vitalink
gegevens delen, van vitaal belang

NOTA

Voorwaarden tot toetreding

Vitalink Circle of Trust (CoT) (v201508)

Vitalink
18-08-2015

INHOUD

Vitalink wordt hoofdzakelijk gebruikt door individuele zorgverleners of hulpverleners en hulpverleners. Het collectief gebruik van Vitalink door meerdere gebruikers onder de hoedanigheid van een voorziening is mogelijk na de ondertekening van een overeenkomst, met de nodige bijlagen.

De overeenkomst bevat volgende belangrijke elementen:
- respecteren van volgende regelgeving
    - de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (wet Verwerking Persoonsgegevens);
    - de wet van 22 augustus 2002 betreffende de rechten van de patiënt;
    - de wettelijke en reglementaire bepalingen met betrekking tot de uitoefening van de geneeskunde;
    - het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer;
    - het decreet van 13 juli 2012 houdende de oprichting en organisatie van een Vlaamse dienstenintegrator;
    - de wettelijke en reglementaire bepalingen met betrekking tot het beroepsgeheim, met inbegrip van artikel 458 van het Strafwetboek;
    - het decreet van 25 april 2014 betreffende de organisatie van het netwerk voor de gegevensdeling tussen de actoren in de zorg.
- aanwijzen van, al dan niet onder zijn medewerkers, een veiligheidsconsulent
- opstellen van een veiligheidsbeleid, dat verder werkt op het ontwerp van veiligheidsplan

Na ondertekening van de overeenkomst krijgt de voorziening uitsluitend toegang tot de gegevens die die relevant, noodzakelijk en pertinent zijn voor de concrete behandeling van de zorggebruiker (patiënt/cliënt) en voor het verzekeren van de continuïteit van de zorg.

De voorziening draagt de verantwoordelijkheid om te bepalen in welke mate en op welke wijze de gegevens in individuele dossiers toegankelijk zijn voor personen die bij hun activiteiten in het kader van de gezondheidszorg of welzijnszorg betrokken zijn. Hierbij houdt de voorziening rekening met de functie van deze personen, de aard van en de potentiële risico's verbonden aan de gegevens. Specifiek voor Vitalink werd door het Sectoraal Comité Gezondheid bepaald dat het registeren en bewijzen van een zorgrelatie tussen een zorggebruiker en een zorgverlener of hulpverlener of hulpverlener van de voorziening door de voorziening wordt georganiseerd.

Bij de overeenkomst horen 2 formulieren. Een eerste formulier voor de evaluatie van de beveiliging van het informatiesysteem voor de bescherming van persoonsgegevens. En een tweede formulier voor de zelfevaluatie ivm toetreding tot de Vitalink Circle of Trust (CoT). Het formulier wordt best door de veiligheidsconsulent ingevuld, samen met de verantwoordelijke voor de verwerkingen van de voorziening. Het tweede formulier is eerder praktische checklist. De voorziening dient voor dit formulier de conformiteit met de regelgeving en met de machtigingen van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (waaronder eveneens de sectorale comités worden begrepen), de toegang tot de diensten van het eHealth-platform, garanties op het gebied van informatieveiligheidsbeleid, van logische toegangsbeveiliging, procedures voor het beheer van therapeutische en zorgrelaties, klachtenprocedures, de interne organisatie van de voorziening en opleidingen na te gaan.

1 REALISEREN VAN EEN COT (PROCESBESCHRIJVING)

Hieronder beschrijven we de verschillende stappen van het proces.

1.1 Eerste contact met Zorg en Gezondheid

Voorzieningen die willen toetreden tot de CoT van Vitalink nemen schriftelijk (e-mail, brief) contact op met Zorg en Gezondheid met het verzoek om een toe te treden tot de Vitalink CoT. Zorg en Gezondheid bezorgt de geïnteresseerde de overeenkomst met de bijhorende formulieren. Een veiligheidsconsulent is het best geplaatst om de nodige toelichting te geven bij de overeenkomst en de inhoud van de formulieren. Alle documenten en informatie zijn ook beschikbaar op de website van Vitalink (http://www.vitalink.be).

