/haar bekend zijn, herleidbaar naar een unieke identiteit. Het tonen en toetsen van een document, incl. foto en handtekening, volgens Artikel 1 van de Wet op de identificatieplicht.	Indien van toepassing worden gebruikersnaam en wachtwoord afzonderlijk verstrekt, via verschillende kanalen, en moeten direct worden geactiveerd.
3 online	Bij online-registratie verificatie van meervoudige unieke gegevens waarvan kan worden aangenomen dat deze uitsluitend bekend zijn bij de entiteit, herleidbaar naar een unieke identiteit, en toetsbaar bij een erkend register. Eenvoudige digitale handtekening vereist.	Wordt ter beschikking gesteld via aangetekende post naar een getoetst adres of elektronisch beschikbaar gesteld na invoer van (persoonlijk verstrekt) wachtwoord of elektronische handtekening.
4	Ten minste directe controle (face-to-face), eenmalig, aan de hand van een document volgens Artikel 1 van de Wet op de identificatieplicht. Strenge toetsing van een wettelijk ID, incl. foto en handtekening. Verificatie van meervoudige unieke gegevens waarvan kan worden aangenomen dat deze uitsluitend bekend zijn bij de entiteit, herleidbaar naar een unieke identiteit, en toetsbaar bij een erkend register.	Persoonlijke verstrekking van het middel direct na strenge toetsing van identiteit. Of, na uitgebreide toetsing van de identiteit, wordt later ter beschikking gesteld (zoals onder registratiewijze 3).

Tabel 2 Overzicht registratiewijzen

2.3. Autorisatie

Autorisatie beschrijft het proces van toekennen van rechten aan gebruikers.

Autorisatie is daarmee een direct vervolg op Authenticatie. In de authenticatie wordt vastgesteld wie de gebruiker is en wat de functie van deze gebruiker is. Op basis van de functie worden rechten toegekend.

Voor het toekennen van rechten wordt gebruik gemaakt van een rollen gebaseerd systeem met 2 lagen. Op basis van de functie wordt een primaire rol toegekend die de rechten bepaalt, welke bij de bewuste functie horen. Er zijn in een organisatie een beperkt aantal functies en er is een gefundeerde relatie tussen de functie en de daarbij behorende rechten. Een bepaalde gebruiker kan verantwoordelijkheden hebben gekregen die verder gaan dan de verantwoordelijkheden behorend bij de functie. Die gebruiker kan één of meerdere additionele rollen toegekend krijgen die de rechten beschrijven behorend bij de specifieke verantwoordelijkheden.

H-3 Authenticatie en Autorisatie

3.1. Inleiding

Dit hoofdstuk is een handreiking in de vorm van een set van eisen waaraan authenticatie en autorisatie moeten voldoen, om tegemoet te komen aan wettelijke regels, normen en richtlijnen voor toegangslogging.
In de 'toelichting conformiteit' (bijlage 3) is beschreven hoe partijen kunnen voldoen aan de eisen.

3.2. Eisen aan Identificatie en Authenticatie

1. De identiteit van elke gebruiker wordt geverifieerd op basis van een wettelijk identiteitsdocument (WID). Deze verificatie wordt vastgelegd in het systeem met de datum en de identiteit van degene die de identiteit heeft vastgesteld;

2. Elke gebruiker moet eenduidig worden geïdentificeerd in het systeem op basis van één van de volgende registraties:
   a) Het UZI-nummer van de gebruiker;
   b) Het BSN nummer van de gebruiker;
   c) Het URA-nummer van de organisatie aangevuld met een uniek intern nummer;
   d) Een ander nummer dat gebruikers of organisaties uniek en controleerbaar identificeert;

3. Het Informatiesysteem kent een unieke gebruikersnaam of code toe aan elke gebruiker;

4. De organisatie(s) verantwoordelijk voor raadplegingen in andere organisaties is eenduidig geïdentificeerd in het systeem met een nummer dat de organisatie uniek en controleerbaar identificeert;

5. Elk systeem of applicatie via welke een raadpleging kan plaatsvinden in een andere organisatie is eenduidig geïdentificeerd in het informatiesysteem met een nummer (conform eis 2) van de raadplegende organisatie aangevuld met een uniek intern nummer;

6. De gebruiker krijgt de bij zijn verantwoordelijkheden behorende primaire rol en een eigen presentatierol toegekend;

7. Elke organisatie die toegang moet kunnen krijgen tot gegevens van het systeem krijgt een organisatierol toegekend;

8. Elke applicatie die toegang moet kunnen krijgen tot gegevens van het systeem krijgt een applicatierol toegekend;

9. Elke geïdentificeerde gebruiker kan uitsluitend toegang verkrijgen tot het informatiesysteem op basis van een 2-factor authenticatie. Hierbij worden bijvoorbeeld 2 van de volgende middelen gehanteerd:
   a) Wachtwoord, sms;
   b) biometrie;
   c) pas of token;
   d) toetsbare verklaring (digitaal certificaat);

