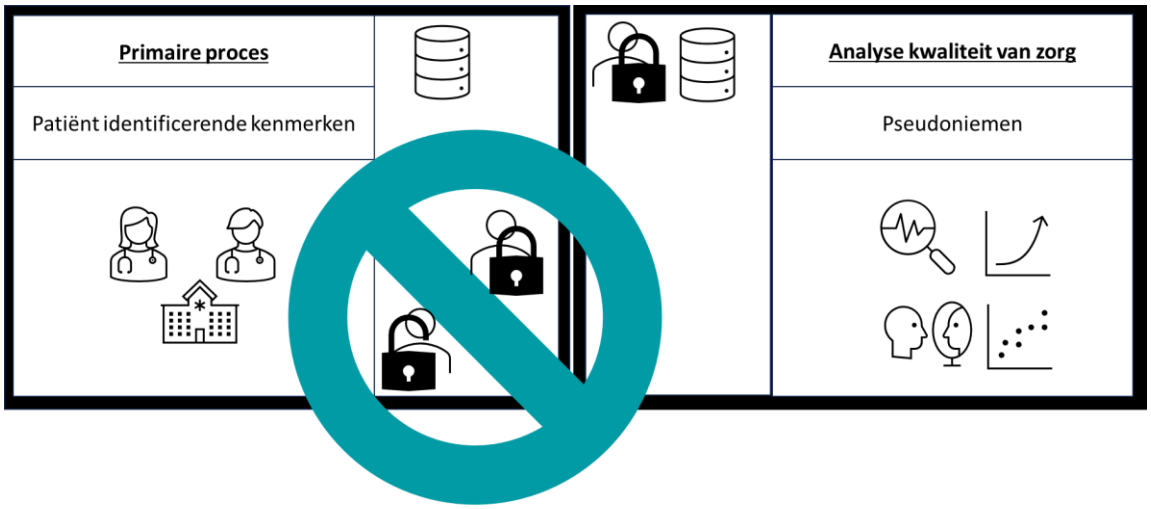
Shared Service Center
Data Governance

Handreiking Pseudonimisering voor gegevensaanlevering aan kwaliteitsregistraties

Voor zorgaanbieders, registratiehouders en dataverwerkers



Inhoudsopgave

Inleiding

Er is een aanpassing van de Wkkgz in voorbereiding
Zorgaanbieders leveren gegevens aan kwaliteitsregistraties[1] volgens de Wet kwaliteit, klachten en geschillen zorg (Wkkgz). Kwaliteitsregistraties verzorgen vervolgens de verzameling, gegevensopslag en verwerking van gegevens over een gespecificeerde patiëntenpopulatie. Bij deze verzameling, gegevensopslag en verwerking hebben ook in opdracht van zorgaanbieder en/of registratiehouder opererende dataverwerkers een rol. Op basis van rapportages van kwaliteitsregistraties kunnen zorgverleners leren van elkaar en zo de kwaliteit van zorg verbeteren. Het wetswijzigingsvoorstel van de Wkkgz[2] dat momenteel in voorbereiding is, treedt naar verwachting in 2024 in werking.

Wat gaat er veranderen?
De wetswijziging voorziet in:

1. een **wettelijke grondslag** voor kwaliteitsregistraties en hun gegevensverwerkers om gepseudonimiseerde (bijzondere) persoonsgegevens te mogen verwerken;
2. het instellen van een **register voor kwaliteitsregistraties** bij het Zorginstituut Nederland[3] voor de noodzakelijke beheersing van kwaliteitsregistraties en vermindering van de administratieve lasten;
3. een **aanleververplichting voor zorgaanbieders** om gegevens aan te leveren aan de in het register voor kwaliteitsregistraties opgenomen kwaliteitsregistraties;
4. de verplichting voor zorgaanbieders om de aan kwaliteitsregistraties aan te leveren **persoonsgegevens zo dicht als mogelijk aan de bron te pseudonimiseren**.

In deze handreiking leest u wat zorgaanbieders, registratiehouders en dataverwerkers moeten weten om aan deze verplichting te kunnen voldoen. Deze handreiking zal met name ingaan op punt 4 uit bovenstaande opsomming, omdat op dit punt de meeste verandering vereist is qua inrichting en afspraken.

Pseudonimiseren voor kwaliteitsregistraties
Bij pseudonimiseren vervangt men persoonsgegevens door pseudoniemen. Met een pseudoniem kan de kwaliteitsregistratie iemand volgen in de tijd en over verschillende zorgaanbieders heen zonder dat de identiteit bekend wordt. Daarmee kan de kwaliteitsregistratie bijvoorbeeld meten hoeveel personen na een eerste ingreep op een later moment weer in zorg raken. Ook al is dat bij een andere zorgaanbieder.

Om veilige en voor kwaliteitsdoeleinden bruikbare pseudoniemen te maken, is het van belang dat:

1. De kwaliteitsregistratie niet in staat is om zonder aanvullende informatie de identiteit van betrokkenen te kunnen afleiden. De kwaliteitsregistratie mag daarom zelf de pseudoniemen niet maken. De zorgaanbieder kan dat in theorie wel, maar dan kan niet aan de eis worden voldaan dat;
    a. Voor ieder persoonsgegeven dat wordt verwerkt voor dezelfde registratie steeds hetzelfde pseudoniem moet worden gemaakt.
    b. Daarnaast moeten pseudoniemen ook tussen kwaliteitsregistraties uitwisselbaar zijn.
    c. Door gebruik te maken van een Trusted Third Party (TTP), die verantwoordelijk is voor de pseudonimisering, kan aan deze eisen worden voldaan.
2. De werkwijze van een TTP, die verantwoordelijk is voor het maken van pseudoniemen, moet voldoen aan de stand der techniek en geschikt zijn om personen te volgen in de tijd en over locaties heen. In de praktijk kan de TTP voldoen aan deze eisen door te werken volgens de norm NEN7524:2019 – pseudonimisatiedienstverlening.