1.2 Toevoegen aan de lijst van CoT in acceptatie-omgeving

Na het ontvangen van onderstaande informatie krijgt de voorziening toegang tot de acceptatieomgeving van Vitalink.

- Naam van de organisatie
- KBO-nummer
- Rol of hoedanigheid (bv. Woonzorgcentrum, verpleegkundige organisatie, …)

De voorziening krijgt een melding per e-mail van Zorg en Gezondheid dat ze werd opgenomen in de lijst van CoT van voorzieningen voor Vitalink, voor de accepatie-omgeving.

De toegang tot de productie-omgeving is pas mogelijk na ondertekening van de overeenkomst door beide partijen.

1.3 Uitvoeren van de voorwaarden

De voorziening realiseert alle voorwaarden om toe te treden tot de Vitalink CoT. In dit documenten worden de voorwaarden in detail toegelicht.

1.4 Ondertekenen overeenkomst

De voorziening vult de overeenkomst “ICT-veiligheidsbeleid in het kader van een netwerk voor gegevensdeling tussen de actoren in de zorg (Vitalink Circle of Trust (CoT)” in, en bezorgt de ondertekende overeenkomst (3 exemplaren) samen met de checklist aan Zorg en Gezondheid. Dit kan per e-mail via vitalink@vlaanderen.be of per post op het adres Koning Albert II-laan 35 bus 33, B-1030 Brussel, België.

Na validatie van de formulieren en overeenkomst bezorgt Zorg en Gezondheid de voorziening een ondertekend exemplaar van de overeenkomst terug via e-mail of post.

1.5 Toevoegen aan de lijst van CoT in productie-omgeving

Op basis van het KBO-nummer en de hoedanigheid van de voorziening zal Zorg en Gezondheid de voorziening opnemen in de lijst van CoT. Een rechtenmatrix op basis van de hoedanigheid regelt de toegang tot de verschillende gegevenstypes en de rechten (lezen en/of schrijven).

De voorziening krijgt een melding per e-mail van Zorg en Gezondheid dat ze werd opgenomen in de lijst van CoT van voorzieningen voor Vitalink, voor de productie-omgeving.

2 VOORWAARDEN VOOR TOETREDEN TOT VITALINK COT

Hier wordt dieper ingegaan op de verschillende voorwaarden.

2.1 Regelgeving

De voorziening onderschrijft volgende regelgeving. Consulteer steeds de laatste versie via onderstaande bronnen:

- http://www.ejustice.just.fgov.be/cgi/summary.pl
- http://www.codex.vlaanderen.be/

2.1.1 De wet verwerking persoonsgegevens (WVP)

De voorziening onderschrijft de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. Hierna “WVP” als afkorting voor de wet verwerking persoonsgegevens.

Zowel de rechten en plichten van de persoon wiens gegevens worden verwerkt als die van de verwerker van deze gegevens, werden in deze wet vastgelegd.

2.1.2 De wet patiëntenrechten (WPR)

De voorziening onderschrijft de wet van 22 augustus 2002 betreffende de rechten van de patiënt. Hierna “WPR” als afkorting voor de wet patiëntenrechten.

Hierin worden een aantal belangrijke rechten, van de zorggebruiker (patiënt/cliënt) en van de zorgverlener of hulpverlener (beroepsbeoefenaar), opgelijst.

Rechten van de zorggebruiker zijn:

1. het recht op een kwaliteitsvolle dienstverlening
2. het recht op vrije keuze van zorgverlener of hulpverlener
3. het recht op informatie over de gezondheidstoestand
4. het recht op toestemming na informatie
5. de rechten i.v.m. een patiëntendossier
6. het recht op bescherming van de persoonlijke levenssfeer
7. het recht om een klacht neer te leggen bij de bevoegde ombudsinstantie

De WPR regelt de rechten van een beperkte groep van patiënt. Voor Vitalink is er geen beperking, en gelden de rechten voor alle zorggebruikers (zowel zorg als welzijn).

