Privacyreglement

Register Leren van data in Verpleeghuizen

Versie 1.0

13 December 2021

Toelichting

Doel

De doelstelling van het Register Leren van data in Verpleeghuizen (RLV) is het tot stand brengen en onderhouden van een geïntegreerde infrastructuur op basis van routinematig door specialisten ouderengeneeskunde geregistreerde gegevens waarmee het mogelijk is om landelijke gegevens in de ouderengeneeskunde eenduidig te ontsluiten ten behoeve van wetenschappelijk onderzoek van de gezondheidszorg, waaronder begrepen wetenschappelijk onderzoek dat beoogt bij te dragen aan het kwaliteitsbeleid. Om dit doel te bereiken wordt Spiegelinformatie verstrekt aan de bij de Deelnemende verpleeghuisorganisaties werkzame specialisten ouderengeneeskunde.

Het Register Leren van data in Verpleeghuizen is een data-infrastructuur waarin routine zorgdata bij elkaar worden gebracht, uitgevoerd door het Consortium Leren van Data bestaande uit Verenso, UNO Amsterdam en het Nivel, waarbij het Nivel de technisch operationeel uitvoerder van het register is. De invoer en uitvoer van gegevens in het register wordt nauw met de betrokken partijen afgestemd. Hoe dat voor het Register Leren van data in Verpleeghuizen in zijn werk gaat, is beschreven in het Governancedocument. Dit Privacyreglement is een bijlage bij het Governancedocument en maakt daarvan een onverbrekelijk deel uit.

Verkrijging gegevens

De gegevens binnen het Register Leren van data in Verpleeghuizen worden geëxtraheerd op basis van een Minimale Data Set (MDS) bestaande uit gegevens die routinematig door specialisten ouderengeneeskunde worden vastgelegd in het elektronisch patiëntendossier (EPD). Het betreft gegevens van de op naam ingeschreven bewoners van de Deelnemende verpleeghuisorganisaties.

Volgens de besluitvorming beschreven in het Governancedocument kunnen ook andere gegevensbronnen, in voorkomende gevallen op individueel niveau, onder pseudoniem aan de MDS gegevens uit het Register Leren van data in Verpleeghuizen gekoppeld worden, zodat uitspraken gedaan kunnen worden over kenmerken en het zorggebruik van de verpleeghuispopulatie. Dit kan met inachtneming van de privacyaspecten ten aanzien van de te koppelen gegevens gebeuren.

Gebruik Trusted Third Party (TTP)

Bij de gegevensverwerking voor het Register Leren van data in Verpleeghuizen wordt gebruik gemaakt van pseudonimisering door een Trusted Third Party, waardoor uitsluitend gepseudonimiseerde gegevens in het Register Leren van data in Verpleeghuizen worden opgenomen. Bij pseudonimiseren[1]

[1] Artikel 4 lid 5 AVG definieert pseudonimiseren als: 'Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld'.

worden persoonsgegevens verwerkt zonder dat daarbij duidelijk wordt over welke personen de gegevens gaan. Na pseudonimisering zijn de gegevens alleen nog herleidbaar tot een specifiek persoon als er gebruik wordt gemaakt van aanvullende gegevens. De Algemene Verordening Gegevensbescherming (AVG) is ook van toepassing op de gepseudonimiseerde gegevens.

De werkwijze van de TTP is in grote lijnen als volgt. De eerste versleuteling van de identificerende gegevens van Verpleeghuisbewoners vindt plaats bij het elektronisch dossiersysteem van de Deelnemende verpleeghuisorganisatie. Vervolgens vindt een tweede versleuteling door de TTP plaats voordat de gegevens aan het Nivel worden verstrekt.
De procedure voor het verwerken van gegevens voor het Register Leren van data in Verpleeghuizen is zodanig ingericht dat in het register herleiding van gegevens naar individuele verpleeghuisbewoners redelijkerwijs wordt voorkomen. Toch is niet uit te sluiten dat in bepaalde gevallen van indirect identificerende gegevens moet worden gesproken. Dat betreft dan het 'aggregatieniveau'[2] van de gegevens die aan een pseudoniem zijn gekoppeld. Bepaalde 'bijzondere' bewoners[3] van de Deelnemende verpleeghuisorganisaties zullen mogelijk indirect herleidbaar kunnen worden geacht. Het zou een ernstige belemmering opleveren voor het wetenschappelijk onderzoek dat met het Register Leren van data in Verpleeghuizen moet worden gedaan, indien een deel van de gegevens nog globaler moet worden gemaakt teneinde deze zeldzame mogelijkheid tot herleiding te vermijden. Dit is in overeenstemming met de richtlijnen in de Federa-COREON Gedragscode Gezondheidsonderzoek.[4]
Omdat het niet uit te sluiten is dat in bepaalde gevallen van indirect identificerende gegevens moet worden gesproken vallen de gegevens in het Register Leren van data in Verpleeghuizen onder het regime van de AVG en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). Het Register Leren van data in Verpleeghuizen verzamelt geen NAW-gegevens of geboortedata.
Mede daarom is, in het belang van de bescherming van de persoonlijke levenssfeer, aansluitend op het Governancedocument, de wijze waarop de gegevensverwerking plaatsvindt en de verantwoordelijkheden van de betrokken partijen daarbij in dit privacyreglement vastgelegd.