   Zolang er nog geen algemeen beschikbare 2-factor authenticatie beschikbaar is voor patiënten/cliënten mag voor de authenticatie van patiënten/cliënten gebruik gemaakt worden van DigiD met sms;

10. Een wachtwoord moet voldoen aan de normen die daaraan naar huidige maatstaven worden gesteld. Bijvoorbeeld aan de volgende eisen:
    a) lengte van het wachtwoord is minimaal 9 karakters;

b) een wachtwoord wordt toegekend door het systeem wanneer een gebruiker is toegevoegd;
c) het toegekende wachtwoord moet bij tijdens de eerste toegang met dat wachtwoord worden gewijzigd in een door de gebruiker ingegeven wachtwoord dat niet gelijk mag zijn aan het toegekende wachtwoord;

11. Biometrie moet voldoen aan de normen die daarvoor naar huidige maatstaven worden gesteld;

12. Pas of token moet voldoen aan de normen die daarvoor naar huidige maatstaven worden gesteld, en tenminste aan de volgende eisen:
    a) uitgiftebeheersing conform registratiewijze 3 (NEN7510:2015 6.3.2) (Tabel 2 Overzicht registratiewijzen);
    b) procedure voor verliesmelding;
    c) een maximum van één pas per gebruiker per organisatie;

3.3. Eisen aan de Autorisatie

13. Een Gebruiker krijgt altijd 1 Primaire rol toegekend en kan op basis van verantwoordelijkheden binnen de organisatie een of meerdere Additionele rollen verkrijgen;

14. Een gebruiker die een patiënt/cliënt is, krijgt de primaire rol Patiënt toegekend en kan uitsluitend zijn eigen patiëntendossier en toegangslog benaderen;

15. Toegang tot gegevens kan uitsluitend op basis van rechten uit een rol;

16. De organisatie moet een lijst Primaire rollen definiëren en de rol Patiënt moet hier deel van uitmaken;

17. De organisatie moet een lijst Additionele rollen definiëren en de rol Toegangslogverantwoordelijke moet hier deel van uitmaken;

18. Elke wijziging in gebruikers, organisaties en applicaties en/of de daaraan gekoppelde rollen moet worden gelogd;

19. Het systeem heeft een rol-rechtenmatrix die de relatie legt tussen rollen en rechten en een gebruiker-rolmatrix die de relatie legt tussen gebruiker en rol(len);

20. Elke wijziging in de matrices uit 19 moet worden gelogd in een autorisatielog met de volgende elementen:
    a) Datum en tijd;
    b) Identificatie van degene die de wijziging uitvoert [id gebruiker];
    c) Aanduiding van de matrix die is gewijzigd [id matrix];
    d) Type wijziging: create, delete, change [id wijziging];
    e) Aanduiding van het record dat is gewijzigd: persoon, rol [id record];
    f) De feitelijke wijziging [beschrijvende tekst];
    In bijlage 3 is een voorbeeld opgenomen van een autorisatielog en de mogelijke presentatie ervan.

21. Wijziging aan de matrices in 20 is voorbehouden aan een beperkt aantal specifieke functionarissen binnen de organisatie. Deze wijziging moet bij voorkeur uitgevoerd worden op basis van het 4 ogen principe. Zie ook NEN7510:2011 par 11.1.1 (h,i,j,k).

22. het systeem verwijst eenduidig naar geldende protocollen (document of module) voor het afleiden van de rechten voor toegang voor een gebruiker, de toestemming door de patiënt en het vaststellen van de behandelrelatie;

23. Het systeem beoordeelt
    a) de rechten;
    b) de toestemming door de patiënt;
    c) de behandelrelatie;

24. Het systeem heeft ten minste één manier om de behandelrelatie te kunnen vaststellen. Dit proces wordt ingericht in overeenstemming met de Gedragscode Elektronische Gegevensuitwisseling in de Zorg - EGiZ.

25. De noodknop is een recht dat met een rol moet worden toegekend. Dit geldt voor bypass van autorisatie, toestemming en/of behandelrelatie;

26. Wijziging in een protocol voor autorisatie, toestemming, controle behandelrelatie, alsmede in gebruik van de noodknop of wijzigingen in het systeem die de toegang tot gegeven moet worden gelogd en deze wijzigingen moeten kunnen worden gepresenteerd in een of meer overzichten.

