Privacyreglement
met technische toelichting pseudonimisering

NIVEL Zorgregistraties eerste lijn

Versie 2.1
Datum: 7 mei 2014
Documentnaam:
Privacyreglement met toelichting pseudonimisering v2.1 20140507

Toelichting

Doel
De doelstelling van NIVEL Zorgregistraties eerste lijn is het verwerken van gegevens over morbiditeit en de door de Deelnemers geboden zorg en de financiering van deze ten behoeve van wetenschappelijk onderzoek van de gezondheidszorg, waaronder begrepen wetenschappelijk onderzoek dat beoogt bij te dragen aan het kwaliteitsbeleid van de betrokken disciplines; wetenschappelijke vraagstellingen op het gebied van het gezondheidszorgbeleid; beleidsinformatie voor bij de zorg betrokken organen, zoals het Ministerie van VWS, beleid- of beroepsorganisaties of patiëntenorganisaties, een en ander zoals bepaald in het Governance-document en het verstrekken van Spiegelinformatie aan de Deelnemers.

NIVEL Zorgregistraties eerste lijn is de opvolger van de registraties die het NIVEL voor een aantal disciplines voerde. Evenals de voorheen bestaande registraties wordt de invoer en uitvoer van gegevens nauw met de betrokken disciplines afgestemd. Hoe dat voor NIVEL Zorgregistraties eerste lijn in zijn werk gaat, is beschreven in het Governance-document. Dit document is als bijlage bij dit Privacyreglement gevoegd en maakt daarvan een onverbrekelijk deel uit.

Verkrijging gegevens
De informatie uit NIVEL Zorgregistraties eerste lijn is gebaseerd op gegevens die primair routinematig in de eerstelijnszorg worden geregistreerd. Dat betreft gegevens van de volgende zorgverleners of zorgorganisaties: huisartsenpraktijken, gezondheidscentra, zorggroepen, fysiotherapeuten, oefentherapeuten Cesar/Mensendieck, diëtisten, logopedisten, eerstelijnspsychologen en huisartsendienstenstructuren.

Volgens de besluitvorming beschreven in het Governance-document zullen daartoe de verschillende gegevensbronnen in voorkomende gevallen, op patiëntniveau, onder pseudoniem aan elkaar gekoppeld kunnen worden, zodat uitspraken gedaan kunnen worden over het totale zorggebruik van een populatie van ongeveer 400.000 mensen.

Gebruik Trusted Third Party (TTP)
Ook de gegevensverwerking wordt bij NIVEL Zorgregistraties eerste lijn anders ingericht dan bij de voorheen bestaande NIVEL registraties, met additionele privacywaarborgen. Bij de gegevensverwerking wordt bij NIVEL Zorgregistraties eerste lijn gebruik gemaakt van een Trusted Third Party waardoor in beginsel uitsluitend anonieme gegevens in NIVEL Zorgregistraties eerste lijn worden opgenomen.
De werkwijze van de TTP is in grote lijnen als volgt. De eerste versleuteling van de identificerende gegevens van patiënten/cliënten vindt plaats bij de Deelnemer. Vervolgens vindt een tweede versleuteling bij de TTP plaats voordat de gegevens aan het NIVEL worden verstrekt. Deze tweede versleuteling is voor elke discipline uniek. De TTP heeft een procedure waardoor in

voorkomende gevallen een set gegevens tussen de onderscheiden disciplines kan worden gekoppeld.
De gehele procedure is zodanig ingericht dat in NIVEL Zorgregistraties eerste lijn in beginsel niet langer sprake is van persoonsgegevens in de zin van de Wet bescherming persoonsgegevens (Wbp). Toch is niet uit te sluiten dat in bepaalde gevallen van indirect identificerende gegevens moet worden gesproken. Dat betreft dan het 'aggregatieniveau'[1] van de gegevens die aan een pseudoniem zijn gekoppeld. Met name wanneer gegevens worden onderzocht van zorg aan patiënten tussen de verschillende disciplines. Dat zou in bepaalde gevallen voor bepaalde patiënten 'indirect identificerende gegevens' kunnen opleveren. Ook zouden bepaalde 'bijzondere' patiënten[2] van de Deelnemers mogelijk indirect herleidbaar kunnen worden geacht. Het zou een ernstige belemmering opleveren voor het wetenschappelijk onderzoek dat met NIVEL Zorgregistraties eerste lijn mogelijk moet worden gemaakt, indien een deel van de gegevens nog globaler moet worden gemaakt teneinde deze zeldzame mogelijkheid tot herleiding te vermijden. Het NIVEL handelt hiermee volgens de richtlijnen in de Code Goed Gedrag[3] die is goedgekeurd door het College Bescherming Persoonsgegevens.