Inhoud reglement

In dit reglement wordt beschreven hoe de gegevens voor het Register Leren van data in Verpleeghuizen worden verkregen en vervolgens verwerkt, welke organisatorische en technische maatregelen zijn getroffen ter bescherming van de persoonlijke levenssfeer van betrokken personen en welke procedures worden gevolgd ter effectuering van deze maatregelen.

De afspraken tussen het Nivel en de Deelnemende verpleeghuisorganisaties zijn neergelegd in een Deelnemersovereenkomst. De governancestructuur is beschreven in het Governancedocument.

Dit reglement is vastgesteld door de consortiumpartijen vertegenwoordigd in de Stuurgroep.

---

[2] Zie voor dit begrip E.B. van Veen. Patient data for health research. MedLawconsult, Den Haag, 2011.
[3] Bijvoorbeeld een zeer hoge of juist jonge leeftijd en een bijzonder medisch beeld zou bij Deelnemende verpleeghuisorganisatie met relatief weinig verpleeghuisbewoners mogelijk tot indirecte herleidbaarheid kunnen leiden.

[4] Gedragscode van de Nederlandse biomedische onderzoeksgemeenschap goedgekeurd door het College

Bescherming Persoonsgegevens in 2004. http://www.federa.org/sites/default/files/bijlagen/coreon/gedragscode_gezondheidsonderzoek.pdf

Artikel 1 – Definities
In dit privacyreglement wordt uitgegaan van de volgende definities, telkens geschreven met een hoofdletter:

Governancedocument	**:** het Governancedocument van het Register Leren van data in Verpleeghuizen waarvan dit privacyreglement een bijlage is;
Deelnemende verpleeghuisorganisatie	**:** alle verpleeghuisorganisaties waarmee een Deelnemersovereenkomst is gesloten;
Verpleeghuisbewoner(s)	**:** alle verpleeghuisbewoners, of de vertegenwoordigers van deze bewoners, zoals omschreven in artikel art. 7:465 lid 3 BW (Wgbo), die op naam zijn ingeschreven bij de Deelnemende verpleeghuisorganisatie en waarvan de specialist ouderengeneeskunde behandelaar is.
Privacycommissie	**:** de Privacycommissie van het Register Leren van data in Verpleeghuizen, bestaande uit een Functionaris Gegevensbescherming, een Security Officer en een onafhankelijk jurist.
Deelnemers-overeenkomst	: de overeenkomst tussen het Nivel en de Deelnemende verpleeghuisorganisatie waarin de rechten en plichten van deze partijen in het kader van het Register Leren van data in Verpleeghuizen zijn beschreven;
Spiegelinformatie	**:** de door het Nivel aan de bij de Deelnemende verpleeghuisorganisatie werkzame specialisten ouderengeneeskunde te verstrekken informatie, bestaande uit een vergelijking van de cijfers van de ontvangende specialisten ouderengeneeskunde uit het Register Leren van data in Verpleeghuizen met referentiegegevens uit het Register Leren van data in Verpleeghuizen. De referentiegegevens in de Spiegelinformatie zijn niet herleidbaar tot natuurlijke personen i.c. individuele Verpleeghuisbewoners, andere individuen of organisaties.
Gegevens	**:** de Gegevens die voor het Register Leren van data in Verpleeghuizen worden verwerkt;
Beoordelingscommissie	**:** de Beoordelingscommissie Register Leren van data in Verpleeghuizen, zoals beschreven in het Governancedocument;
Trusted Third Party (TTP)	**:** de partij die de door de Deelnemende verpleeghuisorganisaties aan te leveren Gegevens pseudonimiseert voordat deze aan het Nivel worden verstrekt;
Register Leren van data in Verpleeghuizen	: het Register Leren van data in Verpleeghuizen, zoals beschreven in het Governancedocument;
Stuurgroep	**:** de Stuurgroep van het Register Leren van data in Verpleeghuizen, zoals beschreven in het Governancedocument;

Artikel 2 – Doelstelling en Verwerkingsverantwoordelijkheid

2.1 De doelstelling van het Register Leren van data in Verpleeghuizen is het tot stand brengen en onderhouden van een geïntegreerde infrastructuur op basis van routinematig door specialisten ouderengeneeskunde geregistreerde gegevens waarmee het mogelijk is om landelijke gegevens in de ouderengeneeskunde eenduidig te ontsluiten ten behoeve van wetenschappelijk onderzoek van de gezondheidszorg, waaronder begrepen wetenschappelijk onderzoek dat beoogt bij te dragen aan het kwaliteitsbeleid. Om dit doel te bereiken wordt Spiegelinformatie verstrekt aan de bij de Deelnemende verpleeghuisorganisaties werkzame specialisten ouderengeneeskunde.

2.2 Voor zover binnen het Register Leren van data in Verpleeghuizen persoonsgegevens worden verwerkt, zijn de consortiumpartners vertegenwoordigd in de Stuurgroep gezamenlijk verantwoordelijk zoals bedoeld in artikel 26 AVG voor het vaststellen van het doel en middelen van het RLV. Het Nivel is als technisch operationeel uitvoerder verantwoordelijk voor de feitelijke verwerking van (persoons)gegevens die binnen de infrastructuur van het RLV verwerkt worden. Het Nivel draagt daarbij zorg en verantwoordelijkheid dat de Gegevens, of dat nu persoonsgegevens zijn of niet, uitsluitend worden verwerkt, zoals in dit reglement is bepaald en vormt het eerste aanspreekpunt voor vragen van betrokkenen en instanties, zoals de Autoriteit Persoonsgegevens.