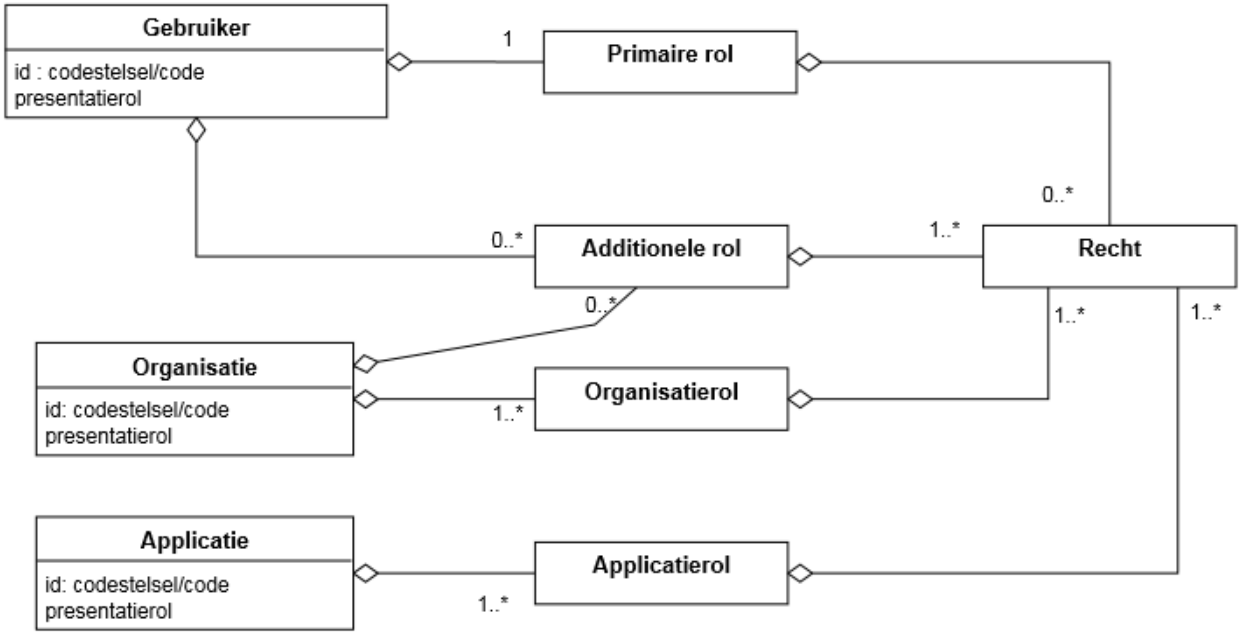
Bijlage 1. Begrippen en gegevensmodel

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.
Inzage	zie: Toegang
Gebruiker	Een gebruiker is altijd een medewerker of patiënt/cliënt geïdentificeerd door de organisatie. Gebruikers van systemen van andere organisaties zijn hier dus geen gebruikers. Gebruikers van andere organisaties worden niet geïdentificeerd door het informatiesysteem, slechts de andere organisatie. De identificatie van die gebruikers is de verantwoordelijkheid van de andere organisatie.
Presentatierol	De presentatierol beschrijft op (voor medewerker en patiënt) herkenbare wijze de functie van de gebruiker binnen de organisatie. Is dus geen 'Rol' met rechten. Voorbeelden: huisarts, POH-ggz, apotheker. N.B. de presentatierol wordt in het toegangsoverzicht voor de patiënt gepresenteerd
Rol	Een (verplicht) mechanisme gebruikt bij authenticatie om binnen autorisatie gelijke rechten voor meerdere personen (of applicaties onder hun verantwoordelijkheid) te beheren. Een rol omvat een pakket rechten in een systeem. Deze handreiking hanteert vier soorten rollen: • primaire rol, • additionele rol, • applicatierol, • organisatierol.
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
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.
Toestemming patiënt	Voor de invulling van de toestemming van de patient verwijzen wij naar: Van wet naar praktijk: implementatie van de WGBO Deel 4. Toegang tot patiëntengegevens (2004), paragraaf 2.2.5

Gegevensmodel authenticatie



Beschrijving van klassen

Recht	Toestemming tot het uitvoeren van een functie of logischerwijs bij elkaar behorende functies in het systeem.	Hieronder vallen ook toegang tot (onderdelen) van het systeem, exporteren van gegevens, maken van rapportages et cetera.
Functie	Het schrijven, lezen, exporteren of een andere actie van (een of meerdere soorten) gegevens in het systeem.	Hieronder vallen ook patiëntgegevens.
Gebruiker	Elke gebruiker van het systeem die via authenticatie een rol verkrijgt	Hieronder vallen ook patiënten
Organisatie	Elke organisatie die toegang moet kunnen krijgen tot gegevens van het systeem	
Applicatie	Elke applicatie die toegang moet kunnen krijgen tot gegevens van het systeem	
Primaire rol	Een rol (zie begrippen) toegekend aan een gebruiker. Verwijst naar bevoegdheden en verantwoordelijkheden naar patiënten. Iedere gebruiker heeft precies één primaire rol.	Primaire rol wordt alleen gebruikt op de 'achtergrond', voor het bepalen van het basispakket aan rechten. Op het overzicht voor patiënt en praktijk wordt de 'presentatierol' gebruikt, zie begrippen

		Voorbeelden van primaire rollen staan in kader 1. Patiënt is een verplichte primaire rol.
Additionele rol	Een aanvullende rol.	Wordt gebruikt om een extra pakketje rechten toe te kunnen kennen. Voorbeelden staan in kader 3.
Organisatierol	Een rol die kan worden toegekend aan een organisatie.	
Applicatierol	Een rol toegekend aan een applicatie.	

