|  |
| --- |
|  |
| **OVEREENKOMST**  |
| Overeenkomst voor het toetreden tot de BelRAI Circle Of Trust  BelRAI03.05.2017  |

**Overeenkomst betreffende het gebruik van de BelRAI web services voor gegevensdeling met zorginstellingen en -Organisaties**

Tussen

“**De Belgische Staat**”, vertegenwoordigd door Pedro Facon, Directeur-generaal Gezondheidszorg, Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, hierna genoemd “**De Staat**”,

enerzijds

en

“**de voorziening**” zijnde <naam voorziening> met KBO-nummer <nummer>, <adres>, <Riziv-nummer(s)>, vertegenwoordigd door <naam & functie>, hierna genoemd “de voorziening”,

anderzijds

wordt als volgt overeengekomen:

## Art. 1.

Onder “**strategisch ICT-veiligheidsbeleid**” wordt verstaan: het veiligheidsbeleid, opgebouwd en onderhouden door de voorziening, dat zich conformeert aan de ISO27002-norm.

Onder “**de toepassing**” wordt verstaan BelRAI. BelRAI is een digitaal platform voor het registreren en delen van zorgevaluaties volgens de interRAI instrumenten.

## Art. 2

Deze overeenkomst kan geen afbreuk doen aan de Wet Verwerking Persoonsgegevens, aan de wet van 22 augustus 2002 betreffende de rechten van de patiënt, aan de wettelijke en reglementaire bepalingen met betrekking tot de uitoefening van de geneeskunde, aan de wettelijke en reglementaire bepalingen met betrekking tot het beroepsgeheim, met inbegrip van artikel 458 van het Strafwetboek.

## Art. 3.

Met behoud van de toepassing van artikel 16, §4, van de Wet Verwerking persoonsgegevens, bepaalt de voorziening en, in voorkomend geval, de zorgverleners of de hulpverleners, 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 zorg betrokken zijn, rekening houdend met de functie van die personen, de aard van de gegevens en de potentiële risico’s die eraan verbonden zijn, alsook de bepalingen van deze overeenkomst. De voorziening neemt die regeling op in een strategisch ICT-veiligheidsbeleid, conform aan de ISO27002-norm.

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-2), toegangsmatrices op pagina’s 36-40.

De voorziening verklaart kennis te hebben van de inhoud van de ISO27002-norm en aanvaardt deze als strategische norm voor zijn strategisch ICT-veiligheidsbeleid. De voorziening zal zijn eigen veiligheidsbeleid en de bijhorende implementatie dan ook conformeren aan deze norm.

Naast die keuze voor de voornoemde ICT-veiligheidsnorm zal de voorziening de nodige operationele maatregelen nemen teneinde een afdoende implementatie te voorzien voor de diverse aandachtsgebieden uit die norm.

De voorziening stelt een veiligheidsbeleid op, aangevuld met de wijze waarop de zorggebruiker geïnformeerd wordt over zijn rechten in kader van deze overeenkomst en de rol die de informatieveiligheidsconsulent opneemt.

Hiertoe wordt door de voorziening minimaal onderstaande documentatie opgebouwd en onderhouden, telkens conform de ISO27002-norm:

* operationeel ICT-veiligheidsbeleid, actuele toestand: daarin zal de voorziening de actuele toestand van de genomen ICT-veiligheidsimplementatie documenteren;
* operationeel ICT-veiligheidsbeleid, streefdoel: daarin zal de voorziening de toestand documenteren waarheen gestreefd wordt voor de toekomst;
* operationeel ICT-veiligheidsplan: daarin zal de voorziening aanduiden welke acties hij in het kader van de ICT-veiligheid voor een termijn van 3 jaar prioritair zal uitvoeren en welke de voorziene planning daarbij is.

## Art 4.

Iedere voorziening wijst, al dan niet onder zijn medewerkers, een informatieveiligheidsconsulent aan, overeenkomstig artikel 8, §2, en 10 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en overeenkomstig artikel 9 van de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen.

De identificatie (naam, voornaam, rijksregisternummer) en de functie (overeenkomst) van de informatieveiligheidsconsulent, alsook elke wijziging wordt meegedeeld aan de Staat.

## Art. 5.

De voorziening verbindt zich er in het kader van BelRAI specifiek toe om op eenvoudige aanvraag van De Staat, volgende gegevens permanent ter beschikking te houden:

* de identiteit van de gebruikers van de toepassing;
* de netwerkapparatuur van de omgeving voor zover die relevant is in het kader van BelRAI en de toepassing(en) die met BelRAI gegevens uitwisselen;
* elke gegevensuitwisseling door eindgebruikers betreffende persoonsgegevens in het kader van BelRAI moet terug traceerbaar zijn en kan worden opgevraagd.

## Art. 6.

De voorziening verklaart steeds toegankelijk te zijn voor een audit door de door hem aangeduide informatieveiligheidsconsulent. Die audit wordt al dan niet voorafgaand aangekondigd.

## Art. 7.

Het operationeel veiligheidsbeleid moet door de voorziening onderhouden worden. De voorziening verbindt zich ertoe om de door hem aangeduide informatieveiligheidsconsulent:

* elke belangrijke wijziging aan het operationeel veiligheidsbeleid zo snel mogelijk te bezorgen;
* minstens jaarlijks (in januari) een update van het operationeel veiligheidsbeleid te bezorgen, vergezeld van een nieuw operationeel ICT-veiligheidsplan;
* een jaarlijks activiteitenverslag te laten maken met vermelding van de acties die werden ondernomen om de informatieveiligheid optimaal uit te bouwen en te handhaven, van het aantal en de scope van controles en de reacties en het gevolg dat daaraan werd gegeven.

