Shared Service Center
Data Governance

FAQ pseudonimiseren voor registratiehouders en dataverwerkers

V2.0, 9 oktober 2025

De vragen in deze FAQ zijn onderverdeeld in 6 categorieën:

1. Proces – input
2. Proces – output
3. Methodiek
4. DPIA
5. Financiering
6. Algemeen/overig

1. Proces – input

1. **Voor kwaliteitsregistraties zijn o.a. geslacht, geboortedatum en postcode soms onversleuteld nodig voor kwaliteitsbewaking. Hoe krijgen we deze gegevens als de wet van kracht is?**
   In de beschrijving van de registratie moet duidelijk worden gemaakt welke persoonsgegevens nodig zijn. In de DPIA moet vervolgens worden onderbouwd waarom deze gegevens soms zonder versleuteling gebruikt moeten kunnen worden, bijvoorbeeld in een bewerkte vorm zoals generalisatie (geboortejaar in plaats van geboortedatum) of afkappen (alleen de vier cijfers van de postcode). In de DPIA-vraag over pseudonimiseren wordt dit verder toegelicht met voorbeelden. Deze gegeneraliseerde of afgekapte gegevens moeten vervolgens door de verstrekker apart worden aangeleverd.

2. **Registratiehouders ontvangen vragen vanuit de zorgaanbieders m.b.t. (gepseudonimiseerde) aanleveringen. Hoe kan een registratiehouder zorgaanbieders het beste informeren over wijzigingen in de kwaliteitsregistratie m.b.t.:**
   - **Aanleveringen via XML-berichten uit het epd**
   - **CSV's die in een web portal worden geüpload**
   - **Handmatige invoer in een web portal (wordt ook gebruikt voor correcties n.a.v. kwaliteitscontroles)**

- Aanleveren vanuit het epd: doe een API-call vanuit het epd (of elders binnen de omgeving van de zorgaanbieder) en neem de tijdelijke pseudoniemen op in de datastroom vanuit het epd richting de kwaliteitsregistratie.
- CSV aanleveren vanuit een webportal: portal aanpassen zodanig dat met API wordt gecommuniceerd. Voeg de pseudoniemen toe aan het bestand. Alternatief: zorg ervoor dat er reeds in het ziekenhuis pseudoniemen worden opgevraagd die aan de CSV worden toegevoegd voorafgaand aan het uploaden.
- Handmatige invoer webportal: portal laten praten met de service voorafgaand aan opslaan/doorsturen gegevens.

3. **Bij aanlevering vanuit het epd, moeten epd's ook iets aanpassen voor pseudonimisatie?**
   De gegevens die gepseudonimiseerd moeten worden, worden – al dan niet samen met de zorginhoudelijke data – uit het epd of andere zorginformatiesystemen geëxtraheerd. Dat gebeurt nu ook al. Het verschil is (of kan zijn*) dat de direct herleidbare persoonsgegevens

vervolgens (vóór verstrekking) door de TTP gepseudonimiseerd moeten worden. Wij hebben echter onvoldoende inzicht in de extractieprocessen om te kunnen beoordelen of deze processen voor de pseudonimisering aangepast moeten worden.

* Sommige registratie maken ook in de huidige situatie al gebruik van een TTP.

4. **Welke ondersteuning is er voor FHIR-aanleveringen?**
   Die is voorzien, maar we zijn er tijdens de pilots niet in geslaagd om hiermee te testen vanuit lopende gegevensuitwisselingen. Conceptueel is duidelijk waar de pseudoniemen toegevoegd kunnen worden; aan de patient resource kunnen elementen worden toegevoegd die de pseudoniemen bevatten. Er wordt met meerdere dataverwerkers gewerkt aan nadere detaillering van dit proces.

5. **Hoe werkt het werken met tijdelijke pseudoniemen indien gebruikt gemaakt wordt van invoer via web forms van de registratiehouder?**
   Voor webformulieren kan door de dataverwerker interactie plaatsvinden met de pseudonimisatieservice voorafgaand aan het doorsturen van de gegevens. De SDB Groep heeft dit bijvoorbeeld voor de LROI geïmplementeerd. Velden die persoonsgegevens bevatten worden tijdens de sessie omgezet naar pseudoniemen. Ook met dataverwerker IVZ is voor de QRNS-registratie in een pilot getest met het opvragen van pseudoniemen vanuit een webformulier. Zowel de tijdelijke als definitieve pseudoniemen worden daar binnen één sessie toegevoegd aan de dataset. Het is voor aanleveringen via een webformulier van belang dat duidelijk beschreven wordt wie verantwoordelijk is voor welke stap in het aanleverproces.