Toelichting datamodel & begrippen

Elke gebruiker krijgt een primaire rol, sommigen krijgen daarnaast aanvullende rollen

Toegang tot patiëntendossiers moet geregeld en gecontroleerd worden. Het is niet handig – en ook niet betrouwbaar – om voor elke nieuwe gebruiker te gaan uitzoeken wat hij wel of niet mag. In plaats daarvan stelt een zorgorganisatie vast welke 'basispakketten' en 'aanvullende pakketten' nodig zijn. Een nieuwe gebruiker krijgt een 'basispakket' en zo nodig een 'aanvullend pakket'. *Voor het basispakket gebruiken we in het datamodel de term 'primaire rol'. Zie Kader 1 voor voorbeelden van primaire rollen. Elke gebruiker krijgt precies één primaire rol. Dit is een belangrijk uitgangspunt om het ongewenst stapelen van rechten te voorkomen. Maatwerk is mogelijk door een (of meerdere) op een taak toegespitste 'additionele rol(len)' toe te voegen. Het kan ook voorkomen dat een gebruiker een primaire rol krijgt die geen enkel recht geeft.*

Kader 1

VOORBEELDEN PRIMAIRE ROLLEN	VOORBEELDEN PRESENTATIEROL
1 = apotheker	
2 = arts	**huisarts, waarnemer, AIOS, specialist, oogarts, internist, ..**
3 = fysiotherapeut	
4 = gezondheidszorgpsycholoog	**POH-GGZ**
5 = psychotherapeut	
6 = tandarts	
7 = verloskundige	
8 = verpleegkundige	**POH, POH-somatiek, centralist, POH-GGZ**
9 = paramedicus	**fysiotherapeut, logopedist, podotherapeut, POH-GGZ, huidtherapeut, ..**
10 = praktijkassistente	**assistente**
11 = stagiair	**coassistent, leerling verpleegkundige**
12 = ***patiënt*** (verplichte rol)	
13 = rechtenloze	**gemachtigde voor patiënt, manager, ..**

Toelichting

- de tabel PRIMAIRE ROLLEN is landelijk afgesproken voor de eerste lijn
- de PRIMAIRE ROL voor een medewerker wordt binnen de organisatie toegekend, op grond van BIG-rol en functie binnen de organisatie
- de rechten bij een PRIMAIRE ROL zijn vaak (deels) in het systeem verankerd
- de PRIMAIRE ROL geeft toegang, de PRESENTATIEROL geeft geen rechten maar verduidelijkt voor de patiënt om welke medewerker het gaat
- PRESENTATIEROL wordt niet landelijk afgestemd, elke organisatie kiest termen die voor de patiënt duidelijk zijn
- medewerkers met verschillende PRIMAIRE ROL kunnen dezelfde PRESENTATIEROL krijgen, zoals bijvoorbeeld POH-GGZ
- als bij een medewerker presentatierol niet is ingevuld geldt de primaire rol als presentatierol

een rechtenloze heeft geen rechten vanuit de PRIMAIRE ROL, maar kan wel een additioneel recht hebben om het dossier in te zien: in zo'n geval is het verhelderend als de organisatie voor die betrokkene ook een duidelijke presentatierol kiest

Controle van uitgegeven rechten en van gedrag gebruikers wordt zo gemakkelijk

Voor degene die binnen de organisatie de toegang regelt is het handig werken met een overzichtelijk pakket primaire rollen en aanvullende rollen. De toegangslogverantwoordelijke ziet op zijn 'overzicht per gebruiker' diens primaire rol, en diens additionele rollen.

Controle van toegang door de patiënt

Het is gewenst dat een patiënt gemakkelijk kan zien welke gebruikers zijn dossier hebben ingezien. En dat hij kan snappen waarom die inzage nodig was. We geven hem dat inzicht met lijstje met naam en functie van de gebruiker (naast bijvoorbeeld datum en dossierdeel).

Welke functiebenaming duidelijk is naar de patiënt bepaalt een organisatie zelf. Vaak is die gelijk aan primaire rol, maar ook vaak zal de organisatie liever een andere functiebenaming gebruiken. Hiervoor gebruiken we in het datamodel het attribuut 'presentatierol', dat dus aan een gebruiker hangt. Zie kader 2 voor voorbeelden van presentatierol.

Additionele rol
Met additionele rol regel je een pakketje rechten dat niet specifiek aan een primaire rol valt te koppelen. De organisatie of leverancier bepaalt welke aanvullende pakketten nodig zijn. Bijvoorbeeld: patiëntselecties, toegangslogbeheer, facturen, pakket gemachtigde voor patiënt, et cetera. Zie Kader 2 voor voorbeelden.

Organisatierol
Organisatierol wordt gehanteerd indien een externe organisatie gegevens kan ophalen *zonder* dat de zorgverlener die de gegevens opvraagt bekend wordt bij de bevraagde organisatie. Denk aan het LSP. Ook een organisatierol kent een presentatierol. Zie kader 3.