2.1.3 Andere regelgeving of reglementeringen

- de wettelijke en reglementaire bepalingen met betrekking tot de uitoefening van de geneeskunde
- het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer http://codex.vlaanderen.be/Zoeken/Document.aspx?DID=1017242&param=informatie
- het besluit van de Vlaamse Regering van 15 mei 2009 betreffende veiligheidsconsulenten http://codex.vlaanderen.be/Zoeken/Document.aspx?DID=1018127&param=informatie
- het decreet van 13 juli 2012 houdende de oprichting en organisatie van een Vlaamse dienstenintegrator http://codex.vlaanderen.be/Zoeken/Document.aspx?DID=1021994&param=informatie

– de wettelijke en reglementaire bepalingen met betrekking tot het beroepsgeheim, met inbegrip van artikel 458 van het Strafwetboek
– het decreet van 25 april 2014 betreffende de organisatie van het netwerk voor de gegevensdeling tussen de actoren in de zorg http://www.codex.vlaanderen.be/Portals/Codex/documenten/1024441.html

2.2 Machtigingen van Commissie voor de bescherming van de persoonlijke levenssfeer

Indien van toepassing moet de voorziening beschikken over **de nodige machtigingen om persoonsgegevens te mogen verwerken**. Zij moet deze machtigingen aanvragen bij de Commissie voor de bescherming van de persoonlijke levenssfeer (hierna "CBPL") ook wel gekend als de Privacy Commissie. De CBPL werd, als onafhankelijk controleorgaan, door de WVP opgericht. Het ziet er op toe dat de persoonsgegevens zorgvuldig gebruikt en beveiligd worden, met als doel de privacy van de burgers te garanderen.

De CBPL bestaat uit verschillende sectorale comités. Deze sectorale comités zien er, in een specifieke sector, op toe dat de privacy bij de verwerking van persoonsgegevens beschermd wordt. Bepaalde verwerkingen zijn echter zo delicaat dat ze enkel mogelijk zijn indien daar, door het bevoegde Sectoraal comité, een specifieke toestemming (machtiging) voor gegeven wordt. Een voorbeeld hiervan is het Sectoraal comité van het Rijksregister dat aan een persoon of voorziening de toestemming (machtiging) kan verlenen om toegang te verkrijgen tot de informatie van het Rijksregister. De rol van dit Sectoraal comité werd bij wet[1] vastgelegd. Ook de rol van de andere Sectorale comités werd bij wet vastgelegd.

Meer informatie betreffende de CBPL kan u hier terugvinden.

2.2.1 Beraadslagingen Commissie voor de bescherming van de persoonlijke levenssfeer

Onderstaande beraadslagingen kunt u raadplegen op de website van het eHealth-platform. Deze zijn onderhevig aan wijzigingen. Consulteer daarom steeds de laatste versie op de website van het eHealth-platform: https://www.ehealth.fgov.be/nl/over-het-ehealth-platform/organisatie/sectoraal-comite/presentatie

Beraadslaging nr. 12/046 van 19 juni 2012 met betrekking tot de uitwisseling van gezondheidsgegevens via het Vitalink-platform

Beraadslaging nr 12/047 van 19 juni 2012 met betrekking tot de geïnformeerde toestemming van een betrokkene met de elektronische uitwisseling van zijn persoonsgegevens die de gezondheid betreffen en de wijze waarop deze toestemming kan worden geregistreerd.

Beraadslaging nr 11/088 van 18 oktober 2011 met betrekking tot de nota betreffende de elektronische bewijsmiddelen van een therapeutische relatie en van een zorgrelatie

Beraadslaging nr. 12/081 van 18 september 2012 met betrekking tot de mededeling van persoonsgegevens aan en door het eHealth-platform in het kader van de webtoepassing 'eHealthConsent' en webservice 'Therapeutic links management' en de webservice 'Consent Management'

Beraadslaging nr. 14/016 van 18 februari 2014 betreffende het reglement betreffende de uitwisseling van gezondheidsgegevens tussen gezondheidssystemen verbonden via het verwijzingsrepertorium van het eHealth-platform

[1] De Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen.