Mede daarom is het van belang om in het kader van de bescherming van de persoonlijke levenssfeer aansluitend op het Governance-document afspraken te maken over wijze waarop de gegevensverwerking plaatsvindt en de verantwoordelijkheden van de betrokken partijen daarbij.

Inhoud Reglement
In dit reglement wordt beschreven hoe de gegevens voor NIVEL Zorgregistraties eerste lijn 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 Deelnemers zijn neergelegd in een Samenwerkingsovereenkomst. De governance-structuur is beschreven in het Governance-document.

Dit reglement is vastgesteld door de directie van het NIVEL, gehoord de Stuurgroep NIVEL Zorgregistraties eerste lijn zoals omschreven in het Governance-document.

[1] Zie voor dit begrip E.B. van Veen. Patiënt data for health research. MedLawconsult, Den Haag, 2011.
[2] Bijvoorbeeld een zeer hoge of juist jonge leeftijd en een medisch beeld dat niet bij die leeftijd past, zoals heupvervanging bij patiënten ouder dan 90 jaar. In relatie met de bekendheid bij het NIVEL van de Deelnemer zou dat bij Deelnemers met relatief weinig patiënten mogelijk tot indirecte herleidbaarheid kunnen leiden. Globaler maken of het verhogen van het aggregatieniveau zou betekenen dat men dan de leeftijd aanpast tot vanaf 85 jaar of wellicht nog lager teneinde de eventuele mogelijkheid van herleidbaarheid te minimaliseren.
[3] Gedragscode van de Nederlandse biomedische onderzoeksgemeenschap goedgekeurd door het College Bescherming Persoonsgegevens in 2004.
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:

Governance-document	:	het Governance-document NIVEL Zorgregistraties eerste lijn (opgenomen als bijlage 1);
Deelnemers	:	alle individuele beroepsbeoefenaren of rechtspersonen van een bepaalde Discipline die hebben toegezegd gegevens aan NIVEL Zorgregistraties eerste lijn te leveren;
Discipline	:	een binnen de eerste lijn werkzame beroepsgroep of type zorg-organisatie waarvoor binnen NIVEL Zorgregistraties eerste lijn een aparte deelregistratie is ingesteld;
Patiënten	:	alle patiënten of cliënten die zijn ingeschreven bij of zorg ontvangen van een Deelnemer;
Samenwerkings-overeenkomst	:	de overeenkomst tussen het NIVEL en de Deelnemer waarin de rechten en plichten van het NIVEL en de Deelnemer in het kader van NIVEL Zorgregistraties eerste lijn zijn beschreven;
Spiegelinformatie	:	de door het NIVEL aan de Deelnemer te verstrekken informatie, bestaande uit een vergelijking van de cijfers van de praktijk van de Deelnemer met referentiegegevens van de andere Deelnemers van dezelfde Discipline. De Gegevens in de Spiegelinformatie zijn niet herleidbaar tot Patiënten of andere individuele Deelnemers, uitgezonderd die binnen de praktijk van de Deelnemer. Zie http://www.nivel.nl/dossier/spiegelinformatie
Gegevens	:	de Gegevens die voor NIVEL Zorgregistraties eerste lijn worden verwerkt;
Stuurgroep	:	de Stuurgroep NIVEL Zorgregistraties eerste lijn, zoals beschreven in het Governance-document;
Kamer	:	het overlegorgaan, zoals beschreven in het Governance-document NIVEL Zorgregistraties eerste lijn, waarbinnen per beroepsgroep beslissingen worden genomen ten aanzien van de Gegevens van die beroepsgroep;
Trusted Third Party (TTP)	:	de partij die de door de Deelnemer aan te leveren Gegevens *pseudonimiseert* voordat deze aan het NIVEL worden verstrekt;
NIVEL Zorgregistraties eerste lijn	:	de NIVEL Zorgregistraties eerste lijn, zoals beschreven in het Governance-document.