Kader 2
VOORBEELDEN ADDITIONELE ROLLEN

- Klaarzetten exports
- Facturering
- Functioneel beheer
- POH-GGZ
- Rapportages / overzichten
- Toegangsbeheer
- Toegangslog
- Toekennen rechten
- (pakket) huisarts
- (pakket) waarnemer
- (pakket) Internist
- (pakket) Oogarts
- (pakket) Podotherapeut
- ..

Opmerkingen
- Het kan nodig zijn om fijnmaziger te werken, bijvoorbeeld per type Export een additionele rol: Export-LINH; export Zorgdomein, ..
- Een additionele rol kan nodig zijn indien een specialist bijvoorbeeld extra rechten nodig heeft, bijvoorbeeld om eigen aantekeningen te kunnen opslaan.
- Een additionele rol "oogarts" bevat dan het pakket rechten dat een oogarts heeft bovenop de basale rechten voor arts.

Kader 3

VOORBEELDEN ORGANISATIEROL	VOORBEELDEN PRESENTATIEROL
- VNVN	**landelijk schakelpunt EPD**

Opmerkingen
- Het doel van het benoemen van organisatierol is aan de patiënt (en toegangslogverantwoordelijke) kunnen tonen dat gegevens op deze wijze zijn opgehaald.
- De eigen organisatie kan niet tonen wie de gegevens heeft opgevraagd: daarvoor moet de patiënt bij de betreffende organisatie het logoverzicht opvragen.

Applicatierol
Applicatierol wordt gehanteerd indien een eigen (deel-)applicatie gegevens kan exporteren zonder tussenkomst van een gebruiker, denk aan LINH, NHG-doc, ZorgDomein, Digitalis. Ook een applicatierol kent een presentatierol. Zie kader 4.

Kader 4

VOORBEELDEN APPLICATIEROLLEN	VOORBEELDEN PRESENTATIEROL	ANONIEM
- LINH-export		ja
- Meetpunt kwaliteit-export	**gegevenscontrole**	**nee**
- Zorgdomein	**verwijsbrief**	**nee**
- ..		

Opmerkingen
- Het doel van het benoemen van applicatierollen is het verschaffen van duidelijkheid bij de toegangslogbeheerder welke exports hebben plaatsgevonden, hier volstaat meestal de technische naam
- **Extra aandacht is nodig** als gegevens niet-geanonimiseerd de organisatie verlaten: in dat geval komt de export ook op het overzicht dat de patiënt kan opvragen. In dat geval is het van belang om een "presentatierol" toe te voegen die voor de patiënt inzicht geeft in de noodzaak om gegevens te delen. Het kan handig zijn om dan in 'presentatierol" te refereren aan de persoon die bij de ontvangende organisatie de gegevens inziet of bewerkt

Afwegingen bij dit ontwerp
We hebben gezocht naar een oplossing met zo weinig mogelijk rollen, en toch maximale duidelijkheid naar de patiënt. Volgende stap is dit ontwerp met de leveranciers bespreken.

Bijlage 2. Rollen overzicht

Primaire rollen

De primaire rol bepaalt het basisrechtenpakket voor medewerkers met die rol, en het ligt voor de hand de primaire rollen te laten aansluiten bij functies die in de organisatie zijn vastgesteld. Kader 1 geeft een goed bruikbare voorzet voor primaire rollen die nodig zijn in de eerstelijn.
Het beperkt houden van het aantal primaire rollen is een voorwaarde voor het goed zicht kunnen houden op de vigerende toegangsrechten binnen die organisatie, een taak voor de verantwoordelijke voor toegang binnen de organisatie.
Bij het koppelen van rechten aan een primaire rol (soms door de systeemleverancier in het systeem vervlochten) moet bedacht worden dat alle medewerkers die deze primaire rol krijgen dan ook die rechten hebben. Wederom geldt dat dit goed moet aansluiten op wat in de praktijk gewenst en op maat is.
Het aangewezen mechanisme om een individu extra rechten te geven is het toekennen van een of meerdere additionele rollen (zie onder).

Verplichte primaire rol

Patiënt

Additionele rollen

Enkele verplichte procesrollen, verder vrij te definiëren. De additionele rol heeft betrekking op een specifieke verantwoordelijkheid waarvoor toegang tot gegevens noodzakelijk is. Het verdient aanbeveling deze verantwoordelijkheden zoveel mogelijk in aparte rollen onder te brengen.

Verplichte procesrol

Toegangslogverantwoordelijke

Presentatierollen

De presentatierol maakt het mogelijk om desgewenst af te wijken van de naam die aan de primaire rol hangt, en te kiezen voor een naamgeving die richting patiënt in de praktijk gehanteerd wordt voor een functionaris. Bedenk daarbij dat de presentatierol dan verschijnt op het op de patiënt toegespitste ‘Overzicht inzage in uw dossier’. De presentatierol is dus gekoppeld aan de medewerker, niet aan de rol. Vrij te definiëren.

Organisatierollen

Vrij te definiëren. Betreft externe partij die toegang kan krijgen tot gegevens.