2.3 Toegang tot eHealth

De voorziening moet **een toegang aanvragen** tot de beveiligde onlinediensten van eHealth. Op volgende plaats kan hierover meer informatie worden teruggevonden.

De voorziening moet een toegangsbeheerder aanstellen. In het kader van eHealth spreekt men over **een Verantwoordelijke Toegangen Entiteit (VTE)**. De VTE is verantwoordelijk voor de toegangen van de voorziening tot de beveiligde onlinediensten van eHealth. Op volgende plaats kan hierover meer informatie worden teruggevonden.

2.4 Informatieveiligheidsbeleid

2.4.1 Veiligheidsplan

Onder een veiligheidsplan verstaan we een plan van aanpak / stappenplan om tot een informatieveiligheidsbeleid te komen en /of om het bestaande informatieveiligheidsbeleid te bewaken.

Het veiligheidsplan zal bestaan uit volgende elementen:

- strategische veiligheidsbeleid;
- operationeel veiligheidsbeleid, actuele situatie;
- operationeel veiligheidsbeleid, streefdoel;
- operationeel veiligheidsplan;
- eventuele auditverslagen.

2.4.1.1 Strategisch veiligheidsbeleid

Het strategisch veiligheidsbeleid geeft de strategische richtlijnen betreffende de beveiliging van de voorziening weer. Het is een goedgekeurd kader waarin elke werknemer van de voorziening alsook derde partijen in relatie ermee hun taken uitvoeren.

2.4.1.2 Operationeel veiligheidsbeleid, actuele toestand

Een operationeel veiligheidsbeleid implementeert het strategisch veiligheidsbeleid van de voorziening. Het omvat alle maatregelen, afspraken, … actueel van kracht binnen de voorziening die bij de dagelijkse werkzaamheden van kracht zijn in de context van informatiebeveiliging . Het operationeel veiligheidsbeleid wordt afgestemd op het kader dat geboden wordt door het strategisch veiligheidsbeleid en dient aan alle aandachtsdomeinen uit dit laatste een invulling te geven. (cfr. AS-IS)

2.4.1.3 Operationeel veiligheidsbeleid, streefdoel

De actuele invulling die aan het strategisch veiligheidsbeleid wordt gegeven is zelden de wenselijke eindsituatie en evenmin een stabiel gegeven (vooral ICT en organisatorische aspecten fluctueren) Naast de actuele situatie wordt ook gedocumenteerd welke het streefdoel is voor de voorziening. (cfr. TO-BE)

2.4.1.4 Operationeel veiligheidsplan

Het operationeel veiligheidsplan heeft als doel om de voorziening op een planmatige wijze te laten evolueren naar het streefdoel. Het operationeel veiligheidsplan documenteert welke implementatieaanpassingen, nieuwe afspraken, … zullen worden geïntroduceerd in de voorziening teneinde de veiligheidssituatie te verbeteren. Dit omvat een gedocumenteerde weerslag van:

- inventaris van verbeteracties
- prioritisatie ervan

- inplanning ervan

2.4.2 Informatieveiligheidsbeleid

Het informatieveiligheidsbeleid somt de fundamentele principes inzake informatieveiligheid op. De basis voor het veiligheidsbeleid is de ISO norm 27002.

U kan zich bij de opstelling van het veiligheidsbeleid baseren op het "Information Security Management System (ISMS)" zoals beschreven door de Kruispuntbank van de Sociale Zekerheid (KSZ).

Dit zijn de 12 minimale normen die we binnen het ISMS kunnen onderscheiden.