Artikel 2 – Doelstelling en Verantwoordelijke

2.1 De doelstelling van NIVEL Zorgregistraties eerste lijn is het verwerken van Gegevens over morbiditeit en de door de Deelnemers geboden zorg en de financiering van deze, ten behoeve van:
   a. wetenschappelijk onderzoek van de gezondheidszorg, waaronder begrepen wetenschappelijk onderzoek dat beoogt bij te dragen aan het kwaliteitsbeleid van de betrokken Disciplines;
   b. wetenschappelijke vraagstellingen op het gebied van het gezondheidszorgbeleid;
   c. beleidsinformatie voor bij de zorg betrokken organen, zoals het Ministerie van VWS, beleid- of beroepsorganisaties of patiëntenorganisaties, een en ander zoals bepaald in het Governance-document;
   d. Spiegelinformatie voor de Deelnemers.

2.2 Voor zover binnen NIVEL Zorgregistraties eerste lijn persoonsgegevens worden verwerkt, is het NIVEL verantwoordelijke voor de gegevensverwerking in de zin van de Wet bescherming persoonsgegevens. Het NIVEL draagt er zorg voor dat de Gegevens, of dat nu persoonsgegevens zijn of niet, uitsluitend worden verwerkt, zoals in dit Reglement is bepaald.

Artikel 3 – Verzamelen van Gegevens

3.1 Gegevens kunnen op 3 manieren worden verkregen:
   a. Vanuit de dossiersystemen van de Deelnemers;
   b. Vanuit door de Deelnemers beantwoorde vragen;
   c. Vanuit door de Patiënten beantwoorde vragen.

3.2 Verzamelen van Gegevens uit het elektronisch dossiersysteem van de Deelnemer geschiedt zodanig dat vanuit het dossiersysteem gepseudonimiseerde Gegevens worden aangeleverd aan de TTP. 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 een bijlage bij dit Reglement (bijlage 2).

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

3.4 Voor de doelstelling van NIVEL Zorgregistraties eerste lijn zoals genoemd in artikel 2.1 wordt het evenwel niet uitgesloten dat over bepaalde Patiënten vanuit het dossiersysteem indirect identificerende Gegevens worden verzameld of dat samenvoegen van Gegevens tussen verschillende Disciplines een bestand met indirect identificerende Gegevens kan opleveren.

3.5 De Deelnemer zal diens Patiënten door middel verstrekking van de NIVEL Zorgregistraties patiëntenfolder en door middel van de NIVEL Zorgregistraties-posters informeren over de gegevensverwerking van (mogelijk) niet volstrekt anonieme Gegevens ten behoeve van wetenschappelijk onderzoek zoals met NIVEL Zorgregistraties eerste lijn en biedt de Patiënt de gelegenheid bezwaar te maken. Een voorbeeld van zulke informatie is opgenomen bij de Samenwerkingsovereenkomst.

3.6 Zoals geregeld in de Samenwerkingsovereenkomst vindt geen verstrekking van Gegevens aan NIVEL Zorgregistraties eerste lijn plaats indien de Patiënt een bezwaar heeft gemaakt als bedoeld in het vorige lid.

3.7 Naast in beginsel anonieme Gegevens over Patiënten van de Deelnemers worden ook Gegevens over de Deelnemers zelf verzameld. De aard van deze Gegevens en de wijze van verzamelen wordt steeds vastgesteld zoals bepaald in het Governance-document. De Deelnemers blijven in NIVEL Zorgregistraties eerste lijn identificeerbaar. De verwerking en eventuele uitvoer van zulke Gegevens geschiedt uitsluitend zoals in dit Reglement is bepaald.

3.8 Mits de Deelnemer hierin toestemt zal het NIVEL ook Patiënten kunnen uitnodigen om aan een deelonderzoek mee te werken door het eenmalig of vaker invullen van enquêtes. Tot een dergelijk onderzoek wordt besloten zoals bepaald in het Governance-document. De uitnodiging wordt namens het NIVEL gerealiseerd door de Deelnemer. De Deelnemer verkrijgt de hiertoe noodzakelijke persoonsgegevens via de TTP.

