Onderstaand leest u de antwoorden van de Kerngroep Pseudonimiseren zorggegevens voor hergebruik SSC-DG op de vragen die de Expert Community Secundair Datagebruik onlangs aan VWS heeft gesteld met betrekking tot de vereiste pseudonimisering.

1. **Is de beschrijving van ‘technische maatregelen rondom het delen van gegevens’ voldoende duidelijk? In hoeverre is er ruimte voor verschillende interpretaties en in hoeverre kunnen die de huidige praktijk en de verdere ontwikkeling van hergebruik frustreren?**

**[Antw.]** De beschrijving van de technische maatregelen kan verduidelijkt worden door gebruikte terminologie helder te definiëren. Bijvoorbeeld het begrip “onafgebroken gecontinueerd”.

Aanvullend kunnen deze definities opgenomen worden in een centraal beheerde thesaurus. Door het beheer van de thesaurus open te stellen voor vertegenwoordigingen uit andere organisaties op het gebied van secundair gebruik, kunnen we voornoemde frustraties voorkomen.

De Kerngroep pseudonimiseren van de SSC-DG stelt handreikingen op voor Zorgaanbieders en Registratiehouders over hoe om te gaan met de wettelijke eisen voor pseudonimiseren van zorgdata voor hergebruik in kwaliteitsregistraties. In deze handreikingen zijn ook (concept-) definities opgesteld die ter beoordeling én opname ingebracht worden in de projectgroep ‘Thesaurus definities kwaliteitsregistraties’.

1. **Is de beschrijving van technische maatregelen rondom het delen van gegevens niet te technisch en te specifiek, waardoor het minder goed mogelijk is om mee te gaan met huidige en nieuwe ontwikkelingen? Hierbij denken we aan een algemenere beschrijving, passend bij de ambities zoals verwoord in de Nationale visie en Strategie op het gezondheidsinformatiestelsel.**

**[Antw.]** Wij zijn van mening dat de huidige beschrijving van technische maatregelen rondom het delen van gegevens toekomstige ontwikkelingen niet in de weg staat. Op korte termijn is echter wel duidelijkheid nodig, voor zowel zorgaanbieders als registratiehouders omdat de wijziging van de Wkkgz een technische maatregel als pseudonimisering vereist.

De nadruk op pseudonimiseren als één van de technische maatregelen is daarbij een bewuste keuze omdat het een bewezen werkzame techniek betreft. Deze wordt momenteel breed toegepast en biedt een goede balans tussen het beschermen van de privacy en het volgen van individuen voor kwaliteitsdoeleinden.   
*(Zie ook de recente publicatie van E.B. van Veen en R. Verheij in opdracht van Health-RI*)[[1]](#footnote-2).

1. **Kan er in de Uitvoeringsregeling verwezen worden naar de NEN 7524 en de verschillende vormen van pseudonimisering, welke hierin worden beschreven, of naar de normering zelf zodat ook toekomstige wijzigingen worden meegenomen?**

**[Antw.]** Advies aan VWS; verwijzen naar normen als NEN 7524 en NEN 7510 is gebruikelijk om wet- en regelgeving zo veel mogelijk technologie-neutraal te houden. De NEN 7524 beschrijft een aantal varianten van pseudonimisering. Inhoudelijk is er geen bezwaar om naar deze norm te verwijzen.

1. **In hoeverre staan de voorgenomen wijzigingen de mogelijkheden om terug te gaan naar de patiënt in de weg?**

**[Antw.]** De voorgenomen wijzigingen staan die weg terug technisch niet in de weg. Wel zal van geval tot geval de afweging gemaakt moeten worden in hoeverre de weg terug noodzakelijk is. Een dergelijke afweging hoort thuis in de gegevensbeschermingseffectbeoordeling die iedere kwaliteitsregistratie verplicht is uit te voeren.

1. **In hoeverre laten de voorgenomen wijzigingen ruimte voor het koppelen van gegevens waarvan we nu nog niet weten dat ze nodig zijn?**

**[Antw.]** Die ruimte is er. De volgende implementaties (niet uitputtend) zijn denkbaar:

1. Koppelen op basis van pseudoniemen:
   1. Omkeerbare (tweeweg) pseudoniemen kunnen worden teruggebracht naar de onderliggende, identificerende gegevens door deze te ontsleutelen. Vervolgens kan, mits de te koppelen set dezelfde identificerende gegevens bevat, op basis van deze gegevens gekoppeld worden.
   2. Onomkeerbare (éénweg) pseudoniemen kunnen gekoppeld worden, mits de te koppelen bronnen op vergelijkbare wijze gepseudonimiseerd zijn. Dat kan bijvoorbeeld tussen dataverzamelingen die op basis van, de in opdracht van VWS opgestelde, pseudonimiseringsmethode[[2]](#footnote-3) zijn gepseudonimiseerd.
2. Een waarschijnlijkheidskoppeling op geaggregeerd niveau.
3. **In hoeverre sluiten de voorgenomen wijzigingen aan bij de plannen zoals verwoord in de visie en strategie secundair datagebruik?**

[**Antw.]** In de opzet wordt rekening gehouden met de visie en strategie secundair datagebruik door een servicemodel te hanteren waarbij pseudoniemen kunnen worden opgevraagd en middels een API call omgezet naar een webservice. In meerdere van de visie en strategie afgeleide architectuurmodellen is een pseudonimiseringsservice voorzien. Met stakeholders als Health-RI, Cumuluz, OncoNext en VZVZ wordt getoetst of en in hoeverre deze opzet aansluit. Dat blijkt tot nu toe steeds het geval.