1. Risico bepaling
2. Beleid voor informatieveiligheid
3. Organisatie van de informatieveiligheid
4. Beheer van bedrijfsmiddelen
5. Medewerkers gerelateerde veiligheid
6. Fysieke beveiliging en omgevingsbeveiliging
7. Operationeel beheer
8. Logische toegangsbeveiliging
9. Ontwikkeling en onderhoud van systemen
10. Beheer van (informatieveiligheids-)incidenten
11. Continuïteitsbeheer
12. Naleving

Op volgende pagina kan u onderaan volgende relevante documenten terugvinden.

- Het document "Minimale Normen" beschrijft kort en overzichtelijk de minimumnormen van het informatieveiligheidsbeleid.
- Het document "Vragenlijst ter uitvoering van de minimale veiligheidsnormen" is een interessant evaluatiemiddel om te controleren of uw voorziening voldoet aan de minimale veiligheidsnormen.
- Het document "Beleid voor Informatieveiligheid" is een goed voorbeeld van een informatieveiligheidsbeleid.

2.4.3 Veiligheidsdienst en veiligheidsconsulent

Enkele belangrijke aandachtpunten in het informatieveiligheidsbeleid zijn:

- Er moet *een informatieveiligheidsdienst* ingericht worden.
- Er moet *een informatieveiligheidsconsulent* aangesteld worden. Deze persoon zal volgende taken vervullen:
  - het verstrekken van deskundige adviezen aan de persoon belast met het dagelijks bestuur;
  - het uitvoeren van opdrachten die hem door de persoon belast met het dagelijks bestuur worden toevertrouwd.
- Deze informatieveiligheidsconsulent zal de informatieveiligheidsdienst leiden.
- De identiteit van de informatieveiligheidsconsulent moet meegedeeld worden aan de toezichthoudende instellingen.

2.5 Verwerking van gegevens op afstand ('cloud')

De Werkgroep ICT van 3 december 2014 heeft een nota hierover besproken en goedgekeurd. Dit standpunt biedt een duidelijk kader waarbinnen informatie afkomstig uit Vitalink op afstand

mag verwerkt en eventueel opgeslagen worden. De voorziening die deel uit maakt van de Vitalink CoT dient dit standpunt te respecteren.

Vitalink Standpunt cloud vPublicatie.pd

2.6 Logische toegangsbeveiliging

De logische toegangsbeveiliging is een onderdeel van het informatieveiligheidsbeleid. De toegang tot de gegevens moet beveiligd zijn door middel van een identificatie-, authenticatie- en autorisatiesysteem. Dit betekent ook dat de voorziening er op toe kijkt dat de geldende regels, betreffende informed consent en therapeutische / zorgrelatie op elk moment en door alle zorgverleners of hulpverleners, gerespecteerd worden. In dit kader moet de voorziening te allen tijde kunnen voorzien in een geactualiseerde lijst van zorgverleners of hulpverleners met mogelijke toegang tot Vitalink. De voorziening moet ook in een procedure tot toegangslogging voorzien, alsook het beheren van deze logging gegevens. De gegevens die zo'n toegangslogging zeker moeten capteren zijn wie, heeft wat, wanneer gedaan en in welke context (waarom). De voorziening voorziet dus ook in een getrapt systeem van veiligheidslogging, zodat het steeds mogelijk is om vast te stellen wie welke gegevens geraadpleegd heeft. De voorziening moet de patiënt ook toegang geven tot de toegangslogging tot zijn gegevens. Ook in een onderzoeks- en tuchtprocedure, bij gemeld of verondersteld misbruik van toegang tot de gegevens, moet voorzien worden.

De voorziening is verantwoordelijk voor de interne organisatie van de identificatie, authenticatie en autorisatie van gebruikers. Hiervoor moet de voorziening beschikken over een informatieveiligheidsbeleid.

Zorg en Gezondheid is verantwoordelijk voor de organisatie van de identificatie, authenticatie en autorisatie van zorggebruikers, individuele zorgverleners of hulpverleners en voorzieningen op het Vitalink-platform.