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 De vanuit de onderscheiden Disciplines aangeleverde Gegevens (als bedoeld in art. 3.1.a) blijven gescheiden tenzij de desbetreffende koepel- en beroepsorganisaties zoals bepaald in het Governance-document besluiten tot een onderzoek dat over meerdere Disciplines heen reikt.

4.3 Tot de verwerking van de Gegevens binnen één Discipline wordt slechts overgegaan na het besluit van de desbetreffende koepel- of beroepsorganisatie zoals bepaald in het Governance-document.

4.4 Voor onderzoek waarbij Gegevens worden verwerkt als bedoeld in art. 3.1 onder b en c wordt een apart bestand aangelegd, dat uitsluitend voor het desbetreffende onderzoek wordt gebruikt (waaronder begrepen een eventueel vervolg op dat onderzoek).

4.5 De Gegevens kunnen ook worden verwerkt voor onderzoek door andere onderzoeksinstellingen dan het NIVEL. Het bepaalde in art. 6 is op zulk onderzoek van toepassing.

Artikel 5 - Uitvoer uit NIVEL Zorgregistraties eerste lijn

5.1 De uitvoer uit NIVEL Zorgregistraties eerste lijn in welke vorm dan ook, zoals rapporten, artikelen, statische overzichten, etc. is steeds zodanig dat individuele Patiënten daarin volstrekt niet herkenbaar zijn.

5.2 De uitvoer is tevens zodanig dat de Deelnemers daarin voor elke ander dan de Deelnemer zelf redelijkerwijs niet herkenbaar zijn tenzij de Deelnemer voor een zodanige uitvoer uitdrukkelijke toestemming heeft gegeven.

Artikel 6 - Gebruik van Gegevens voor aanvullend onderzoek

6.1 Onderzoeksgroepen (bij externe onderzoeksinstellingen of van binnen het NIVEL) kunnen bij het NIVEL een aanvraag indienen om van de Gegevens gebruik te maken voor door deze instelling voorgenomen onderzoek. Het NIVEL kan nadere regels stellen voor het doen van de aanvraag en de daarin opgenomen beschrijving van het onderzoek.

6.2 Over het goedkeuren van de aanvraag (volgens de procedure beschreven in het Governance-document) beslist de koepel- of beroepsorganisatie van de Discipline waarop het onderzoek betrekking heeft. Een goedgekeurde aanvraag leidt tot een overeenkomst met 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 Het bepaalde in de vorige artikelen is op onderzoek door een andere onderzoeksinstelling eveneens van toepassing. De voor het goedgekeurde onderzoek benodigde verwerking van Gegevens wordt 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 is kosten verschuldigd 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 NIVEL Zorgregistraties eerste lijn voldoet aan de daaraan te stellen veiligheidseisen. Bij het informatiebeveiligingsbeleid worden de daarop van toepassing zijnde ISO en NEN normen gevolgd. Indien het NIVEL voor (onderdelen van) de NIVEL Zorgregistraties eerste lijn database een bewerker zal inschakelen, zullen gelijke veiligheidseisen aan de bewerker worden gesteld en in een bewerkersovereenkomst worden vastgelegd.

7.2 Van elke zoekvraag in NIVEL Zorgregistraties eerste lijn en de daartoe uitgevoerde bewerkingen en van elke uitvoer uit NIVEL Zorgregistraties eerste lijn wordt aantekening gehouden via een systeem van logfiles.

7.3 Uitsluitend daartoe specifiek gemachtigde medewerkers 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 systeem. Dit zijn twee onderscheiden functies en medewerkers kunnen niet beide vervullen. Deze medewerkers hebben een geheimhoudingsverklaring afgelegd.

Artikel 8 - Privacycommissie

8.1 Een privacycommissie houdt toezicht op de werking van NIVEL Zorgregistraties eerste lijn. De samenstelling, taken en bevoegdheden van deze commissie zijn in het Governance-document NIVEL Zorgregistraties eerste lijn beschreven.