Applicatierollen

Vrij te definiëren. Betreft interne applicaties die toegang krijgen tot gegevens.

Bijlage 3. Rol-rechtenmatrix, Gebruiker-rolmatrix en Autorisatielog

Deze bijlage beschrijft de Rol-rechtenmatrix en de Gebruikerrolmatrix en hoe deze eruit kunnen zien. Tevens wordt een voorbeeld gegeven van de autorisatielog en hoe deze getoond zou kunnen worden.

Rol-rechtenmatrix

In de rol-rechtenmatrix wordt vastgelegd welke rechten zijn toegekend aan welke rol. Deze matrix bevat op de ene as alle verschillende rollen die binnen het systeem worden gehanteerd en op de andere as de verschillende rechten die gebruikers kunnen hebben om in het systeem hun taken uit te voeren. Hoewel dat niet de voorkeur heeft zal in de praktijk deze structuur vaak zijn verankerd in het systeem.

Rechten Rollen	Recht 1	Recht 2	Recht 3	Recht 4	Recht 5	Recht 6	Recht 7	Recht 8	Recht 9
Primaire Rol 1	x		x		x	x	X		
Primaire Rol 2		X	x	x					
Primaire Rol 3		x			x			x	X
Primaire Rol 4				x			x	x	
Additionele Rol A									
Additionele Rol B									
Additionele Rol C									
Additionele Rol D									

Gebruiker-rolmatrix

In de gebruiker-rolmatrix legt de verantwoordelijke voor toegang vast welke rollen zijn toegekend aan welke gebruiker in het systeem. De rolmatrix bevat op de ene as alle gebruikers die toegang kunnen krijgen tot het systeem en op de andere as de rollen die deze gebruikers kunnen krijgen toegekend.

Een medewerker mag in het systeem maar 1x voorkomen als gebruiker met een rol (primair plus evt. additioneel) die rechten geeft[1]. Bij voorkeur is de gebruiker-rol dan ook gekoppeld met het HRM systeem, zodat er *by design* een goede bewaking mogelijk is dat gebruikers niet blijven bestaan als de medewerker uit dienst is, of dat oude rechten blijven bestaan als medewerkers van functie wisselen.

Uiteindelijk leidt autorisatie tot een koppeling van een geïdentificeerde gebruiker (persoon) aan de rollen die deze gebruiker mag uit voeren binnen het systeem.

Rollen Gebruikers	Primaire Rol 1	Primaire Rol 2	Primaire Rol 3	Primaire Rol 4	Additionele Rol A	Additionele Rol B	Additionele Rol C	Additionele Rol D
Gebruiker 1	x				x	x	X	
Gebruiker 2		X						
Gebruiker 3		x			x			X
Gebruiker 4				x			x	

Autorisatielog

In de autorisatielog worden alle wijzigingen vastgelegd die zijn uitgevoerd op de Rol-rechtenmatrix en op de Gebruiker-rolmatrix . Tevens worden vastgelegd alle wijzigingen op de protocollen die bepalen hoe het systeem controleert of een gebruiker toegang krijgt, en de systeemwijzigingen Met behulp van de autorisatielog kan worden vastgesteld welke rollen op

[1] In de uitzonderlijke situatie dat een persoon bij een organisatie twee aanstellingen heeft is het natuurlijk ongewenst dat het systeem de rechten vanuit beide aanstellingen samenvoegt. Bij elke raadpleging of actie in het systeem moet duidelijk zijn vanuit welke aanstelling deze actie plaatsvindt, waarbij het systeem de rollen en rechten vanuit die aanstelling hanteert.

een bepaald moment aan een gebruiker waren toegekend en welke acties tot die situatie hebben geleid. Tevens kan worden vastgesteld welke rechten op een bepaald moment aan een rol waren toegekend en welke acties tot die rechten hebben geleid.

Met de onderstaande aanzetten voor overzichten geven we impliciet aan welke zaken moeten worden vastgelegd in de autorisatielog[2].

Voor de verantwoordelijke voor de toegang is het van belang om snel inzage te hebben in de geldende toegangsrechten van medewerkers. Met het 'Overzicht uitgegeven toegangsrechten' komt hij gemakkelijk ongewenste toegangsrechten bij een medewerker op het spoor[3].