2.6.1 Toegangsrechten

Bij de elektronische uitwisseling van gezondheids- en welzijnsinformatie zijn een adequate bescherming van de persoonlijke levenssfeer van de zorggebruiker (patiënt/cliënt) en een zeer degelijke informatieveiligheid uiteraard heel belangrijk. De maatregelen inzake bescherming van de persoonlijke levenssfeer en de informatieveiligheid moeten zodanig worden geïmplementeerd dat de risico's op onrechtmatig gebruik van de persoonsgegevens betreffende de gezondheid maximaal worden voorkomen, terwijl de nagestreefde voordelen inzake kwaliteit en continuïteit van de zorg, patiëntveiligheid en lastenvermindering worden bereikt. Daarom moet dus een goed evenwicht worden gevonden tussen informatieveiligheid en efficiënte gegevensuitwisseling.

De beperking van de toegangsrechten moet gebeuren op een manier die nog steeds de maximaal mogelijke kwaliteit van behandeling waarborgt.

Zelfs indien een zorgverlener of hulpverlener toegang heeft tot alle, dan wel bepaalde gezondheids- en welzijnsinformatie, mogen conform het finaliteits- en proportionaliteitsbeginsel enkel die gegevens worden gebruikt die relevant, noodzakelijk en pertinent zijn voor de concrete behandeling van de zorggebruiker (patiënt/cliënt) en voor het verzekeren van de continuïteit van de zorg.

De voorziening is verantwoordelijk voor de interne organisatie van een matrix voor regeling van de toegangsrechten. Hiervoor moet de voorziening beschikken over een logische toegangsbeveiliging als onderdeel van het informatieveiligheidsbeleid.

Zorg en Gezondheid is verantwoordelijk voor de organisatie van een matrix voor regeling van de toegangsrechten voor zorggebruikers, individuele zorgverleners of hulpverleners (op basis van hoedanigheid) en voorzieningen (op basis van type voorziening) op het Vitalink-platform.

2.6.2 Voorzien in een loggingsmechanisme

Het bijhouden van veiligheidsloggings is één van de maatregelen die veiligheid en de confidentialiteit van de gezondheids- en welzijnsinformatie garanderen. Met deze maatregel kan er controle worden uitgevoerd op de correcte werking van het toegangsbeheer en kunnen (pogingen tot) inbreuken worden gecontroleerd zowel door de beheerders in het kader van de correcte werking van het systeem als op vraag van de zorggebruiker (patiënt/cliënt) bij de uitoefening van zijn patiëntenrechten. Een dergelijk systeem moet steeds in staat zijn om vast te stellen wie welke gegevens heeft geraadpleegd.

De voorziening is verantwoordelijk voor de interne organisatie van een loggingsmechanisme voor zowel functionele als technische logging van het netwerk voor gezondheids- en welzijnsinformatie via het Vitalink-platform en betrokken ICT-oplossingen.

Zorg en Gezondheid is verantwoordelijk voor de organisatie van een loggingsmechanisme voor zowel functionele[2] als technische logging[3] van het Vitalink-platform.

2.6.3 Noodgevallen

In noodgevallen (bijvoorbeeld bij een spoedopname met levensbedreigende aandoening) kan het vereist zijn dat een zorgverlener of hulpverlener toegang krijgt tot gegevens van de zorggebruiker (patiënt/cliënt) zonder de informering van de zorggebruiker (patiënt/cliënt) of de aanwezigheid van een therapeutische-/zorgrelatie. Het gebruik van een dergelijke noodprocedure moet gemotiveerd en gelogd worden door de voorziening.