Artikel 9 - Betrokkenen

9.1 Betrokkenen zijn Deelnemers en Patiënten van Deelnemers van wie eventueel indirect identificerende Gegevens worden verwerkt. De betrokkene kan bezwaar maken tegen zulke verwerking. De verdere verwerking wordt dan gestaakt. Omdat de Gegevens eerder kunnen zijn gebruikt voor onder meer wetenschappelijke publicaties en deze langdurig moeten kunnen worden gevalideerd, kunnen de eerder verwerkte Gegevens niet worden verwijderd. Gelet op de pseudonimiseringsprocedures kan de betrokkene uitsluitend bij de Deelnemer bezwaar maken tegen verdere verwerking. Ook al is wellicht sprake van indirect identificerende Gegevens binnen NIVEL Zorgregistraties eerste lijn, de medewerkers van het NIVEL zullen de betrokkene niet zonder onevenredige tijd en moeite in de database kunnen terugvinden aan de hand van door de Patiënt zelf opgegeven niet specifiek medische kenmerken.

Artikel 10 Inwerkingtreding en geldingsduur

10.1 Dit reglement treedt in werking op 1 januari 2014 en geldt gedurende de looptijd van NIVEL Zorgregistraties eerste lijn of tot het moment waarop een opvolgend reglement wordt vastgesteld.

10.2 In afwijking van het in artikel 3.2 bepaalde kunnen, zolang de pseudonimiseringssoftware bij de Deelnemer nog niet is geïnstalleerd, in plaats van het pseudoniem Gegevens van de Patiënt onder het bij de Deelnemer aan die Patiënt toegekende patiëntnummer worden verzameld. Zodra de pseudonimiseringssoftware is geïnstalleerd wordt dit patiëntnummer vervangen door het pseudoniem.

10.3 Wijzigingen van het privacyreglement kunnen alleen worden doorgevoerd met goedkeuring van de Privacycommissie. Stuurgroep en Kamers worden in kennis gesteld van wijzigingen. Wijzigingen van het privacyreglement worden gepubliceerd op de website van NIVEL Zorgregistraties eerste lijn.

Artikel 12 Bijlagen

Dit reglement kent twee bijlagen:

- Bijlage 1 is het Governance-document. Deze maakt van het Reglement een onverbrekelijk deel uit.
- Bijlage 2 is de technische beschrijving van het verzamelen van Gegevens als bedoeld in art. 3.1a, de rol van de TTP, het eventuele samenvoegen van Gegevens over verschillende Disciplines en de ontsleuteling door de TTP ten behoeve van enquêtes als beschreven in art. 3.7. Deze bijlage kan op ondergeschikte punten worden aangepast als de stand van de techniek daartoe aanleiding geeft.

Bijlage 2 bij Privacyreglement NIVEL Zorgregistraties eerste lijn

Technische beschrijving pseudonimisatie gegevensverzameling NIVEL Zorgregistraties eerste lijn

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 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.

Het College Bescherming Persoonsgegevens (CBP) stelt de volgende eisen aan een TTP die pseudonimisatie dienstverlening aanbiedt[4]:

1) Er wordt vakkundig gebruik gemaakt van pseudonimisering, waarbij de eerste pseudonimisatie plaatsvindt bij de aanbieder;
2) Er zijn technische en organisatorische maatregelen genomen om herhaalbaarheid van de versleuteling (‘replay attack’) te voorkomen;
3) De verwerkte gegevens zijn niet indirect identificerend;
4) In een onafhankelijk deskundig oordeel (audit) wordt vooraf en daarna periodiek vastgesteld dat aan voorwaarden 1), 2) en 3) is voldaan;
5) De werkwijze wordt beschreven en gepubliceerd.

Voor het pseudonimiseren van privacygevoelige gegevens heeft ZorgTTP een pseudonimisatieplatform ontwikkeld. Dit omvat naast de ontwikkelde software ook technische en organisatorische voorzieningen om zorgvuldig alle werkzaamheden te kunnen uitvoeren.

Het pseudonimisatieplatform wordt jaarlijks onderworpen aan zowel interne als externe audits. De externe audit wordt uitgevoerd door Pricewaterhouse Coopers (PwC). Deze audit wordt, conform door het CBP gestelde eisen, jaarlijks herhaald om de vorderingen te beoordelen. De door ZorgTTP gehanteerde werkwijze is daarbij steeds positief beoordeeld.