Overzicht uitgegeven toegangsrechten	**Overzicht wijzigingen toegangsrechten**	**Overzicht wijziging autorisatie**
wanneer afdrukken bijv. maandelijks op papier door verantwoordelijke voor toegang (bijv. huisarts, apotheker, directeur zorggroep); adhoc **in de kop** datum, organisatie **in de regels** medewerker, primaire rol, presentatierol, additionele rollen applicatie, applicatierol organisatie, organisatierol	**wanneer afdrukken** bijv. maandelijks op papier door toegangsverantwoordelijke; adhoc **in de kop** datum van-tot, organisatie **in de regels** datum + tijdstip wijziging, wijzigende medewerker, verantwoordelijke voor wijziging, betreft medewerker, wijzigingsnr*, oude toegangsrechten, nieuwe toegangsrechten idem applicatie, organisatie * wijzigingstabel, bijvoorbeeld 'nieuwe medewerker', 'wijziging presentatierol', 'nieuwe additionele rol', 'wijziging primaire rol', schrappen additionele rol.	**wanneer afdrukken** bijv. maandelijks op papier door toegangsverantwoordelijke; adhoc **in de kop** datum van-tot, organisatie **regels** datum + tijdstip wijziging, wijzigende, medewerker, verantwoordelijke voor wijziging, betreft systeem, wijzigingsnr**, oud oid, nieuw oid ** wijzigingstabel, bijvoorbeeld 'procedure toestemming gewijzigd' 'autorisatietabel gewijzigd', procedure autorisatie gewijzigd', procedure controle behandelrelatie gewijzigd', 'procedure gebruik noodknop gewijzigd'

Echt bedoeld voor het grip krijgen op vermeend misbruik van rechten zijn twee aanvullende overzichten: 'Overzicht wijzigingen toegangsrechten' en 'Overzicht wijziging autorisatie'. Hiermee ziet de verantwoordelijke voor toegang ook tijdelijke wijziging van in toegangsrecht respectievelijk wijziging in de autorisatiestructuur. Deze laatste overzichten geven ook inzicht in de wijziging van de autorisatiestructuur.

[2] Autorisatielog is gehanteerd als functionele term. Het kan onderdeel uitmaken van de gewone logging, maar ook van de systeemlog. Belangrijk is dat de overzichten kunnen worden geproduceerd.
[3] NB de wijzigingen in de autorisatie zijn niet te zien in het Overzicht wijzigingen toegangsrechten. Dus als bij een rol de rechten worden uitgebreid of beperkt, dan wordt dit niet afgedrukt per medewerker in dit Overzicht.

Bijlage 4. Voorbeelden van overzichten

Overzicht uitgereikte rechten

Deze bijlage bespreekt hoe de uitgereikte rechten worden getoond aan de toegangsverantwoordelijke. Het overzicht betreft:

- Overzicht uitgereikte rechten aan gebruikers
- Overzicht uitgereikte rechten aan applicaties
- Overzicht uitgereikte rechten aan organisaties

Overzicht uitgereikte rechten aan gebruikers

De toegangslogverantwoordelijke mag dit overzicht inzien.

Huisartsenpraktijk Bovensmilde Overzicht uitgegeven rechten aan gebruikers				Gemaakt op 21-04-2016; 12:30:02	
	primaire rol	**additionele rol**	**presentatierol**	**laatste wijziging**	
Jan Los	arts	pakket huisarts	huisarts	21-03-2014	
Meta Bool	praktijkassistente	naw en afspraken		21-03-2014	
Pieter Nel	stagiair		coassistent	21-03-2014	

Overzicht uitgereikte rechten aan organisaties

De toegangslogverantwoordelijke mag dit overzicht inzien.

Huisartsenpraktijk Bovensmilde Overzicht uitgegeven rechten aan organisaties				Gemaakt op 21-04-2016; 12:30:02	
	organisatierol		**presentatierol**	**laatste wijziging**	
VZVZ	LSP		Landelijk schakelpunt EPD	21-03-2014	

Overzicht uitgereikte rechten aan applicaties

De toegangslogverantwoordelijke mag dit overzicht inzien.

Huisartsenpraktijk Bovensmilde Overzicht uitgegeven rechten aan organisaties				Gemaakt op 21-04-2016; 12:30:02	
	applicatierol	**additionele rol**	**presentatierol**	**laatste wijziging**	**Gegevens geanonimiseerd**
ExportLinH	export		ExportLinH	21-03-2014	Ja
Export kwaliteit	export		Export kwaliteit	21-03-2014	nee

Bijlage 5. Toelichting conformiteit authenticatie en autorisatie

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 authenticatie en autorisatie.

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 voor leverancier en gebruiker, en is hier afzonderlijk beschreven voor authenticatie en autorisatie.

1. Conformiteit voor de leverancier

a. authenticatie

1. Het systeem geeft een persoon slechts toegang tot het systeem en de daarin opgeslagen gegevens als hij is ingevoerd als gebruiker[4] en op grond van bij de gebruiker geldende identificatie en authenticatie
2. Het systeem geeft een externe organisatie slechts toegang tot het systeem en de daarin opgeslagen gegevens als deze organisatie is ingevoerd met geldende identificatie en authenticatie
3. Het systeem geeft een applicatie binnen het informatiedomein (inclusief de eigen applicatie) slechts rechten voor exports als deze applicatie is ingevoerd met geldende identificatie en authenticatie