Artikel 3 – Verzamelen van Gegevens

3.1 De wettelijke grondslag voor het verzamelen van de gegevens voor de consortiumpartners van het programma Leren van Data is voor het Nivel en Verenso dat de gegevens noodzakelijk zijn voor de behartiging van een gerechtvaardigd belang van deze Partijen(artikel 6 lid 1 sub f AVG) en voor UNO Amsterdam dat de gegevens noodzakelijk zijn voor vervulling van een taak van algemeen belang (artikel 6 lid 1 sub e).

Er kan volgens de Autoriteit Persoonsgegevens sprake zijn van een gerechtvaardigd belang van de samenleving bij wetenschappelijk activiteiten.[5] Het belang van Partijen bij het RLV is om de uitvoering van wetenschappelijk onderzoek dat beoogt bij te dragen aan kwaliteitsverbetering in de verpleeghuiszorg mogelijk te maken. In het kader van het programma Leren van Data is een basisgegevensset (de MDS) ontwikkeld gericht op het mogelijk maken van kennisontwikkeling en kwaliteitsverbetering. Daarvoor zijn gegevens geselecteerd t.b.v. het RLV die noodzakelijk zijn om dit doel te kunnen bereiken. Daarbij zal per onderzoeksaanvraag of gegevensaanvraag middels de opgetekende governance van het programma worden bekeken welke gegevens noodzakelijk zijn en zullen alleen die gegevens of rapportages worden verstrekt die voor de betreffende vraag nodig zijn.

Er zijn diverse maatregelen genomen om de inbreuk op de privacy van de betrokkenen zo beperkt mogelijk te houden. Door het pseudonimiseren zijn de gegevens niet of alleen in zeer uitzonderlijke situaties te herleiden tot de betrokkenen. Daarnaast is een strikt informatiebeveiligingsbeleid conform ISO 27001 opgezet en is er een governancestructuur ingericht waarbinnen ook wordt toegezien op de naleving van wet- en regelgeving. Bovendien hebben betrokkenen steeds de mogelijkheid om bezwaar te maken tegen het gebruik van hun

[5] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf

gegevens. Gelet op deze maatregelen en het feit dat het belang bij wetenschappelijk onderzoek groot is en voor een zeer grote groep mensen (in de toekomst) grote voordelen kan opleveren, staat het doel in verhouding tot de inbreuk op de privacy van betrokkenen.
De grondslag voor het doorbreken van het verbod op het verwerken van gegevens inzake de gezondheid, artikel 9 lid 1 AVG, is de uitzonderingsgrond voor wetenschappelijk onderzoek (artikel 9 lid 2 sub j AVG jo artikel 24 UAVG).

3.2 De Deelnemende Verpleeghuisorganisaties leveren de Gegevens betreffende de verpleeghuisbewoners uit het elektronisch dossiersysteem gepseudonimiseerd aan de TTP ten behoeve van het Register Leren van data in Verpleeghuizen. De TTP versleutelt deze Gegevens een tweede maal voordat deze worden verstrekt aan het Nivel. De technische aspecten van deze systematiek zijn gedetailleerd beschreven in bijlage 1 van dit reglement.

3.3 De in het vorige lid genoemde procedure leidt er in beginsel toe dat uitsluitend Gegevens vanuit het elektronisch dossiersysteem van de Deelnemende verpleeghuisorganisaties worden verwerkt die niet of niet zonder onevenredige tijd en moeite herleidbaar zijn tot geïdentificeerde of identificeerbare natuurlijke personen.

3.4 Voor de doelstelling van het Register Leren van data in Verpleeghuizen zoals genoemd in artikel 2.1 wordt evenwel niet uitgesloten dat over bepaalde Verpleeghuisbewoners vanuit het dossiersysteem indirect identificerende Gegevens worden verzameld.

3.5 De Deelnemende verpleeghuisorganisatie zal alle betrokken Verpleeghuisbewoners informeren over de gegevensverwerking van (mogelijk) niet volstrekt anonieme Gegevens ten behoeve van de doelstellingen van het Register Leren van data in Verpleeghuizen zoals beschreven in artikel 2.1 van dit reglement. De Deelnemende verpleeghuisorganisatie zal de Verpleeghuisbewoner verzoeken toestemming te geven voor het gebruik van zijn gegevens voor het Register Leren van data in Verpleeghuizen, zoals bepaald in artikel 7:457 BW (WGBO) dan wel zal de verpleeghuisorganisatie de Verpleeghuisbewoners de mogelijkheid geven om bezwaar te maken tegen de gegevensverwerking.[6] De Stuurgroep draagt zorg voor toegankelijk voorlichtingsmateriaal over het Register Leren van data in Verpleeghuizen en over dit privacyreglement, dat door het Nivel aan de Deelnemende verpleeghuisorganisaties kan worden verstrekt.

3.6 Zoals ook geregeld in de Deelnemersovereenkomst vindt geen verstrekking van Gegevens aan het Register Leren van data in Verpleeghuizen plaats indien de Verpleeghuisbewoner van de Deelnemende verpleeghuisorganisatie hiervoor geen toestemming heeft gegeven of hiertegen bezwaar heeft gemaakt als bedoeld in artikel 3.5.