Uw juridische afdeling kan de verplichting om te pseudonimiseren en de nadere eisen die gesteld worden, nalezen in de sectie 'wettelijk kader pseudonimiseren'.

Hoe werkt het?
Er bestaan meerdere Privacy Enhancing Technologies (PET) voor het maken van pseudoniemen. Rekening houdend met de bestaande werkprocessen, wettelijke en functionele eisen, kunnen zorgaanbieders straks op twee manieren pseudoniemen aanvragen. Deze staan ook beschreven in de NEN7524:2019.

[1] Feitelijk is de entiteit waaraan wordt aangeleverd de registratiehouder die verantwoordelijk is voor de kwaliteitsregistratie. In deze notitie worden omwille van de leesbaarheid deze begrippen als synoniem gebruikt. Waar kwaliteitsregistratie staat kan dus registratiehouder worden gelezen.
[2] https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A36278
[3] https://www.landelijkekwaliteitsregistratie.nl/het-proces/opname-in-het-register/

1. De zorgaanbieder vraagt een pseudoniem op bij de pseudonimiseringsservice en levert deze zelf door aan de kwaliteitsregistratie.
2. De zorgaanbieder vraagt een pseudoniem op, de pseudonimiseringsservice levert deze, samen met de gerelateerde data door aan de kwaliteitsregistratie.

Model 1 is bedoeld voor registraties waar op basis van ZIB's en HL7 FHIR wordt aangeleverd. Model 2 houdt rekening met registraties en/of zorgaanbieders die nog niet zo ver zijn. De te pseudonimiseren gegevens worden in model 2 volgens een door de kwaliteitsregistratie opgestelde bestandsdefinitie aangeboden aan de pseudonimisatieservice.

De modellen worden voor de IT-afdeling, BI-specialisten, kwaliteits- en registratiemedewerkers toegelicht in de sectie 'implementatie pseudonimiseringsservice'.

Wat wordt er van zorgaanbieders verwacht?
De wetswijziging is nog in behandeling. De toetsing van de eerste kwaliteitsregistraties is gaande. En er wordt nog gewerkt aan standaardisatie van gegevensaanlevering, contractering en financiering. Dat bekent echter niet dat zorgaanbieders nog niets kunnen doen.

Wat kan een zorgaanbieder nu al doen om zijn organisatie voor te bereiden op de situatie na in werking treden van de wetswijziging?

1. Inventariseer voor welke kwaliteitsregistraties gegevens worden aangeleverd;
2. Inventariseer en stem af met de kwaliteitsregistraties in hoeverre er reeds met ZIB's gewerkt wordt;
3. Ga na of er al gepseudonimiseerd wordt aangeleverd aan kwaliteitsregistraties;
4. Breng in kaart op welke wijze aanlevering van data plaatsvindt of kan vinden in relatie tot de geschetste modellen;
5. Overleg met de EPD-leverancier(s) de impact van gepseudonimiseerde aanlevering volgens de hiervoor genoemde modellen.

Zijn er werkzaamheden extern te beleggen?
Omdat de eisen voor pseudonimisering voor alle kwaliteitsregistraties gelden, en het gegeven de eisen niet waarschijnlijk is dat ziekenhuizen zelfstandig aan de eisen kunnen voldoen, wordt momenteel gewerkt aan een plan van aanpak om pseudonimisering centraal te organiseren. Centrale inkoop en aansturing is naar verwachting bovendien voordeliger en bevordert de gewenste standaardisatie op dit thema. In het plan van aanpak komen ook onderwerpen zoals hoe dit georganiseerd en bekostigd zou kunnen worden aan bod.

Onafhankelijk van de uitkomst van dit onderzoek, moet de zorgaanbieder gegevens gaan aanleveren conform het door de kwaliteitsregistratie voorgeschreven formaat. Voor zover dit niet reeds in gang is gezet, moeten zorgaanbieders nagaan of, en in hoeverre de aan te leveren gegevens reeds beschikbaar gemaakt kunnen worden in het voorgeschreven formaat.

Wat kost het en wat levert het op?
Om samen te kunnen leren en verbeteren, zijn kwaliteitsregistraties afhankelijk van de binnen het zorgproces vastgelegde gegevens. Het voornaamste doel van de wetswijziging is het bieden van regie op en een grondslag voor kwaliteitsregistraties. De wetswijziging zal daarmee naar verwachting helpen om het vastleggen en aanleveren van deze gegevens te standaardiseren en daarmee de administratieve lasten te beperken. Wanneer alle kwaliteitsregistraties via hetzelfde aanleverproces van gegevens voorzien worden en als de gegevens-uitvraag gestandaardiseerd is, nemen de administratieve lasten af.