1. **In hoeverre hebben de wijzigingen invloed op de mogelijkheden om wetenschappelijk (beleids-)onderzoek te doen met gegevens die verzameld worden in het kader van de Wkkgz?**

**[Antw.]** Dit is meer een juridische dan een technische vraag. Doorleveren of koppelen van gegevens voor andere doelen dan de in de Wkkgz geboden grondslag, moet voldoen aan een andere binnen de AVG mogelijke grondslag. Door gebruik te maken van een Trusted Third Party (TTP), die tevens een regiefunctie op sleutelbeheer vervult, zijn er technisch gezien geen belemmeringen om de gegevens ook voor wetenschappelijk (beleids-) onderzoek te verwerken.

1. **Hoe moet het begrip ‘continue pseudonimisering’ worden geïnterpreteerd en gehanteerd? Stel: je past tweeweg-pseudonimisering toe en keert terug naar de bron - bijvoorbeeld met een vraag over de gegevens betreffende outlyers-, is dit dan een onderbreking van de continuering van de pseudonimisering? (Hierbij is de enige ontsleuteling aan de kant van de bronhouder.)**

[**Antw.]** Dit is geen onderbreking van de continuering van de pseudonimisering. Het begrip ziet op de afnemer van gepseudonimiseerde data, in dit geval de kwaliteitsregistratie. Zie ook het antwoord bij vraag 4.

In de handreiking voor Zorgaanbieders die momenteel in voorbereiding is, hebben we de volgende toelichting op dit begrip opgenomen:

*De pseudonimisering van gegevens moet zodanig zijn dat de ontvanger van de gepseudonimiseerde gegevens steeds in staat is om individuen te herkennen onder pseudoniem en niet op basis van andere identificerende gegevens. ‘Onafgebroken gecontinueerd’ is in deze omschrijving met name van toepassing op de afnemer (i.e. de registratiehouder van een kwaliteitsregistratie) van pseudoniemen. Tegelijkertijd dient de pseudonimisering voor dezelfde persoon voor hetzelfde doel steeds dezelfde waarde krijgen. Dit sluit communicatie tussen afnemer (bijvoorbeeld een kwaliteitsregistratie) en aanbieder (ziekenhuis) over individuen voor specifieke gevallen overigens niet geheel uit. Technische en organisatorische maatregelen voorkomen ongeautoriseerde doorbreking. Geautoriseerde doorbreking kan alleen verlopen via een Trusted Third Party, waarbij deze iedere transactie logt en daarmee transparant maakt voor alle belanghebbenden. Op deze wijze is het mogelijk om gericht aanvullende data op te vragen over individuen. Zie paragraaf 3.4.1 omkeerbare pseudonimisering.*

1. **Wat is de definitie van de ‘bron’ van de data? Is dat de zorgverlener of zorgorganisatie, of kan dit ook bij een dataverwerker zijn? Is het mogelijk dat de pseudonimisering vanuit deze verwerker gebeurt (oftewel in een latere stap van de dataverwerking)?**

**[Antw.]** De zorgaanbieder is de bron, maar de zorgaanbieder kan ook een dataverwerker aanwijzen die optreedt als verwerker van de brondata namens de zorgaanbieder.

1. **In hoeverre impliceert te term ‘pseudonimisering aan de bron’ dat er sprak zou moeten zijn van tweeweg- of juist eenweg-pseudonimisering?**

**[Antw.]** De term ‘pseudonimisering aan de bron’ staat los van de vorm van pseudonimisering. Deze term ‘*aan de bron’* zegt iets over de plaats in het proces waar de pseudonimisering wordt gestart. De vorm van pseudonimiseren is een afgeleide van de in de gegevensbeschermingseffectbeoordeling onderkende risico’s en de maatregelen om deze tot een aanvaardbaar niveau te reduceren.

1. **Is er rekening gehouden met de implicaties van de beschrijving van tweeweg-pseudonimisering op de rol van een TTP? Zoals nu beschreven in de Memorie van Toelichting wordt de TTP centraal gezet voor alle koppelingen. Aandachtspunt wat ons betreft is het eisenpakket dat aan TTP’s gesteld zouden moeten worden, plus monitoring op deze eisen.**

**[Antw.]** Er wordt momenteel een plan van aanpak opgesteld voor een pseudonimiseringsservice. Dit in opdracht van de data governance-commissie kwaliteitsregistraties. Onderdeel van dat plan is de afweging van voor- en nadelen van het beleggen van de rol bij één of meerdere TTP’s. En er is een programma van eisen opgesteld waaraan een TTP voor deze rol zou moeten voldoen.

1. https://www.health-ri.nl/nl/nieuws/vergelijking-van-wet-en-regelgeving-europa-voor-hergebruik-van-gezondheidsdata-voor [↑](#footnote-ref-2)
2. Zie <https://www.zorgttp.nl/wp-content/uploads/2023/01/NEN-pseudonimisering-specificatie-voorstel-VWS-1.0.pdf>. [↑](#footnote-ref-3)