3.7 Naast in beginsel Gepseudonimiseerde Gegevens over bewoners van de Deelnemende verpleeghuisorganisaties worden ook Gegevens over de organisaties of hun medewerkers zelf verzameld. De aard van deze Gegevens en de wijze van verzamelen wordt steeds vastgesteld zoals bepaald in het Governancedocument. De Deelnemende verpleeghuisorganisaties blijven in het Register Leren van data in Verpleeghuizen identificeerbaar. De verwerking en eventuele uitvoer van zulke Gegevens geschiedt uitsluitend zoals in dit privacyreglement is bepaald.

[6] Zoals bepaald in artikel 7:458 BW (WGBO). Dit artikel is in overeenstemming met art.9 lid 2 sub a AVG jo. art. 6 lid 1 sub a AVG en art. 89 lid 1 AVG.

Artikel 4 – Verwerken van Gegevens

4.1 De Gegevens worden uitsluitend verwerkt voor de doeleinden zoals bepaald in art. 2 van dit reglement.

4.2 Gegevens uit het Register Leren van data in Verpleeghuizen kunnen worden verrijkt met gegevens uit andere registraties, waarbij de bepalingen uit dit privacyreglement en het Governancedocument onverkort van kracht blijven op de Gegevens uit het Register Leren van data in Verpleeghuizen. Hiertoe kan slechts worden overgegaan na een besluit van de Stuurgroep naar aanleiding van het oordeel van de Beoordelingscommissie en de Privacycommissie zoals bepaald in het Governancedocument.

4.3 Persoonsgegevens worden alleen verwerkt binnen de Europese Economische Ruimte (EER).

4.4 Bij de verwerking van gegevens binnen het Register Leren van data in Verpleeghuizen is op geen enkele wijze sprake van geautomatiseerde besluitvorming.

Artikel 5 - Uitvoer uit het Register Leren van data in Verpleeghuizen

5.1 De uitvoer uit het Register Leren van data in Verpleeghuizen in welke vorm dan ook, zoals rapporten, artikelen, statistische overzichten, etc. is steeds zodanig dat individuele betrokkenen e.g. Verpleeghuisbewoners daarin volstrekt niet herleidbaar zijn.

5.2 De uitvoer is tevens zodanig dat de Deelnemende verpleeghuisorganisaties en de bij de Deelnemende verpleeghuisorganisaties werkzame specialisten ouderengeneeskunde daarin voor elke ander dan de Deelnemende verpleeghuisorganisaties en de daar werkzame specialisten zelf niet herkenbaar herleidbaar zijn.

Artikel 6 - Gebruik van Gegevens voor onderzoek

6.1 Onderzoeksgroepen (bij externe instellingen of van een van de leden van het Consortium Leren van Data) kunnen bij het Nivel een aanvraag indienen om van de Gegevens gebruik te maken voor door deze onderzoeksgroep voorgenomen onderzoek. Het Nivel kan nadere regels stellen voor het doen van de gegevensaanvraag en de daarin opgenomen beschrijving van het onderzoek, alvorens de gegevensaanvraag ter beoordeling wordt voorgelegd aan de Beoordelingscommissie en, indien van toepassing, de Privacycommissie.

6.2 Over het uitleveren van gegevens aan derden (volgens de procedure beschreven in het Governancedocument) beslist de Stuurgroep, na ontvangst van het oordeel van de Beoordelingscommissie en, indien van toepassing, de Privacycommissie. De Stuurgroep kan alleen besluiten tot uitleveren van de gegevens na een positieve beoordeling van de gegevensaanvraag door de Beoordelingscommissie. Een goedgekeurde aanvraag leidt tot een overeenkomst tussen de aanvrager en het Nivel waarin de termijnen voor het onderzoek, de wijze van ontsluiten van de Gegevens, levering van de daaruit voortvloeiende resultaten, de kosten, auteursrechtelijke aspecten en dergelijke worden vastgelegd.

6.3 De voor het goedgekeurde onderzoek benodigde verwerking van Gegevens wordt in beginsel uitgevoerd door medewerkers van het Nivel. Bij de in het vorige lid bedoelde overeenkomst kan evenwel worden bepaald dat onderzoekers van de onderzoeksinstelling onder begeleiding van deze medewerkers rechtstreeks toegang hebben tot de Gegevens. Het Nivel ziet er op toe dat de uitvoer voldoet aan het in artikel 5 gestelde.

6.4 De aanvrager kan kosten verschuldigd zijn voor de behandeling van de aanvraag en bij goedkeuring van deze voor het ontsluiten van de Gegevens,

Artikel 7 - Veiligheid van de Gegevens

7.1 De Gegevensverwerking ten behoeve van het Register Leren van data in Verpleeghuizen voldoet aan de daaraan te stellen veiligheidseisen. Bij het informatiebeveiligingsbeleid worden de daarop van toepassing zijnde ISO27001 en NEN7510 en de hierbij behorende normen en NTA's , voor zover deze van toepassing zijn op partijen, gevolgd. Indien het Nivel voor (onderdelen van) het Register Leren van data in Verpleeghuizen een verwerker zal inschakelen, zullen gelijke veiligheidseisen aan de verwerker worden gesteld en in een verwerkersovereenkomst worden vastgelegd.

