|  |
| --- |
|  |
| **NOTA**  |
| Toetreden tot de BelRAI circle of trust: toelichting bij de checklist BelRAIVersie 06/10/2015  |

# Regelgeving

De voorziening onderschrijft volgende regelgeving.

## 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](http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=1992120832). 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.

## De wet patiëntenrechten (WPR)

De voorziening onderschrijft [de wet van 22 augustus 2002 betreffende de rechten van de patiënt.](http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2002082245) 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 (zie ook **bijlage** 1 en 2):

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 ombudsdienst.

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

## Beraadslagingen Commissie voor de bescherming van de persoonlijke levenssfeer

Onderstaande beraadslagingen kunt u raadplegen op de [website](https://www.ehealth.fgov.be/nl/over-het-ehealth-platform/organisatie/sectoraal-comite/presentatie) van het eHealth-platform.

[Beraadslaging nr. 09/018 van 19 mei 2009, laatst gewijzigd op 19 mei 2015, met betrekking tot de uitwisseling van persoonsgegevens die de gezondheid betreffen tussen de betrokken zorgverstrekkers en de database BelRAI met tussenkomst van het eHealth-platform](https://www.ehealth.fgov.be/sites/default/files/assets/nl/pdf/sector_committee/2015/09-018-n085-belrai_gewijzigd_op_19_mei_2015.pdf)

Beraadslaging nr 11/088 van 18 oktober 2011, gewijzigd op 9 juni 2015, met betrekking tot de nota betreffende de elektronische bewijsmiddelen van een therapeutische relatie en van een zorgrelatie.

Beraadslaging nr. 14/016 van 18 februari 2014, gewijzigd op 9 juni 2015, betreffende het reglement betreffende de uitwisseling van gezondheidsgegevens tussen gezondheidssystemen verbonden via het verwijzingsrepertorium van het eHealth-platform.

## Andere regelgeving of reglementeringen

* de wettelijke en reglementaire bepalingen met betrekking tot de uitoefening van de geneeskunde
* de wettelijke en reglementaire bepalingen met betrekking tot het beroepsgeheim, met inbegrip van artikel 458 van het Strafwetboek

# Machtigingen van Commissie voor de bescherming van de persoonlijke levenssfeer

## De voorziening beschikt over de nodige machtigingen

De voorziening moet 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 de Sociale Zekerheid & Gezondheid. Dit Comité beschermt de privacy van de verzekerden binnen het Belgische socialezekerheidsnetwerk bij de verwerking van hun persoonsgegevens, en houdt bijzonder toezicht op de mededeling van gezondheidsgegevens. Het Comité bestaat uit 2 afdelingen, nl. afdeling Sociale Zekerheid en afdeling Gezondheid. De rol van dit Sectoraal comité werd bij wet vastgelegd. Het Sectoraal comité van de Sociale Zekerheid en van de Gezondheid is binnen de Commissie opgericht door de Belgische Wet van 15 januari 1990.

Meer informatie betreffende de CBPL kan u [hier](http://www.privacycommission.be/nl/) terugvinden.

# Toegang tot eHealth

## De voorziening beschikt over een eHealth certificaat

De voorziening moet **een toegang aanvragen** tot de beveiligde onlinediensten van eHealth. Op volgende [plaats](https://www.ehealth.fgov.be/nl/support/basisdiensten/ehealth-certificaten) kan hierover meer informatie worden teruggevonden.

## De voorziening heeft een toegangsbeheerder aangesteld

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](https://www.ehealth.fgov.be/nl/basisdiensten/geintegreerd-gebruikers-en-toegangsbeheer/presentatie) kan hierover meer informatie worden teruggevonden.

# Informatieveiligheidsbeleid

## 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.

#### 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.

#### 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)

#### 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)

#### 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

## Informatieveiligheidsbeleid

Het informatieveiligheidsbeleid somt de fundamentele principes inzake informatieveiligheid op. De basis voor het veiligheidsbeleid is de [ISO norm 27002](http://en.wikipedia.org/wiki/ISO/IEC_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](http://www.ksz-bcss.fgov.be/nl/bcss/page/content/websites/belgium/security/security_04/security_04_02.html) 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.