1 Wettelijk kader pseudonimiseren

Het wijzigingsvoorstel voor de Wet kwaliteit, klachten en geschillen zorg (Wkkgz)[4] dat momenteel in voorbereiding is, treedt naar verwachting in 2024 in werking. Dit wetsvoorstel verplicht het gebruik van pseudonimiseren van de direct identificerende persoonsgegevens als passende maatregel conform de verplichting uit de Algemene Verordening Gegevensbescherming (AGV) voor het treffen van (o.a. technische) maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen.

De Wkkgz stelt daarnaast aanvullende eisen aan de verwerking van de persoonsgegevens om koppeling van gegevens over zorgpaden, zorgaanbieders en zorgketens heen mogelijk te maken (paragraaf 1.2).

In deze handreiking vindt u een toelichting op de gevolgen van deze verplichting tot pseudonimiseren en de aanvullende eisen m.b.t. koppelbaarheid, een omschrijving van wat deze maatregelen betekenen voor de rollen en werkzaamheden van zorgaanbieders, registratiehouders en dataverwerkers en welke voorbereidingen getroffen moeten worden om te kunnen voldoen aan deze maatregelen.

1.1 Pseudonimiseren volgens de AVG

De AVG verplicht (in artikel 32 lid 1a) de verwerkingsverantwoordelijke en de onder diens verantwoordelijkheid betrokken verwerker(s) om passende technische en organisatorische maatregelen te treffen om de verwerkte gegevens te beschermen. Pseudonimisering en versleuteling worden daarbij als maatregelen genoemd:

> *"Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten: a) de pseudonimisering en versleuteling van persoonsgegevens."*

De AVG definieert pseudonimisering als volgt in art. 4[5]:

> *"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."*

Concreet betekent dit dat alleen de technische maatregel om persoonsgegevens te versleutelen niet volstaat. Organisatorisch moet worden geborgd dat de sleutel of aanvullende gegevens die nodig zijn voor directe herleiding apart van de versleutelde gegevens, worden bewaard.

1.2 Pseudonimiseren en de Wkkgz

Het wetswijzigingsvoorstel van de Wkkgz[6] dat momenteel in voorbereiding is, treedt naar verwachting in 2024 in werking. Het voorstel voor aanpassing van de Wkkgz volgt de AVG en stelt aanvullende eisen:

1. **De registratiehouder verwerkt uitsluitend gepseudonimiseerde gegevens**
   Artikel 11p, lid 2: *"De registratiehouder, of een onder diens verantwoordelijkheid werkzame verwerker, verwerkt slechts persoonsgegevens als daarop pseudonimisering is toegepast en vervolgens ten aanzien van deze verwerkingen onafgebroken is gecontinueerd."*
2. **Een zorgaanbieder pseudonimiseert gegevens voor verstrekking**
   Artikel 11q lid 3: *"Een zorgaanbieder als bedoeld in het eerste lid, past op de in dat lid bedoelde gegevens pseudonimisering toe, alvorens de gegevens te verstrekken."*

Ook de Memorie van Toelichting[7] stelt aanvullende eisen;

3. **Pseudonimisering zo vroeg mogelijk in het proces (aan de bron)**
   'Op grond van de AVG dient pseudonimisering plaats te vinden in combinatie met andere maatregelen die erop gericht zijn de herleidbaarheid van de gegevens te beperken. Daarom verdient het de voorkeur om de pseudonimisering zo vroeg mogelijk in het proces, liefst aan de bron, te laten plaatsvinden."
4. **Koppelbaarheid in de tijd en over locaties heen (herhaalbaarheid en koppelbaarheid)**

[4] https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A36278
[5] https://autoriteitpersoonsgegevens.nl/uploads/imported/verordening_2016_-_679_definitief.pdf
[6] https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A36278
[7] https://www.tweedekamer.nl/downloads/document?id=2022D55107

'Zoals al is aangegeven, moeten behandeltrajecten en waar mogelijk ook verschillende elementen van een behandeling aan een unieke cliënt gekoppeld kunnen worden en dubbelingen in de registratie van unieke cliënten zoveel mogelijk worden tegengegaan. Pseudonimisering van gegevens over dezelfde cliënt maakt het alleen mogelijk om deze gegevens uit verschillende bronnen te koppelen indien gebruik wordt gemaakt van hetzelfde pseudoniem."

5. **State of the art (kwaliteit van de pseudonimisering)**
   Waar in dit wetsvoorstel gesproken wordt over de verplichte en ononderbroken toepassing van pseudonimisering, zullen alle betrokken partijen zich dienen te richten naar de eisen in die ministeriële regeling die voldoen aan de actuele stand van de techniek. Daarmee wordt een heldere en objectieve standaard geboden voor het (door)ontwikkelen van het kader waaraan alle uitwisselingen van persoonsgegevens tussen kwaliteitsregistraties en zorgaanbieders en kwaliteitsregistraties onderling moeten voldoen, wanneer zij binnen de kaders van dit wetsvoorstel gegevens verwerken."

Tot slot staat in de Ministeriële regeling en het aanvraagformulier voor opname in het register de eis:

6. **Gestandaardiseerde methode**.
   De ministeriële regeling verwijst naar het aanvraagformulier voor opname in het register waarin voorgaande eisen deels herhaald worden. Aanvullend wordt gesteld dat gepseudonimiseerde gegevens uit verschillende registraties koppelbaar zijn op basis van een gestandaardiseerde methode.