7.2 Van elke verwerking met betrekking tot een gegevensaanvraag binnen in het Register Leren van data in Verpleeghuizen en de daartoe uitgevoerde bewerkingen en van elke uitvoer uit het Register Leren van data in Verpleeghuizen wordt aantekening gehouden via een systeem van logfiles.

7.3 Uitsluitend daartoe specifiek gemachtigde medewerkers van het Nivel of daartoe gemachtigde onderzoekers onder begeleiding van een medewerker van het Nivel hebben rechtstreeks toegang tot de Gegevens. De toegang dient uitsluitend om Gegevens ten behoeve van onderzoek te verwerken of voor onderhoud van het register. Dit zijn twee onderscheiden functies en medewerkers kunnen niet beide vervullen. Deze medewerkers en gemachtigde onderzoekers hebben een schriftelijke geheimhoudingsverklaring ondertekend.

Artikel 8 - Privacycommissie

8.1 Een Privacycommissie houdt toezicht op de werking van het Register Leren van data in Verpleeghuizen. De samenstelling, taken en bevoegdheden van deze commissie zijn in het Governancedocument van het Register Leren van data in Verpleeghuizen beschreven.

Artikel 9 - Betrokkenen

9.1 Een betrokkene kan de toestemming intrekken voor de verwerking van Gegevens die op hem betrekking hebben of bezwaar maken tegen de verwerking van Gegevens die op hem betrekking hebben. Er zullen dan geen gegevens van deze betrokkene door de deelnemende verpleeghuisorganisatie aan het Nivel worden geleverd. Gelet op de pseudonimiseringsprocedures kan de betrokkene uitsluitend bij de Deelnemende verpleeghuisorganisatie de toestemming intrekken of bezwaar maken tegen verdere verwerking. Een verzoek van een betrokkene hiertoe zal daarom door het Nivel, met toestemming van de betrokkene, worden doorgestuurd naar de Deelnemende verpleeghuisorganisatie of de betrokkene zal worden verzocht zijn of haar verzoek aan de verpleeghuisorganisatie te richten.

9.2 Omdat de Gegevens die tot aan het verzoek van de betrokkene tot het intrekken van de toestemming voor verwerking of het maken van bezwaar tegen de verwerking van gegevens zijn

verzameld, eerder kunnen zijn gebruikt voor onder meer wetenschappelijke publicaties en deze langdurig moeten kunnen worden gevalideerd, kunnen de eerder verwerkte Gegevens conform artikel 17 lid 3 sub d AVG niet uit de onderzoeksbestanden worden verwijderd.

9.3 Ten aanzien van toekomstige verwerking van de Gegevens die tot het intrekken van de toestemming voor verwerking of het maken van bezwaar tegen de verwerking van Gegevens zijn verzameld en de overige in artikel 15 tot en met 20 AVG opgenomen rechten voor betrokkenen geldt dat, ook al is wellicht sprake van indirect identificerende Gegevens binnen het Register Leren van data in Verpleeghuizen, de medewerkers van het Nivel een betrokkene niet zonder onevenredige tijd en moeite zullen kunnen terugvinden, behalve als de betrokkene aanvullende gegevens verstrekt die het mogelijk maken hem of haar te identificeren. Het Register Leren van data in Verpleeghuizen, voldoet daarmee aan artikel 11 AVG, waarmee art. 15 t/m art. 20 AVG dan ook niet van toepassing zijn op de gepseudonimiseerde gegevens in het Register Leren van data in Verpleeghuizen tenzij de betrokkene aanvullende gegevens aan het Nivel verstrekt waarmee hij of zij kan worden geïdentificeerd.

9.4 Indien er een klacht bestaat met betrekking tot het Register Leren van data in Verpleeghuizen dan wordt deze klacht afgehandeld door het Nivel.

Artikel 10 - Duur van het Register Leren van data in Verpleeghuizen

10.1 Het Register Leren van data in Verpleeghuizen blijft in stand gedurende de looptijd van het programma Leren van Data. Over het verlengen of het eventuele opheffen van het Register Leren van data in Verpleeghuizen nadien beslist de Stuurgroep in overleg met de overige gremia van de governancestructuur.

Artikel 11 - Bijlagen

11.1 Bijlage 1 is de technische beschrijving van het verzamelen van Gegevens als bedoeld in art. 3.2 en de rol van de TTP. Deze bijlage kan op ondergeschikte punten worden aangepast als de stand van de techniek daartoe aanleiding geeft.

Artikel 12 - Inwerkingtreding en geldingsduur

12.1 Wijzigingen van dit privacyreglement kunnen door de Stuurgroep alleen worden doorgevoerd met goedkeuring van de Privacycommissie. De Beoordelingscommissie wordt in kennis gesteld van de gewijzigde versie. Wijzigingen van het privacyreglement worden gepubliceerd op *https://www.nivel.nl/nl/register-leren-van-data-verpleeghuizen*.

12.2 Dit reglement is op 13 december 2021 door de consortiumpartners vertegenwoordigd in de Stuurgroep vastgesteld. Dit reglement geldt gedurende de looptijd van het Register Leren van data in Verpleeghuizen of tot het moment waarop een opvolgend reglement wordt vastgesteld.