De kerntaak van ZorgTTP is het depersonaliseren van bestanden om daarmee het uitwisselen van informatie op individueel niveau, conform de wettelijke vereisten,

[4] Brief CPB aan Ministerie van VWS, 6 maart 2007; kopie bij ZorgTTP aanwezig.

mogelijk te maken. De verzendende (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. Het is echter aan het CBP, als toezichthouder op de Wet Bescherming Persoonsgegevens (WBP), voorbehouden om de gemaakte afwegingen te toetsen en een oordeel te vellen over de mate waarin de uitwisseling is toegestaan binnen de kaders die de WBP stelt.

Bij ZorgTTP worden geen data, zoals patiëntbestanden, opgeslagen. Enkel het algoritme waarmee de persoonsgegevens worden gepseudonimiseerd wordt bewaard.

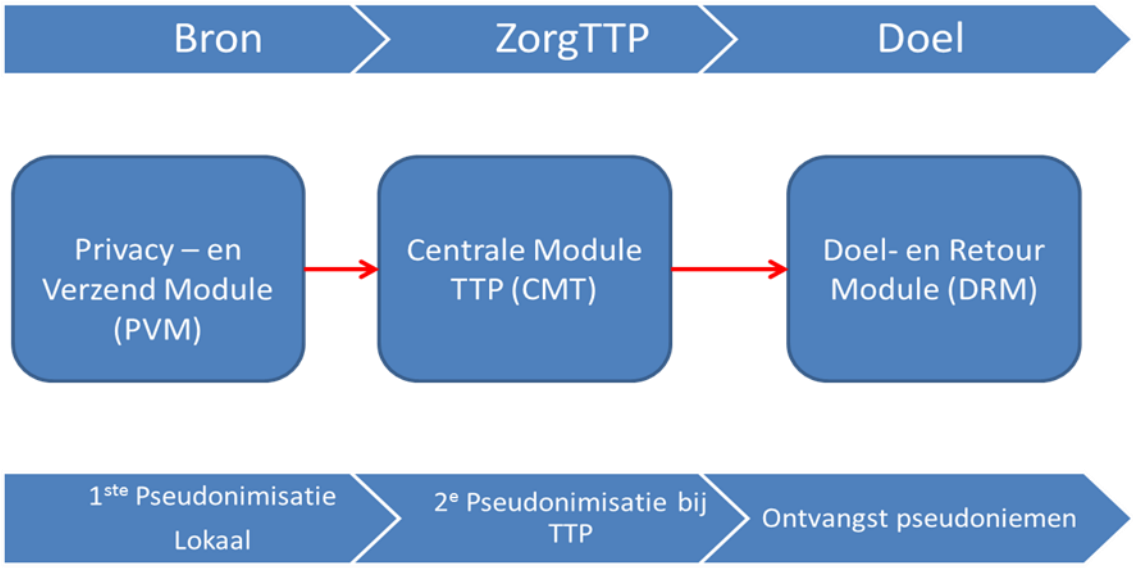
Beknopte beschrijving van het pseudonimisatieproces

Het pseudonimisatieproces bestaat in het kort uit de volgende stappen:

1. Uitgangspunt is dat de verzendende partij (de Deelnemer) een bestand genereert dat voldoet aan vooraf vastgestelde specificaties;
2. Het bestand wordt verwerkt met de door ZorgTTP aan de Deelnemer 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 (het NIVEL) met een daartoe beschikbaar gestelde ontvangstmodule.

In onderstaande figuur wordt het pseudonimisatieproces schematisch weergegeven.

Globaal proces van pseudonimisatie



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.
Het uitvoeren van een eerste bewerking op de te pseudonimiseren gegevens bij de bron is een vereiste binnen het kader dat het CBP heeft opgesteld.
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.