1.3 Begrippen en definities bij pseudonimisering voor kwaliteitsregistraties

Voordat we de opzet van de pseudonimisering voor kwaliteitsregistraties beschrijven, is het van belang om duidelijk te maken wat de in voorgaande paragrafen genoemde begrippen betekenen. Onderstaand overzicht licht de eisen toe die gesteld worden in de AVG en Wkkgz bij pseudonimisering voor kwaliteitsregistraties:

Pseudonimisering	Definitie / toelichting
Wordt toegepast op alle direct identificeerbare gegevens	Onder 'direct identificerende persoonsgegevens' wordt verstaan; informatie die men kan gebruiken om de identiteit van een persoon vast te stellen of te traceren. Denk aan: naam, Burgerservicenummer (BSN), geboortedatum en -plaats, meisjesnaam van de moeder of biometrische gegevens.
Is onafgebroken gecontinueerd	De kwaliteitsregistratie ontvangt uitsluitend pseudoniemen en geen direct identificerende gegevens. Deze identificerende gegevens worden vervangen door een pseudoniem, zodanig dat steeds voor hetzelfde doel hetzelfde gegeven hetzelfde pseudoniem oplevert.
Vindt plaats op basis van een gestandaardiseerde methode die als State-of-the-Art kan worden gezien	Om te kunnen koppelen in de tijd en tussen zorgaanbieders en andere bronhouders[8], moet de werkwijze voor alle kwaliteitsregistraties gelijk zijn voor wat betreft het aanmaken van de pseudoniemen. De kwaliteit van de pseudoniemen is daarbij zodanig dat ze voldoende onderscheidend vermogen hebben en cryptografisch van zodanige kwaliteit dat ze als voldoende veilig mogen worden beschouwd. *Voorbeeld:* In opdracht van het Ministerie van VWS is in 2015 een openbare methodebeschrijving opgesteld en geïmplementeerd voor het aanmaken van onomkeerbare pseudoniemen. Voor een aantal grote landelijke zorgregistraties wordt deze methode sinds lange tijd en op grote schaal toegepast[9]. De methode beschrijft zowel randvoorwaarden voor het proces als technische en cryptografische voorschriften voor het genereren van pseudoniemen. Daarnaast is voorzien in het tussentijds vervangen en overdragen van sleutelmateriaal. De methode kan door iedere Third Trusted Party (TTP) worden geïmplementeerd, en is door minimaal één Nederlandse TTP reeds geïmplementeerd. De beschrijving van deze openbare methode vindt u op deze website[10].
Is herhaalbaar	Een bepaald identificerend gegeven leidt voor dezelfde kwaliteitsregistratie steeds tot hetzelfde pseudoniem. *Voorbeeld:* "Dirk van den Broek" wordt steeds pseudocode fhK30q1wqant voor registratie X en hnfwerio23458g823-cd voor registratie Y.
Vindt zo dicht als mogelijk aan de bron plaats	Pseudoniemen worden aangemaakt net vóór- of tijdens het daadwerkelijk verstrekken van de gegevens vanuit de zorgaanbieder aan de kwaliteitsregistratie. 'Zo dicht als mogelijk' is in ieder geval **niet** bij de kwaliteitsregistratie.
Gepseudonimiseerde gegevens uit	De gehanteerde methode voorziet in de mogelijkheid om pseudoniemen van registratie X via de TTP te vertalen naar registratie Y. Uitgangspunt hierbij is dat de

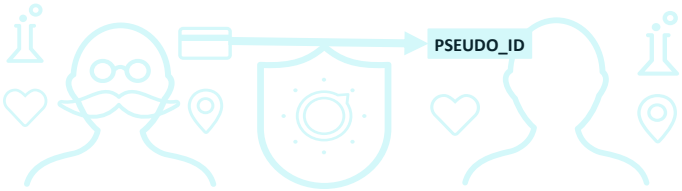
[8] Bronhouders kunnen naast zorgaanbieders ook andere bronnen zijn zoals kwaliteitsregistraties zelf, Palga, IKNL, Vektis, etc.
[9] Ziekenhuizen leveren bijvoorbeeld gegevens aan de Landelijke Basisregistratie Ziekenhuiszorg (LBZ) en het DBC Informatiesysteem (DIS).
[10] https://www.zorgttp.nl/wp-content/uploads/2023/01/NEN-pseudonimisering-specificatie-voorstel-VWS-1.0.pdf

verschillende registraties zijn (onder voorwaarden) koppelbaar	kwaliteitsregistraties hierbij nooit de onderliggende gegevens of de pseudoniemen zoals bekend bij een andere registratie verwerken. Voordeel van deze werkwijze is dat pseudoniemen uniek blijven per registratie (compartimentering). Zo kan de kans op herleiding beperkt worden. Voor iedere koppeling moet de impact op de herleidbaarheid worden ingeschat. Recent is in opdracht van Health RI een rapport door Nivel en MLCF gepubliceerd waarin aan de hand van het gepseudonimiseerd BSN het principe van compartimentering geïllustreerd wordt[11].

1.4 Vormen van pseudonimisering

In de normen ISO25237 en NEN7524 zijn verschillende vormen van pseudonimisering beschreven. In alle gevallen is het resultaat van het proces dat één of meerdere pseudoniemen de oorspronkelijke identificerende gegevens vervangen. In onderstaande afbeelding wordt een pseudoniem aangemaakt. Voor de overige gegevens wordt de afweging gemaakt in hoeverre deze op zichzelf of in combinatie met andere gegevens herleidbaar zijn. De herleidbaarheid wordt zo nodig beperkt door het toepassen van maatregelen als generaliseren, classificeren, maskeren, verwijderen of randomiseren.