## 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.

# Logische toegangsbeveiliging

## Procedure inzake beveiligde toegang tot gegevens

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.

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

In het bijzonder ziet de voorziening erop toe dat de toegang die ze haar zorgverleners verleent tot de gegevens van de BelRAI vragenlijsten, de toegangsrechten respecteert zoals bepaald in de BelRAI privacy commissie machtiging[[1]](#footnote-1), toegangsmatrices op pagina’s 36-40.

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

## Geactualiseerde lijst van zorgverleners

In dit kader moet de voorziening te allen tijde kunnen voorzien in een geactualiseerde lijst van zorgverleners of hulpverleners met mogelijke toegang tot BelRAI.

## Toegangslogging

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.

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 BelRAI-platform en betrokken ICT-oplossingen.

BelRAI is verantwoordelijk voor de organisatie van een loggingsmechanisme in het BelRAI-platform.

## Onderzoeks- en tuchtprocedure

De voorziening moet voorzien in een onderzoeks- en tuchtprocedure, bij gemeld of verondersteld misbruik van toegang tot de gegevens.

## Zorggebruiker toegang geven tot toegangslogging

De voorziening moet de patiënt ook toegang geven tot de toegangslogging tot zijn gegevens.

# Geïnformeerde toestemming binnen de voorziening

## De voorziening beschikt over documentatie betreffende de geïnformeerde toestemming en het opt-in principe

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 BelRAI-platform al dan niet toestaat. Bovendien heeft de zorggebruiker te allen tijde de mogelijkheid niet langer gegevens te delen via het BelRAI-platform.

## De voorziening beschikt over een procedure voor de registratie van de geïnformeerde toestemming

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.

## De voorziening beschikt over een procedure voor de intrekking van de geïnformeerde toestemming

Ook moet de procedure voor de intrekking van de geïnformeerde toestemming meegedeeld worden.

# Therapeutische / zorgrelatie

## De voorziening beschikt over een procedure voor de registratie, uitsluiting, beheer en verificatie van de therapeutische / zorgrelatie

De gegevensdeling van gezondheidsgegevens via het BelRAI-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 gebruik maken van de BelRAI web service gebeurt de controle door de voorziening, en niet langer door het BelRAI-platform.

De voorziening is verantwoordelijk 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.

BelRAI is verantwoordelijk voor de organisatie van de registratie van de therapeutische relatie tussen een zorggebruiker en een individuele zorgverlener of hulpverlener op het BelRAI-platform.

# Klachtenrecht[[2]](#footnote-2)

## De voorziening voldoet aan het klachtenrecht zoals beschreven in de wet patiëntenrechten

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[[3]](#footnote-3), 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.

# Interne organisatie van de voorziening

## De voorziening stelt een contactpersoon voor technische problemen aan

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 stelt een contactpersoon voor inhoudelijke (functionele) problemen aan

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).

# Opleiding / informatie verdeling

## De voorziening organiseert opleidingen voor zorgverstrekkers binnen de voorziening

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 verdeelt informatie en doet aan public relations naar zorggebruikers (patiënten/cliënten), alle medewerkers, andere belanghebbenden

## De voorziening brengt de zorggebruiker (patiënt/cliënt) op de hoogte van zijn rechten

De voorziening brengt de patiënt op de hoogte van zijn rechten. Een goed hulpmiddel hierbij is de brochure van de FOD Volksgezondheid.

1. [Beraadslaging nr. 09/018 van 19 mei 2009, laatst gewijzigd op 19 mei 2015, met betrekking tot de uitwisseling van persoonsgegevens die de gezondheid betreffen tussen de betrokken zorgverstrekkers en de database BelRAI met tussenkomst van het eHealth-platform](https://www.ehealth.fgov.be/sites/default/files/assets/nl/pdf/sector_committee/2015/09-018-n085-belrai_gewijzigd_op_19_mei_2015.pdf) [↑](#footnote-ref-1)
2. Het klachtenrecht wordt beschreven in art. 11 van de WPR. [↑](#footnote-ref-2)
3. 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. [↑](#footnote-ref-3)