De zorggebruiker (patiënt/cliënt), of zijn vertegenwoordiger, dient aan de hand van de motivatie geïnformeerd te worden over wie zijn gezondheids- en welzijnsinformatie heeft geconsulteerd zonder de voorafgaandelijke informering of zonder de aanwezigheid van een therapeutische/zorgrelatie. Bijkomend dient de zorggebruiker (patiënt/cliënt), of zijn vertegenwoordiger geïnformeerd te worden waar hij een klacht kan neerleggen indien de inzage niet gerechtvaardigd kan worden. Bij deze informering kan worden verwezen naar de ombudsdiensten “Rechten van de zorggebruiker (patiënt/cliënt)” (http://www.patientrights.be) of de Privacy Commissie voor de regeling van geschillen.

2.7 Geïnformeerde toestemming binnen de voorziening

De procedure voor de geïnformeerde toestemming moet voorzieningen in staat stellen om een geïnformeerde toestemming van een patiënt te registeren. Eerst en vooral moet de patiënt ingeschreven zijn in de voorziening. De voorziening moet de patiënt, op een duidelijke en niet-technische manier, op de hoogte brengen van de gevolgen van deze toestemming. In dit kader moet ook het principe van opt-in belicht worden. Ook moet de procedure voor de intrekking van de geïnformeerde toestemming meegedeeld worden. De voorziening moet gebruik maken

[2] **Functionele logging**: Logging die inzicht geeft over de algemene werking van het netwerk voor gezondheids- en welzijnsinformatie, en bepaalde situaties die zich hebben voorgedaan. Bv. gegevens m.b.t. de eindgebruiker, uitgevoerde operatie, gebruik van bepaalde procedures, foutboodschappen, …

[3] **Technische logging**: Logging die bestaat uit logging van foutmeldingen (support), access log (toegang), security log (uitzonderingen), netwerk log (SLA).

van de door het eHealth-platform ter beschikking gestelde toepassing om de geïnformeerde toestemming te registeren.

Zonder de geïnformeerde toestemming mogen er geen gegevens over de patiënt in kwestie, tussen zorgverleners of hulpverleners, gedeeld worden.

De voorziening is verantwoordelijk voor de interne organisatie van de informering van de patiënt. De informering gebeurt bij voorkeur aan de hand van ***een informatiebrochure*.**

De elementen van informering zijn:

- vermelding van een verantwoordelijke
- vermelding van een contactpunt voor vragen en bijkomende informatie
- toelichting van de organisatie van verwerking van gezondheids- en welzijnsinformatie
- toelichting “Rechten van de patiënt”

Elke zorggebruiker moet een degelijk, begrijpbaar inzicht krijgen omtrent wie wanneer welke gezondheids- en welzijnsinformatie kan uitwisselen met wie en voor welke doeleinden. Bij de informering van de zorggebruiker dient de voorziening rekening te houden met de leeftijd, opleiding, psychische draagkracht, … van de zorggebruiker. In de communicatie dienen technische termen zo veel mogelijk vermeden te worden en op eenvoudig manier uitgelegd te worden. De zorggebruiker heeft daarbij steeds het recht vrij te beslissen of hij gegevensuitwisseling via het Vitalink-platform al dan niet toestaat. Bovendien heeft de zorggebruiker te allen tijde de mogelijkheid niet langer gegevens te delen via het Vitalink-platform.

2.8 Therapeutische / zorgrelatie

De gegevensdeling van gezondheidsgegevens via het Vitalink-platform vereist de voorafgaande verificatie van het bestaan van een therapeutische of zorgrelatie tussen de zorg-/welzijnsverlener die de gegevens deelt en de patiënt. Bij voorzieningen die vallen onder dit reglement gebeurt de controle door de voorziening, en niet langer door het Vitalink-platform.

De voorziening is verantwoordelijke voor de eigen interne organisatie van de registratie, uitsluiting, beheer en verificatie van de therapeutische-/zorgrelatie. De voorziening maakt gebruik van eigen specifieke gegevensbanken houdende therapeutische/zorgrelaties, of van gegevensbanken die toegankelijk zijn via een basisdienst van het eHealth-platform. Iedere handeling met betrekking tot de registratie, uitsluiting, beheer en verificatie van de therapeutische-/zorgrelatie moet worden gelogd.