De voor deze handreiking meest relevante vormen zijn 'omkeerbare' en 'onomkeerbare pseudonimisering'. Kwaliteitsregistraties kunnen middels een Data Protection Impact Assessment (DPIA) de afweging maken welke vorm voor welke gegevens best passend is. Beide vormen kunnen naast elkaar worden toegepast binnen dezelfde registratie.



Figuur 1. pseudonimisering

1.4.1 Versleuteling versus pseudonimisering

'Versleuteling'[12] en 'pseudonimisering' zijn geen synoniemen van elkaar. Bij versleuteling wordt een leesbare tekst omgezet naar een versleutelde tekst met een sleutel. Als de gebruiker van de versleutelde gegevens ook de sleutel hiervan bezit, is geen sprake van pseudonimisering, maar van versleuteling. Een belangrijk uitgangpunt bij pseudonimisering is het aanbrengen van een scheiding tussen de oorspronkelijke persoonsgegevens, de sleutel waarmee gegevens gepseudonimiseerd worden en de gepseudonimiseerde gegevens.

Om scheiding tussen deze rollen aan te brengen, wordt een combinatie van technische en organisatorische maatregelen ingezet. Met als doel om te voorkomen dat iemand over zo veel informatie beschikt dat de pseudonimisering kan worden doorbroken. Dan zou immers geen sprake meer zijn van de vereiste 'onafgebroken gecontinueerde pseudonimisering'.

In praktijk worden de rollen doorgaans verdeeld over verschillende organisaties; een aanbieder van gegevens, een sleutelbeheerder en een afnemer van gepseudonimiseerde gegevens. Zij hebben elkaars ingrediënten nodig om pseudoniemen te maken of om te keren en kunnen het proces niet zelfstandig uitvoeren. Zie figuur 2.

[11] https://www.health-ri.nl/sites/healthri/files/2023-08/MLCF-Nivel%20Report%20country%20comparison%20further%20use%20final.pdf. (zie paragraaf F.4)

[12] Versleuteling en encryptie zijn synoniemen. Versleuteling en pseudonimisering niet.

Figuur 2. Functiescheiding tussen databron, sleutelbeheer en het verwerken van gepseudonimiseerde gegevens.

1.4.2 Omkeerbare pseudonimisering; tweeweg

Omkeerbare pseudonimisering wordt ook wel tweeweg pseudonimisering genoemd. De essentie is dat het mogelijk is om heen en terug te gaan tussen identificerend gegeven en pseudoniem. Het belangrijkste verschil met encryptie van gegevens, is de functiescheiding tussen het maken van de pseudoniemen en het werken met gepseudonimiseerde gegevens. Concreet betekent functiescheiding dus dat een onderzoeker wel met gepseudonimiseerde gegevens werkt maar dat her-identificatie niet mogelijk is zonder tussenkomst van de sleutelbewaarder.

Bij het gebruik van omkeerbare pseudonimisering verplicht de Wkkgz het gebruik van een TTP. Daarbij moeten afspraken gemaakt worden wie- en onder welke condities, mag overgaan tot her-identificatie.

Voor kwaliteitsregistraties betekent dit in de praktijk dat een registratiemedewerker een verzoek kan indienen voor ontsleuteling via de TTP. Afhankelijk van de gemaakte afspraken[13], kan dit verzoek met menselijke tussenkomst of automatisch worden afgehandeld. De zorgaanbieder krijgt als resultaat van deze actie het verzoek om over een bepaalde patiënt aanvullende gegevens aan te leveren.

Voorbeeld
Het patiëntennummer is uniek binnen het ziekenhuis en daarmee een betrouwbaar gegeven om te gebruiken in de communicatie tussen de kwaliteitsregistratie en het ziekenhuis. Door het nummer omkeerbaar te pseudonimiseren, kan een medewerker van de kwaliteitsregistratie het nummer niet lezen, maar wel gebruiken om gericht te communiceren met het ziekenhuis.

1.4.3 Onomkeerbare pseudonimisering; éénweg

Onomkeerbare pseudonimisering wordt ook wel éénweg-pseudonimisering genoemd. De essentie is dat het *niet* mogelijk is om op basis van het pseudoniem terug te gaan naar het oorspronkelijke, identificerende gegeven. In de praktijk wordt hiervoor met zogenaamde 'tokens' gewerkt of wordt een combinatie van cryptografische technieken ingezet.

Het voordeel hiervan is dat ongeautoriseerde openbaring van persoonsgegevens in opzet (privacy by design) voorkomen kan worden. Voor vormen van verwerking waar geen noodzaak is om terug te gaan naar de

[13] Uit door de kwaliteitsregistraties te maken gegevensbeschermingseffectbeoordelingen moet duidelijk worden of hiervoor noodzaak is en zo ja, in welke gevallen. ISO 25237:2107 noemt in dit kader datakwaliteit, ontdubbelen van records en het verkrijgen van aanvullende of follow-up data op individueel niveau.

oorspronkelijke persoonsgegevens, is dit een veilige keuze. Als er in de gepseudonimiseerde registratie blijkt dat de datakwaliteit voor bepaalde variabelen te wensen overlaat, wordt dit zo mogelijk via een heraanlevering over een bepaalde selectie hersteld. Gericht communiceren over specifieke gevallen is hierbij, in tegenstelling tot omkeerbare pseudonimisering, niet mogelijk.