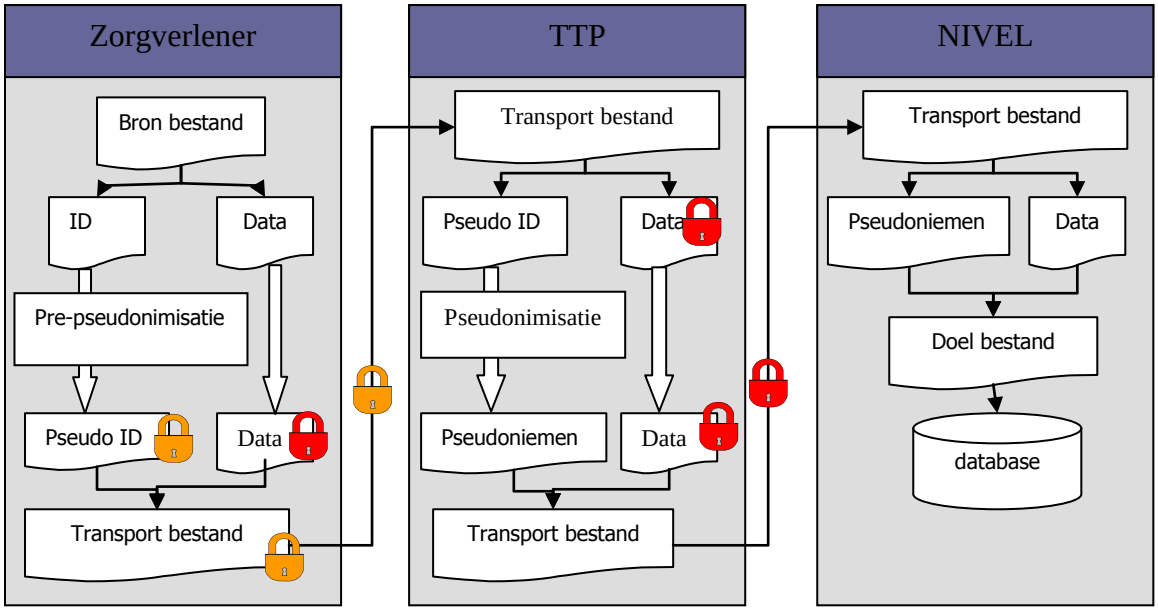
Centrale Module TTP (CMT)

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

Volgens de CBP uitgangspunten wordt gepseudonimiseerde data niet langer beschouwd als tot persoonsgegevens terug te herleiden data. De opgeslagen gegevens blijven echter een zekere mate van gevoeligheid behouden, zeker in het geval van medische gegevens. Daarnaast kan door het koppelen van gepseudonimiseerde dataverzamelingen of door het toevoegen van aanvullende variabelen alsnog op directe of indirecte wijze sprake zijn van tot persoonsgegevens herleidbare data.

In dat geval zal de registratie alsnog dienen te voldoen aan de eisen die de WBP stelt aan het verwerken van persoonsgegevens.

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.

Historische data

Het NIVEL verzamelt al geruime tijd medische informatie. Zorgregistratie huisartsen (LINH) is bijvoorbeeld een netwerk van 84 geautomatiseerde huisartspraktijken met meer dan 335.000 ingeschreven patiënten (juli 2010). De LINH-huisartsen verzamelen op continue basis 'productiegegevens' over aandoeningen (ICPC-gecodeerde diagnose), aantallen contacten/verrichtingen, geneesmiddelvoorschriften en verwijzingen. LINH is vanaf 1991 operationeel.
Vanaf medio 2012 wordt gefaseerd het pseudonimisatieplatform in gebruik genomen. Daarbij wordt de historische dataverzameling ook gepseudonimiseerd. Daardoor zijn de nieuwe gepseudonimiseerde aanleveringen te koppelen aan de historische dataverzameling.