b. autorisatie

1. Een gebruiker (persoon of externe organisatie) krijgt slechts toegang tot het systeem en de daarin opgeslagen gegevens middels een of meerdere rollen
2. Een applicatie binnen het informatiedomein krijgt slechts rechten voor exports middels een applicatierol.
3. Het systeem ondersteunt de zorgaanbieder met een rollenstructuur waarin sprake is van 1 primaire rol, 0, 1 of meerdere additionele rollen, applicatierollen, organisatierollen en presentatierollen. Indien het systeem het onderscheid tussen primaire en additionele rollen niet afdwingt is de leverancier eraan gehouden de zorgaanbieder te wijzen op de noodzaak om dit procedureel te bewaken.
4. Het systeem kan overzichten vervaardigen die de vigerende rechten voor de gebruiker zichtbaar maakt, alsmede de wijzigingen daarin. Het systeem kan ook overzichten maken waarin duidelijk is welke rechten aan een rol worden ontleend.
5. Het systeem ondersteunt het werken met presentatierollen.
6. De leverancier ondersteunt de zorgaanbieder met het inregelen van de rollenstructuur voor medewerkers, externe organisaties en applicaties die gegevens exporteren en het controleren daarvan met de overzichten.
7. De leverancier hanteert de rol patiënt waarmee exclusief toegang wordt verkregen tot een enkel dossier.
8. De leverancier vergewist zich ervan dat alle wijzigingen en rolrechtenmatrix, gebruikerrolmatrix, protocollen voor controle van autorisatie, toestemming,

[4] De NEN7510 hanteert het begrip Informatiedomein om aan te geven wat het geldigheidsgebied is van het stelsel van identificatie, authenticatie, autorisatie en logging.

behandelrelatie en gebruik noodknop en systeemwijzigingen die kunnen resulteren in andere rechten voor gebruikers worden gelogd en kunnen worden bekeken in een overzicht

2. Conformiteit voor de zorgaanbieder

a. authenticatie

1. De zorgaanbieder is verantwoordelijk voor het regelen van rechten tot het systeem voor de medewerkers opdat zij kunnen beschikken over gepaste informatie over de patiënten waarvoor zij zorg moeten verlenen (dit omvat identificatie, authenticatie en autorisatie)

b. autorisatie

2. De zorgaanbieder is verantwoordelijk voor het selecteren van primaire rollen, organisatierollen en additionele rollen.
3. De zorgaanbieder is verantwoordelijk voor het bewaken dat elke gebruiker precies 1 primaire rol heeft.
4. De zorgaanbieder is verantwoordelijk voor het vervaardigen van de overzichten om de toegang te bewaken
5. De zorgaanbieder is verantwoordelijk voor het activeren en beschikbaarstellen van de rol patiënt. In het ideale geval heeft de patiënt zelf toegang tot inzage. Indien dit niet het geval is heeft de zorgaanbieder dit recht, en gebruikt dit samen met de patiënt indien de patiënt inzage wil in de gepleegde toegang. Dit kan zijn via presentatie op het scherm, via een print of vergelijkbaar.

Bijlage 6. Geparkeerde kwesties

	Kwestie	Oplossing
1	**Zijn de rollen niet gewoon de autorisatierollen, dus niet alleen voor privacy ?** Het PvE Informatiebeveiliging voor eerstelijnssystemen focust op privacy rond patiëntgegevens. Echter de gekozen rollen en systematiek zijn bruikbaar voor alle toegangsbeheer van het systeem.	**Breder gebruik oplossing** Gekozen rollen en systematiek zijn bruikbaar voor alle toegangsbeheer van het systeem.
2	De **wijziging van behandelrelatie** van een zorgverlener met een patiënt kan als gevolg hebben dat de resulterende toegang tot het dossier van die patiënt wijzigt. Echter het gaat vooralsnog nogal ver om dat vast te leggen in een autorisatieoverzicht. Iets anders is het wijzigen van het **protocol van het vaststellen van de behandelrelatie**. Die wordt wel getoond in het Overzicht wijziging autorisatie.	**Wijziging van behandelrelatie** op patiëntniveau hoeft vooralsnog niet te kunnen worden getoond in een van de overzichten. **Wijziging van het protocol van het toetsen van behandelrelatie** moet kunnen worden getoond in het Overzicht wijziging autorisatie.
3	De **wijziging van toestemming** van een patiënt kan als gevolg hebben dat de resulterende toegang tot het dossier van die patiënt wijzigt. De toestemming voor toegang tot patiëntgegevens wordt bepaald aan de hand van het toestemmingsprotocol. Daarbij kan de patiënt extra toestemming verlenen, juist intrekken, respectievelijk (delen van) zijn dossier afschermen voor gebruikers. Dat tezamen maakt het toestemmingsschema. Wanneer het schema wordt gewijzigd dan wordt dat gelogd en deze wijziging moet inzichtelijk zijn voor de patiënt. Iets anders is het **wijzigen van het protocol van het vaststellen van de toestemming**. Die wordt getoond in het Overzicht wijziging autorisatie.	**Wijziging van toestemming** op patiëntniveau moet aan de patiënt kunnen worden getoond, maar valt buiten het kader van deze eisen. **Wijziging van het protocol van het toetsen van toestemming** moet kunnen worden getoond in het Overzicht wijziging autorisatie.