Bijlage 1 bij Privacyreglement Register Leren van data in Verpleeghuizen

Technische beschrijving pseudonimisatie gegevensverzameling

Pseudonimisatie

Onder 'pseudonimisatie' verstaan wij het omzetten van een persoonsgegeven naar een niet- herleidbare code. De omzettingen zijn, in de door ZorgTTP gehanteerde variant, onomkeerbaar. Het is daarbij onmogelijk een pseudoniem terug te vertalen naar het oorspronkelijke persoonsgegeven.

De kerntaak van ZorgTTP is het depersonaliseren van bestanden om daarmee het uitwisselen van informatie op individueel niveau, conform de wettelijke vereisten, mogelijk te maken. De verzendende partij (de bron) en de ontvangende partij (het doel) maken gezamenlijk afspraken over welke informatie wordt uitgewisseld en welke gegevens daarbij dienen te worden geanonimiseerd. ZorgTTP zal een adviserende rol spelen bij deze afweging als onderdeel van de werkzaamheden die horen bij het inrichten van een pseudonimisatieketen.

De omzetting verloopt in twee stappen: de partij die in het bezit is van de te verzenden (persoons)gegevens (de bron) maakt gebruik van pseudonimisatiesoftware waarmee een persoonsgegeven wordt omgezet naar een zogenaamd pre-pseudoniem. Volgens wordt als tweede stap in het proces het pre-pseudoniem door de TTP, met behulp van software, omgezet naar een definitief pseudoniem. Dit pseudoniem, en de bijbehorende overige data, worden beschikbaar gesteld aan de ontvangende partij (het doel).

Alleen de TTP weet op welke wijze het definitieve pseudoniem is aangemaakt. Daarmee wordt een situatie bereikt waarbij het voor zowel de bron als het doel (de ontvangende partij) onmogelijk is om het oorspronkelijke persoonsgegeven met het aangemaakte pseudoniem in verband te brengen. Persoons-identificerende kenmerken zoals naam en BSN worden bij pseudonimisatie vervangen door een pseudoniem, zodanig dat voor ieder persoonsgegeven steeds hetzelfde pseudoniem wordt gegenereerd. Individuen worden op deze wijze koppelbaar in tijd en over verschillende bronnen heen zonder dat daartoe de oorspronkelijke persoonsgegevens verstrekt hoeven te worden. Door tussenkomst van de TTP zijn bron en doel niet in staat om persoonsgegeven en het daar uit resulterende pseudoniem aan elkaar te relateren.

De inzet van pseudonimisatie via ZorgTTP werkt via een gelaagd model. Hierin worden een aantal vormen van beveiliging gehanteerd. Het gaat om maatregelen op de volgende niveaus:

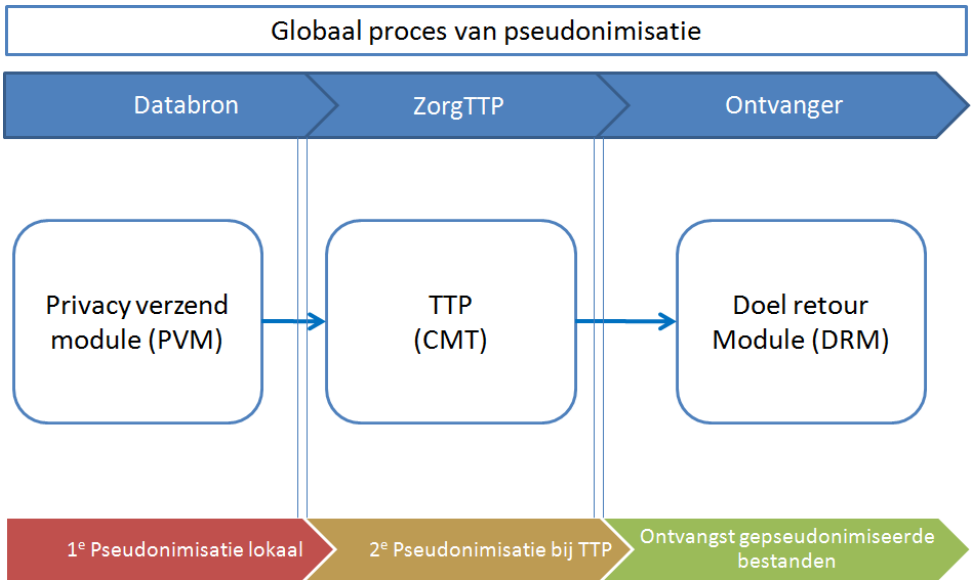
1. Pseudonimisatie op recordniveau
2. Versleuteling op bestandsniveau
3. Transportbeveiliging
4. Controle afzender middels certificaat

Op de volgende pagina wordt het pseudonimisatieproces schematisch weergegeven en toegelicht.

Beschrijving van het pseudonimisatieproces

De pseudonimisatieketen bestaat uit drie onderdelen:

1. Privacy- en Verzend Module (PVM) wordt door de informatiebron gebruikt om de bestanden te pseudonimiseren en te verzenden;
2. Centrale Module TTP (CMT) wordt door ZorgTTP gebruikt;
3. Doel- en Receive Module (DRM) wordt door het informatiedoel gebruikt om de bestanden vanaf de server van ZorgTTP te downloaden.