## Art. 8.

De door de voorziening aangeduide informatieveiligheidsconsulent verzekert de opvolging van die afspraken alsook de goede werking van het ICT-veiligheidsbeleid, inclusief de implementatie daarvan.

Voor die taken rapporteert en adviseert de informatieveiligheidsconsulent zo nodig rechtstreeks aan het leidinggevend management van de voorziening.

De voorziening neemt hierbij ook kennis van het feit dat de informatieveiligheidsconsulent geen (ICT-) eindverantwoordelijkheid kan dragen binnen de voorziening. De verantwoordelijkheid van de informatieveiligheidsconsulent behelst zijn opdracht om de voorziening correct op te volgen en waar nodig kwaliteitsvolle adviezen aan te bieden. De voorziening verbindt zich ertoe om op een dergelijk advies te reageren binnen een termijn van vier weken.

## Art. 9.

De voorziening gaat ermee akkoord dat patiëntgegevens, die ze naar BelRAI doorstuurt, mogelijk in gecodeerde vorm naar interRAI worden gestuurd (steeds binnen de geldende privacy regels) en vergewist zich ervan dat de patiënten er voorafgaandelijk en expliciet mee hebben ingestemd dat hun gegevens kunnen gebruikt worden voor wetenschappelijk onderzoek.

De voorziening vergewist zich ervan dat elke cliënt, voor wie gegevens worden doorgestuurd naar BelRAI, een geïnformeerd toestemmingsformulier heeft ondertekend. Dit formulier is in lijn met het BelRAI “informed consent” formulier, en vermeldt dat gegevens met de BelRAI overheidsdatabank zullen worden uitgewisseld.

## Art. 10.

De voorziening onderschrijft dat de overheidsdatabank BelRAI de centrale authentieke bron is voor BelRAI beoordelingen. Ze zorgt ervoor dat gegevens worden uitgewisseld met een voldoende frequentie. De laatste volledige versie van het assessment dient zich altijd in de BelRAI-databank te bevinden en dit binnen de 24u nadat er gegevens geregistreerd zijn.

**Art. 11.**

In geval van rapportering van incidenten die kunnen gemeld worden door patiënten, familieleden, zorgverleners, koepelorganisaties, patiëntenverenigingen, informatieveiligheidsconsulenten, … gelden de volgende regels :

1. De BelRAI circle of trust-beheerder rapporteert het incident bij de BelRAI informatieveiligheidsconsulent.
2. De BelRAI circle of trust-beheerder, met de informatieveiligheidsconsulent in een adviserende rol, onderzoekt het incident.
3. Indien het incident wijst op een ernstige tekortkoming in de ICT toepassing die met BelRAI web service koppelt, of op het niet-naleven van de voorwaarden gesteld in het cookbook:
4. vraagt de BelRAI circle of trustbeheerder aan de BelRAI helpdesk om de ICT toepassing met onmiddellijke ingang te schrappen uit de lijst van erkende toepassingen binnen de BelRAI Circle of trust.
5. Brengt de BelRAI circle of tust-beheerder de ICT ontwikkelaar hiervan op de hoogte.
6. Om terug te kunnen toetreden tot de BelRAI Circle of trust, dient de ICT ontwikkelaar het probleem te remediëren en daarna opnieuw de volledige procedure te doorlopen om terug tot de Circle of trust te kunnen worden toegelaten.
7. Indien het incident wijst op een ernstige tekortkoming in het veiligheidsbeleid van de zorginstelling, of op het niet-naleven van de voorwaarden gesteld in de checklist voor voorzieningen:
8. vraagt de BelRAI circle of trust-beheerder aan de BelRAI helpdesk om de zorginstelling met onmiddellijke ingang te schrappen uit de BelRAI Circle of trust whitelist
9. Brengt de BelRAI circle of trust-beheerder de zorginstelling hiervan op de hoogte.
10. Om terug te kunnen toetreden tot de BelRAI Circle of trust, dient de zorginstelling het probleem te remediëren en daarna opnieuw de volledige procedure te doorlopen om terug tot de Circle of trust te kunnen worden toegelaten.

## Art. 12.

Deze overeenkomst kan door beide partijen, met een opzegtermijn van 3 maanden opgezegd worden. De opzegging geschiedt schriftelijk met vermelding van de reden van opzegging.

Deze overeenkomst werd opgemaakt in drie exemplaren, waarvan elke onderschrijvende partij verklaart één te hebben ontvangen alsook een exemplaar voor de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL).

In geval er door de Belgische Staat een wijzigingsclausule wordt voorgesteld bij deze overeenkomst heeft de voorziening 1 maand de tijd om zich hiertegen te verzetten. In dat geval vervalt de overeenkomst binnen de 3 maand die volgt op de datum waarop de wijzigingsclausule aan de voorziening werd overgemaakt.

Opgemaakt te Brussel,

Voor <naam voorziening> Voor de Belgische Staat

<naam> Pedro Facon

<functie> Directeur-generaal Gezondheidszorg

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-2)