De voorziening moet over een procedure beschikken om uitsluitingen te registeren en te implementeren. Onder *uitsluiting* verstaan we de mogelijkheid van de patiënt om een individuele zorgverlener of hulpverlener de toegang, tot zijn gezondheidsgegevens, te ontzeggen.

De voorziening respecteert de bepalingen van het Sectoraal comité van de Sociale Zekerheid en van de Gezondheid van de CBPL in zake wat de therapeutische-/zorgrelatie is, en welke de elektronische bewijsmiddelen zijn.

Zorg en Gezondheid is verantwoordelijk voor de organisatie van de verificatie van de therapeutische relatie tussen een zorggebruiker en een individuele zorgverlener of hulpverlener op het Vitalink-platform.

2.9 Klachtenrecht[4]

De patiënt heeft het recht om een klacht neer te leggen die betrekking heeft op de rechten zoals beschreven in de WPR, die door de zorggebruiker (patiënt/cliënt) kunnen worden uitgeoefend. Ook klachten die gestoeld zijn op vermeende medische fouten behoren tot de bevoegdheid van de ombudsfunctie.

De ombudsfunctie heeft volgende opdrachten:

- Het voorkomen van vragen en klachten door de communicatie tussen de zorggebruiker (patiënt/cliënt) en de zorgverlener of hulpverlener (beroepsbeoefenaar)
- Het bemiddelen bij klachten met het oog op het bereiken van een oplossing
- Het inlichten van de patiënt inzake de mogelijkheden voor de afhandeling van zijn klacht als er geen oplossing wordt bereikt
- Het verstrekken van informatie over de organisatie, de werking en de procedureregels van de ombudsfunctie
- Het formuleren van aanbevelingen om herhaling te voorkomen van tekortkomingen die aanleidingen kunnen geven tot een klacht

Niet alleen de patiënt maar ook de benoemde vertegenwoordiger[5], de samenlevende echtgenoot, de wettelijk samenwonende partner of feitelijk samenwonende partner, een meerderjarig kind, een ouder, een meerderjarige broer of zus, kunnen een klacht neerleggen bij de ombudsfunctie.

2.10 Interne organisatie van de voorziening

Er moet een contactpersoon voor technische problemen aangesteld worden. Deze persoon fungeert als single point of contact (SPOC) binnen de voorziening voor wat betreft technische problemen. Onder technische problemen verstaan we problemen met betrekking tot de gebruikte ICT oplossing (bv. trage verbinding, technische foutboodschappen, …).

De voorziening moet een contactpersoon (SPOC) voor inhoudelijke (functionele) problemen aanstellen. Onder functionele problemen verstaan we problemen met betrekking tot de inhoud van de gegevens in de applicatie (bv. foutieve of ontbrekende gegevens).

2.11 Opleiding / informatie verdeling

Er moeten opleidingen voorzien worden voor de zorgverleners of hulpverleners binnen de voorziening. Deze opleidingen moeten het gebruik van de informatieoplossing verduidelijken, alsook de gebruikers op hun rechten en plichten wijzen. Het veiligheidsbeleid mag hier zeker ook kort toegelicht worden. De voorziening brengt de patiënt op de hoogte van zijn rechten.

[4] Het klachtenrecht wordt beschreven in art. 11 van de WPR.

[5] De **benoemde vertegenwoordiger** wordt beschreven in art. 14 § 1 van de WPR. Een benoemde vertegenwoordiger is een door de patiënt voorafgaandelijk aangewezen persoon, die in de plaats van de patiënt zal treden. Dit indien en zolang de patiënt niet in staat is zijn rechten zoals beschreven in de WPR uit te oefenen. De benoemde vertegenwoordiger zal dan deze rechten uitoefenen. De aanwijzing van deze persoon gebeurt met een gedagtekend en door de patiënt en deze persoon ondertekend bijzonder schriftelijk mandaat waaruit de toestemming van deze persoon blijkt.