Het pseudonimisatieproces bestaat in het kort uit de volgende stappen:

1. Uitgangspunt is dat de verzendende partij (de zorgverlener) een bestand genereert dat voldoet aan vooraf vastgestelde specificaties;
2. Het bestand wordt verwerkt met de door ZorgTTP aan de databron beschikbaar gestelde software;
3. Na verwerking volgt beveiligd transport naar ZorgTTP voor het aanmaken van de definitieve pseudoniemen;
4. ZorgTTP voert met behulp van eigen pseudonimisatiesoftware centraal een tweede bewerking uit waarbij een voor de zender en ontvanger geheime ‘sleutel’ wordt gebruikt;
5. Het gepseudonimiseerde bestand wordt vrijgegeven en kan vervolgens worden opgehaald door de ontvangende partij met een daartoe beschikbaar gestelde ontvangstmodule.

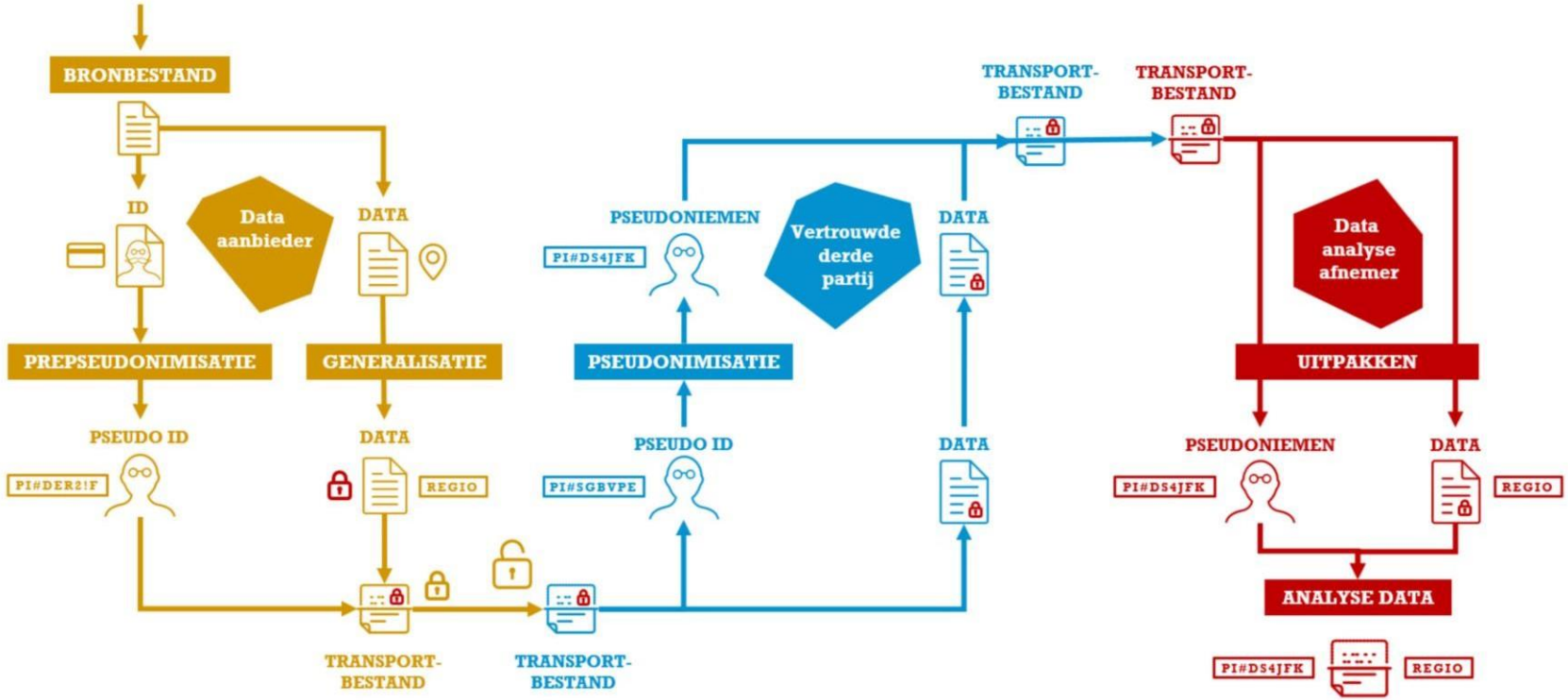
Op de volgende twee pagina’s wordt het pseudonimisatieproces schematisch weergegeven en gedetailleerder beschreven.

Beveiliging van informatie

ZorgTTP stelt de databron software ter beschikking voor de eerste bewerking. Daarbij worden persoonsgegevens omgezet naar pseudoniemen, ook wordt het bestand geanonimiseerd. Bijvoorbeeld door het omzetten van een geboortedatum naar een leeftijdscategorie. De medisch inhoudelijke informatie wordt vervolgens versleuteld, deze informatie is voor ZorgTTP gedurende het transport ontoegankelijk. Vanwege logistieke voordelen worden de pseudoniemen én inhoudelijke data in één levering via ZorgTTP aan de ontvanger aangeboden.

Uitwisseling van gegevens tussen de diverse partijen vindt plaats over beveiligde internetverbindingen (TLS). De identiteit van partijen wordt gevalideerd middels digitale certificaten (Public Key Infrastructure (PKI)).