Deze vorm kan bijvoorbeeld worden gebruikt bij onderzoek waarbij men niet terug hoeft te kunnen naar individuele patiënten. De kwaliteitsregistratie kan in dat geval onomkeerbare pseudoniemen uitgeven voor een bepaald onderzoek.

1.5 Pseudonimiseren van direct identificerende persoonsgegevens

Om personen te volgen in de tijd en over locaties heen, zijn identificerende gegevens nodig die zo uniek mogelijk horen bij één specifieke persoon. In de praktijk is daarbij alleen de naam niet voldoende om er daadwerkelijk zeker van te zijn dat het pseudoniem op dezelfde persoon betrekking heeft. Er zijn bijvoorbeeld meerdere personen met de naam Jan Janssen.

Daarnaast is het van belang rekening te houden met eventuele wettelijke (on)mogelijkheden om de bewuste gegevens te verwerken. Het is voor sommige organisaties bij wet geregeld om bijvoorbeeld een gepseudonimiseerd BSN te verwerken terwijl dit voor andere organisaties niet het geval is. Het voordeel van werken met een gepseudonimiseerd BSN, is dat het een globaal uniek en persistent identificerend gegeven is. Dat wil zeggen dat in Nederland iedere burger exact één uniek BSN heeft dat in principe levenslang ongewijzigd blijft.

Bij het gebruik van andere identificerende gegevens als input voor pseudoniemen, is bekend dat de kans op mismatches toeneemt. Bijvoorbeeld door een verschil in notatie of het bestaan van meerdere personen met dezelfde naam, geboortedatum en geslacht. Dat maakt het BSN - uit het oogpunt van koppelbaarheid - een ideale kandidaat om mensen te kunnen volgen over locaties heen en in de tijd. Uiteraard in gepseudonimiseerde vorm om de privacy van de betrokkenen te beschermen.

Echter, omdat kwaliteitsregistraties het BSN *niet* mogen verwerken, moeten zij werken met pseudoniemen gebaseerd op andere (bijzondere) persoonsgegevens:

- Een patiëntnummer is enkel uniek voor een bepaalde zorgaanbieder en daarmee niet geschikt voor het koppelen over bronnen heen. Het is ook niet per definitie stabiel in de tijd[14].
- De combinatie van geboortenaam, geslacht en voorletter, is een combinatie waarmee - met grote mate van waarschijnlijkheid - gekoppeld kan worden in de tijd en over bronnen heen.

Het gebruik van uit meerdere persoonsgegevens samengestelde pseudoniemen per persoon vergroot de kans op koppelingen tussen gegevens uit verschillende databronnen, en daarmee de koppelbaarheid.

Een aantal veelgebruikte combinaties van persoonsgegevens als basis voor pseudoniemen vindt u in de tabel hieronder[15]:

#	Variabelen die onderdeel uitmaken van het pseudoniem
1	Geboortedatum, geslacht, postcode
2	Naam, geboortedatum, geslacht, voorletter
3	Naam, geboortedatum, geslacht
4	Lokaal Patiëntnummer
5	BSN[16]
6	BSN, geboortedatum[17]
7	Geboortedatum, geslacht
8	Geboortedatum

Het is hier van belang te benadrukken dat voor dezelfde persoon meerdere pseudoniemen kunnen worden aangemaakt, mits daarvoor de input aanwezig is. Het kan bij namen die veel op elkaar lijken nuttig zijn gebruik

14 Bijvoorbeeld bij migratie naar een andere EPD leverancier kan overgestapt worden op een andere nummering.
15 Zie bijvoorbeeld de studie van Koot: https://www.researchgate.net/figure/Number-of-Dutch-citizens-per-anonymity-set-size-for-various-quasi-identifiers_tbl2_241888710)
16 *Technisch verwerkbaar, maar op dit moment niet toegestaan voor kwaliteitsregistraties
17 *Technisch verwerkbaar, maar op dit moment niet toegestaan voor kwaliteitsregistraties

te maken van meerdere typen pseudoniemen om te bepalen of het om dezelfde persoon gaat. Daarnaast kunnen deze zowel omkeerbaar als onomkeerbaar worden aangemaakt. Door meerdere typen pseudoniemen aan te maken voor dezelfde persoon, wordt de kans vergroot op succesvolle koppelingen met andere registraties of voor wetenschappelijk onderzoek.

Hoewel het op dit moment niet is toegestaan om op het BSN gebaseerde pseudoniemen voor kwaliteitsregistraties aan te maken wordt hiermee in technische zin wel rekening gehouden dat dit mogelijk moet zijn. In het Obstakel- Verwijdertraject[18] wordt de noodzaak van het gebruik van het BSN voor onderzoek momenteel onderzocht. Daarnaast mag een aantal zorgregistraties wel gebruik maken van een gepseudonimiseerd BSN, let op dit betreft dus geen kwaliteitsregistraties.

2 Een pseudonimiseringsservice voor kwaliteitsregistraties

Door pseudonimisering bij een gespecialiseerde dienstverlener te beleggen die pseudonimisering als service aanbiedt, kunnen zorgaanbieders en kwaliteitsregistraties ontzorgd worden, kan aan functionele en technische eisen worden voldaan en kan door schaalvoordeel efficiencywinst worden behaald. Een pseudonimiseringsservice kan op meerdere manieren gerealiseerd worden. Voor kwaliteitsregistraties is een tweetal modellen voorgesteld:

1. Webservice.
2. Lokale service. Aanleveren van te pseudonimiseren én overige gegevens via pseudonimiseringsdienst aan kwaliteitsregistraties.