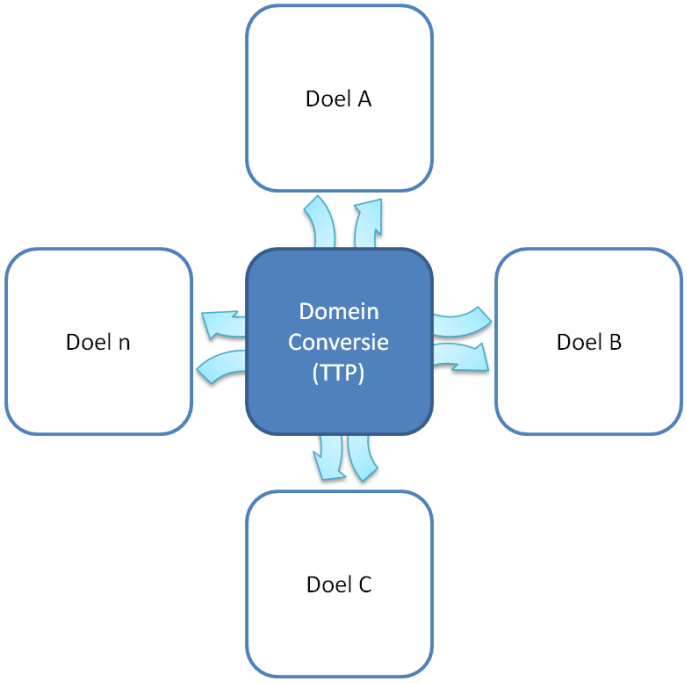
Domeinconversie

ZorgTTP verleent pseudonimisatiediensten aan diverse partijen. Deze en andere partijen die al dan niet over gepseudonimiseerde dataverzamelingen beschikken, hebben behoefte aan de mogelijkheid om – op gecontroleerde wijze – bestanden aan elkaar te kunnen koppelen. Daarom is een functie voor zogenaamde ‘domeinconversie’ ontwikkeld.

Domeinconversie maakt het mogelijk om een pseudoniem van een BSN van het ene domein (lees een gepseudonimiseerde dataverzameling) te converteren naar een pseudoniem, op grond van hetzelfde BSN, zoals bekend binnen een ander domein.
Het reguliere pseudonimisatieproces verloopt in twee stappen. De eerste versleuteling vindt plaats bij de bron, de tweede versleuteling bij ZorgTTP. Onderdeel van de tweede versleuteling is een domeinspecifieke encryptie. Dit betekent dat iedere gepseudonimiseerde dataverzameling van een specifieke serie pseudoniemen wordt voorzien. De kracht van deze domeinspecifieke encryptie is dat kan worden voorkomen dat gepseudonimiseerde dataverzamelingen eenvoudigweg op basis van pseudoniemen aan elkaar gekoppeld kunnen worden. Daarmee zou het risico op indirecte herleidbaarheid naar de oorspronkelijke persoonsgegevens onaanvaardbaar hoog worden.

Voor elke opdrachtgever kan daardoor voorzien worden in één of meer domeinen.
In de praktijk betekent dit dat gelijke input – bijvoorbeeld een bepaald BSN – in de verschillende domeinen verschillende pseudoniemen zal opleveren. Slechts met behulp van domeinconversie kunnen verschillende domeinen aan elkaar gekoppeld worden.

Model voor de functie Domeinconversie



NIVEL-ZorgTTP juli 2011

Communicatiemodel

Aangezien het in specifieke gevallen mogelijk moet zijn om additionele informatie te verzamelen, wordt er gebruik gemaakt van een communicatiemechanisme. De reguliere pseudonimisatie wordt zoals eerder beschreven uitgevoerd. Voor het verzoek om additionele informatie zijn twee zaken noodzakelijk: een identificatie van de behandelaar en een lokaal patiëntnummer.

Als de onderzoeker tot de conclusie komt dat additionele informatie van grote meerwaarde zou zijn, dan kan gebruik worden gemaakt van de communicatiedatabase. Het is dan wel noodzakelijk dat er een gedeelde variabele is tussen beide domeinen. We maken daarvoor gebruik van een communicatiepseudoniem. Dit pseudoniem is zowel beschikbaar in het domein Onderzoek als in het domein Communicatie. Omdat het twee domeinen betreft, zal het pseudoniem – ondanks identieke input – een andere waarde opleveren. ZorgTTP kan het communicatiepseudoniem – onder strikte voorwaarden - converteren van het domein Onderzoek naar het domein Communicatie.

Het proces verloopt dan als volgt:

1. NIVEL bepaalt in welke gevallen er sprake is van grote meerwaarde van additionele informatie. Enkel in die gevallen wordt er gebruik gemaakt van het communicatiemechanisme;
2. De aanvraag betreft een zogenaamde ‘domeinconversie’. Deze moet technisch door twee medewerkers van ZorgTTP worden goedgekeurd;
3. Vanuit NIVEL wordt de zorgverlener gevraagd om de patiënt te benaderen met het verzoek om additionele informatie;
4. De patiënt beslist zelf of hij of zij de informatie verstrekt aan NIVEL;
5. Bij het verstrekken van de informatie wordt gewerkt met een onderzoeksnummer, er zijn geen persoonsgegevens noodzakelijk.

Schematische weergave communicatiemodel