In onderstaand figuur zijn de berichtstromen opgenomen en op de volgende pagina wordt een toelichting op het figuur gegeven.



Privacy- en Verzend Module (PVM)

Deze module wordt gebruikt door de bron en kent een aantal functies. Allereerst wordt een aantal controles uitgevoerd op de aangeboden gegevens. Daarna worden de identificerende persoonsgegevens omgezet in zogenaamde pre-pseudoniemen. Pre-pseudoniemen zijn persoonsgegevens waarop een eerste bewerking heeft plaatsgevonden. Vervolgens wordt een scheiding aangebracht tussen de pseudoniemen (sleuteldeel) en de bijbehorende data (datadeel). Beide delen worden vervolgens geëncrypteerd. Het sleuteldeel kan enkel worden gedecrypteerd door ZorgTTP, het datadeel enkel door de uiteindelijke ontvanger.

Voordat van een onomkeerbaar pseudoniem gesproken kan worden, dient de TTP een definitieve omzetting te doen op de voorbewerkte gegevens. De gegevens worden op beveiligde wijze naar de TTP verstuurd. Daarbij zijn de gegevens zodanig beveiligd dat deze slechts voor de TTP toegankelijk zijn voor verdere bewerking. De hiertoe benodigde op Java gebaseerde software wordt via het internet beschikbaar gesteld en maakt gebruik van door de TTP uitgegeven digitale certificaten. De digitale certificaten worden gebruikt voor ondertekening van de te verzenden berichten, het opbouwen van een beveiligde (HTTPS-) verbinding en encryptie van de te verzenden data.

Centrale Module TTP (CMT)

De centrale applicatie ontvangt een versleuteld bestand. Dit bestand bestaat uit twee onderdelen: een datadeel en een sleuteldeel. Het sleuteldeel bevat de pre-pseudoniemen, deze worden door de centrale applicatie omgezet tot de definitieve pseudoniemen.

De centrale applicatie heeft geen toegang tot het datadeel, deze is beveiligd en enkel door de ontvangstapplicatie te decrypteren. Voor de transportbeveiliging wordt ook weer gebruik gemaakt van een Public Key Infrastructure (PKI).

Doel- en Retour Module (DRM)

De ontvangstmodule wordt gebruikt door de ontvangende partij. De module ontvangt van de centrale applicatie de berichten. De berichten hebben een multipart-xml-indeling. Het is feitelijk een container met daarin bestanden. De module ontsleutelt allereerst het sleuteldeel, vervolgens het datadeel en voegt deze daarna weer samen. Afhankelijk van de grootte van het bestand kost dit proces enkele seconden tot een minuut.

Herleidbaarheid gepseudonimiseerde gegevens

Voor het verwerken van persoonsgegevens is de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (Algemene verordening gegevensbescherming) van toepassing.

Op het moment dat persoonsgegevens worden verwerkt stelt de AVG eisen aan het verwerken van die persoonsgegevens, zoals het treffen van passende organisatorische en technische beveiligingsmaatregelen. Privacy Enhancing Technology (PET) is een verzamelnaam voor die maatregelen. Een vorm van PET is het pseudonimiseren van persoonsgegevens. De opgeslagen gegevens blijven een zekere mate van gevoeligheid behouden, zeker in het geval van medische gegevens. Dit komt omdat door het koppelen van gepseudonimiseerde dataverzamelingen of door het toevoegen van aanvullende variabelen alsnog op indirecte wijze sprake kan zijn van tot persoonsgegevens herleidbare data. Door middel van pseudonimisatie wordt de directe herleidbaarheid van persoonsgegevens tegengegaan en is daarmee een sterke beveiligingsmaatregel om ongewenste herleiding tegen te gaan getroffen. Verder is het van verplicht om naast het inzetten van pseudonimisatie gegevens te verwerken op basis van een grondslag uit de AVG. Daarbij hoort ook het informeren van betrokkenen over het doel van de verwerking en de middelen die worden ingezet om misbruik tegen te gaan.

Om de kans op indirecte herleidbaarheid te minimaliseren adviseert ZorgTTP om:

- Gegevens waar mogelijk op geaggregeerd niveau te verstrekken;
- Per gepseudonimiseerde dataverzameling met een andere geheime sleutelwaarde te werken. Daarmee wordt directe koppeling op grond van de pseudoniemen onmogelijk;
- Gepseudonimiseerde data op het laagste aggregatieniveau alleen op basis van een overeenkomst te verstrekken;
- Gepseudonimiseerde data op het laagste aggregatieniveau uit andere gepseudonimiseerde dataverzamelingen alleen toe te voegen na analyse van het risico op directe op indirecte herleidbaarheid.

ISO Certificering 27001 voor Informatiebeveiligingsbeleid

ISO 27001 is gericht op het informatiebeveiligingsbeleid. Deze ISO norm stelt eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van het Information Security Management Systeem (ISMS). ZorgTTP heeft een up to date ISMS en er heeft mei 2018 een certificerende audit plaatsgevonden. ZorgTTP is door de certificerende partij KIWA voorgedragen voor certificering, wat inhoudt dat ZorgTTP verwacht per juli 2018 officieel gecertificeerd te zijn.

NIVEL
Kennis voor betere zorg

UNO Amsterdam
universitair netwerk ouderenzorg

verenso
vereniging van specialisten
ouderengeneeskunde