Deze modellen houden rekening met de bestaande en beproefde werkwijze voor pseudonimiseren enerzijds en de landelijke visie en ontwikkelingen op het gebied van infrastructuren voor secundair gebruik van zorgdata anderzijds

In beide gevallen worden de gegevens in gestructureerde vorm en conform de daartoe opgestelde specificaties aangeboden aan de service. De specificaties worden opgesteld door de kwaliteitsregistratie. Bepalend voor de aard en vorm van de specificatie zijn de informatiebehoefte, de aan de bron beschikbare gegevens en de - als gevolg van de uitgevoerde data protection impact assessment (DPIA) - te nemen beschermingsmaatregelen om de privacy van de betrokkenen passend te beschermen.

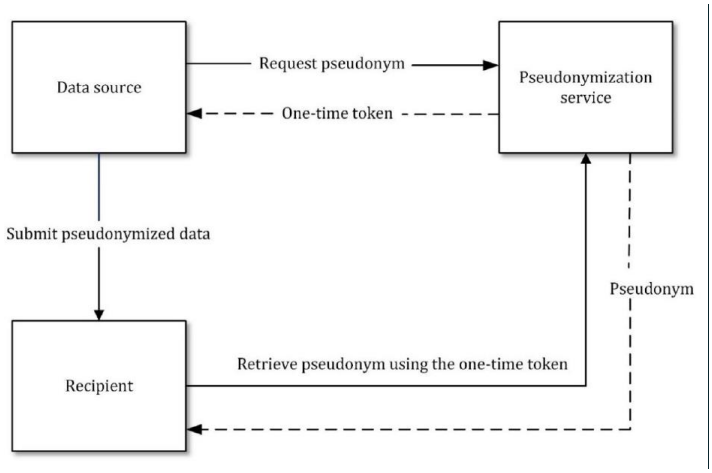
De zorgaanbieder maakt een keuze die passend is voor eigen organisatie. De implementatiemogelijkheden hiervoor lichten we in dit hoofdstuk verder toe.

De hierna beschreven modellen staan beschreven in de norm “NEN7524:2019 Pseudonimisatiedienstverlening”. Een pseudonimisatieservice dient te werken conform deze NEN norm. Omdat er geen certificeringsschema voor deze norm bestaat kan conformiteit met de norm worden vastgesteld middels een door een onafhankelijke externe deskundige uit te voeren assurance onderzoek.

[18] Zie https://www.health-ri.nl/en/participation/obstakel-verwijder-traject.

2.1 Webservice

In dit model vraagt de zorgaanbieder via een beveiligde webservice pseudoniemen aan bij de pseudonimisatieservice. Als resultaat ontvangt de zorgaanbieder pseudoniemen die zijn versleuteld voor de kwaliteitsregistratie.



Figuur 3 Webservice voor pseudonimisering

De zorgaanbieder voegt de versleutelde pseudoniemen toe aan de aan de kwaliteitsregistratie te versturen gegevens. De kwaliteitsregistratie kan vervolgens de versleutelde pseudoniemen omwisselen voor definitieve pseudoniemen bij de pseudonimisatieservice.

In opzet voor dit model wordt uitgegaan van op basis van Zorginformatiebouwstenen (ZIB's) gestructureerde data die in HL7 FHIR formaat wordt aangeboden aan de pseudonimisatieservice. De pseudoniemen worden ontleend aan het 'nl core patient' profiel[19]. Deze werkwijze sluit aan bij de landelijke afspraken op het gebied van het uitwisselen van zorginformatie.

Kenmerken van deze aanleverwijze:

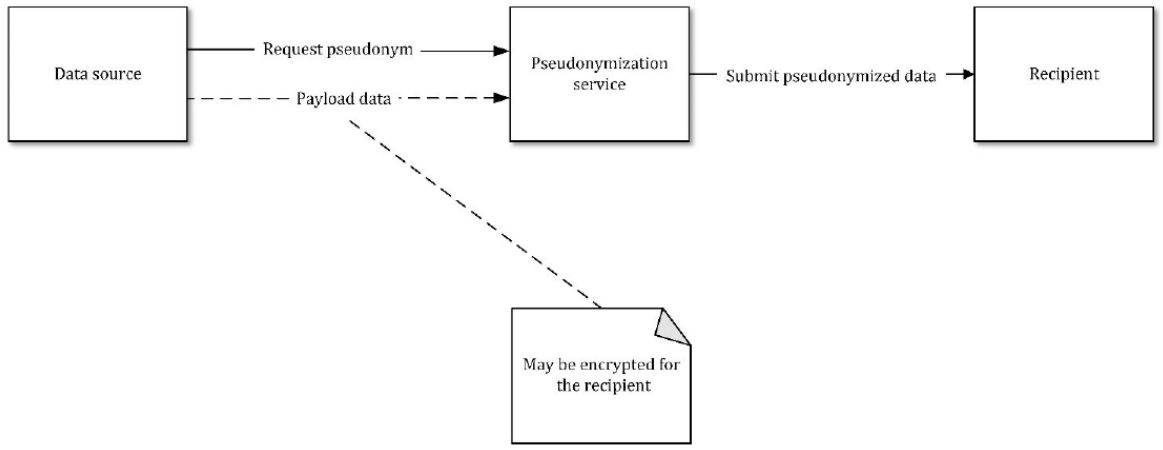
- De zorgaanbieder stuurt (als bron) de te pseudonimiseren persoonsgegevens naar de TTP middels een API-aanroep;
- Daarbij maakt het ziekenhuis gebruik van een beveiligde internetverbinding (TLS);
- De TTP genereert de pseudoniemen en stuurt deze retour aan het ziekenhuis. Het ziekenhuis beschikt daarmee over zogenaamde 'bronpseudoniemen'. De TTP blijft beheerder van de sleutels;
- De zorgaanbieder levert deze bronpseudoniemen en de inhoudelijke gegevens via eigen kanalen aan (de verwerker van) de registratiehouder;
- De (verwerker van de) registratiehouder biedt middels een API-aanroep de pseudoniemen voor conversie aan bij de TTP. De TTP zet de bronpseudoniemen om naar koppelbare pseudoniemen.
- De (verwerker van de) registratiehouder ontvangt de koppelpseudoniemen en gebruikt deze om de informatieproducten te maken;
- De bronpseudoniemen hebben - uit oogpunt van beveiliging - een beperkte houdbaarheid. Dat betekent dat de pseudoniemen na een bepaalde periode niet meer te converteren en daarmee niet langer koppelbaar zijn. Het is dus van belang dat de pseudoniemen binnen een bepaalde periode na het aanmaken, worden geconverteerd naar lang te bewaren koppelpseudoniemen.

De komende maanden wordt deze werkwijze in pilotverband beproefd en verder uitgewerkt.

[19] https://simplifier.net/nictiz-r4-zib2020/nlcorepatient

2.2 Model 2. Lokale service

De zorgaanbieder levert in dit model alle voor de kwaliteitsregistratie bestemde gegevens aan via de pseudonimisatieservice. Deze levert de gepseudonimiseerde gegevens door aan de kwaliteitsregistratie.



Figuur 4 Lokale service voor pseudonimsering

Deze werkwijze wordt vanuit zorgaanbieders al jaren toegepast, bijvoorbeeld voor het aanleveren van gegevens aan het DBC Informatiesysteem, de Landelijke Basisregistratie Ziekenhuiszorg, Pathologiegegevens.

Naast de genoemde HL7 FHIR structuur, wordt in dit model ook input geaccepteerd in een afwijkend formaat voor zorgaanbieders die nog niet in staat zijn om HL7 FHIR aan te leveren.

Kenmerken van deze aanleverwijze:

- De software wordt lokaal geïnstalleerd;
- De eerste pseudonimisering vindt direct plaats aan de bron;
- Door pseudonimisering aan de bron verlaten de oorspronkelijke persoonsgegevens nooit het domein van de zorgaanbieder;
- De inhoudelijke gegevens zijn onderdeel van de aanlevering. Deze informatie wordt versleuteld en is niet toegankelijk voor de TTP. Het gehele bestand wordt op veilige manier (TLS) verzonden.
- Een dergelijke software en werkwijze (aanlevermodule/Privacy- en Verzend Module) is al bekend bij alle ziekenhuizen onder andere vanwege de aanleveringen aan het DBC-informatiesysteem (DIS) van de Nederlandse Zorgautoriteit (NZa), de Landelijke Basisregistratie Zorg (LBZ) van DHD en Palga.

3. Verdieping implementatie in de praktijk

Hoofdstuk 3 van deze handreiking, over de praktische implementatie van pseudonimisatie, volgt in 2024 naar aanleiding van een pilot. In de pilot worden enkele scenario's van implementatie gesimuleerd om te kunnen beschrijven wat er in de praktijk bij de implementatie komt kijken. Hierin komen onderwerpen rondom pseudonimisatie aan de orde waar de wijziging van de Wkkgz hoogstwaarschijnlijk impact op zal hebben. Daarnaast zullen we in hoofdstuk 3 ingaan op scenario's waarvan analyse uit wijst dat ze in de praktijk zouden moeten werken en (waarvan na uitgebreid testen is gebleken dat ze) kunnen voldoen aan wet- en regelgeving en of dat dan ook gewenst is.

Dit hoofdstuk zal twee uitwerkingen kennen:

1) Een uitwerking gericht op de impact, mogelijke scenario's en resultaten van geteste scenario's die relevant zijn voor zorgaanbieder.
2) Een uitwerking gericht op de impact, mogelijke scenario's en resultaten van geteste scenario's die relevant zijn voor registratiehouders en dataverwerkers.

Beide uitwerkingen zullen gepubliceerd worden op de website van het SSC-DG.

4. Vervolgstappen

Naast deze handreiking wordt er gewerkt aan notitie(s) waarin uitwerking wordt gegeven aan:

1. Eisen die aan de service en de dienstverlener van de pseudonimisering worden gesteld
2. Governance op de pseudonimisering dienstverlening
3. Kosten en wijze van inkopen van pseudonimisering
4. Rol van EPD leveranciers

Vragen?
Mocht u vragen hebben over deze handreiking of het onderwerp in het algemeen? Neem dan contact op met het SSC-DGC via https://ssc-dg.nl/contact/, info@ssc-dg.nl of bel 030-8990311.