2. Proces – output

6. **Welke items moeten gepseudonimiseerd worden?**
   De persoonsidentificerende of direct identificerende gegevens, moeten gepseudonimiseerd worden. Hieronder wordt verstaan: burgerservicenummer (uitsluitend voor registraties die een BSN mogen verwerken), geboortenaam, voorletter(s), geboortedatum, geslacht, postcode, straatnaam, huisnummer, (eventueel) toevoeging huisnummer. Indien de registratie vereist dat één of meer van deze items niet of niet geheel gepseudonimiseerd worden dan dient dit in de DPIA gemotiveerd te worden.

7. **Mag het BSN gebruikt worden in de kwaliteitsregistratie?**
   Nee, het BSN mag niet gebruikt worden. De pseudonimisatieservice is wel in staat om BSN-pseudoniemen te maken vooruitlopend op wetgeving én voor bij wet aangewezen gegevensverwerkingen die dit nummer wel mogen pseudonimiseren.

8. **Welke alternatieven zijn er indien het BSN niet gebruikt kan worden om datasets te koppelen?**
   Het koppelen van datasets kan plaatsvinden op andere kenmerken of combinaties van kenmerken van de patiënt. Hiermee wordt bedoeld dat er een koppeling gemaakt wordt op basis van (bijvoorbeeld) geboortenaam + geboortedatum + geslacht van de patiënt.

9. **Als je op dit moment geen naam registreert in je registratie, betekent dit dat je dit veld moet toevoegen aan je registratie omdat deze nodig is voor pseudonimisatie en een hoog koppelpercentage?**
   Naam toevoegen is niet verplicht. Pseudonimiseren is geen doel op zich. Naam is wel nodig om samengestelde pseudoniemen te kunnen maken waarvan de naam onderdeel is. Die pseudoniemen hebben vooral tot doel om te kunnen koppelen met data van andere verstrekkers en andere registraties.

   - Indien er koppelingen plaatsvinden is het opnemen van de naam zeker aan te bevelen omdat dit de sensitiviteit en specificiteit van de koppeling verhoogt.
   - Indien er geen koppelingen plaatsvinden is het toevoegen van de naam aan de gegevensset in principe niet nodig en in het kader van dataminimalisatie zelfs niet wenselijk.

10. **Als een ziekenhuis in een invoerportaal direct een sleutel ziet is dit dan een tijdelijke sleutel?**
    Bij onomkeerbare pseudoniemen ziet het ziekenhuis enkel een tijdelijk pseudoniem.
    Bij omkeerbare pseudoniemen ziet het ziekenhuis het definitieve pseudoniem. Daarom adviseren we om hiervoor slechts lokaal unieke administratieve gegevens te gebruiken, zoals het patiëntennummer. Dit kan gebruikt worden voor follow-up en terugkoppelingsdoeleinden.

11. **Wordt de mogelijkheid om patiënten voor langere tijd op te volgen beperkt, bijvoorbeeld door pseudoniemen op te stellen op basis van postcode?**
    Het klopt dat door een wijziging in postcodes door verhuizingen de koppelbaarheid op basis van dat pseudoniem afneemt. Dit is de reden waarom er meerdere pseudoniemen voor meerdere doeleinden worden ondersteund. Pseudoniemen waarin de postcode is opgenomen worden met name toegepast bij vragen waar naar regio's of huishoudens wordt gekeken. Uiteraard geldt hierbij dezelfde beperking met betrekking tot de stabiliteit van het pseudoniem in de tijd. Het is daarom mogelijk om voor een bepaald record meerdere bekende postcodes in combinatie met het moment waarop deze is vastgelegd aan te leveren, om zo de koppelbaarheid te vergroten.

3. Methodiek

12. **Wordt pseudonimisatie als eenweg versleuteling gezien?**
    De pseudonimisatie is zowel omkeerbaar als onomkeerbaar (eenweg) te implementeren. Tevens kunnen beide implementaties naast elkaar bestaan binnen dezelfde kwaliteitsregistratie. Voor terugkoppeling ligt een omkeerbaar pseudoniem voor de hand, bij voorkeur gebaseerd op een lokaal uniek gegeven in plaats van een globaal uniek gegeven. Het omkeerbaar pseudoniem is enkel omkeerbaar voor de zorgaanbieder. Voor koppeling met andere registraties voldoen onomkeerbare pseudoniemen. De keuzes die hierin gemaakt worden legt de registratiehouder vast in de DPIA.

13. **Wordt het verplicht om het patiëntennummer omkeerbaar te pseudonimiseren?**
    Omdat de registratiehouder zonder toegang tot het epd van de zorgaanbieder het patiëntnummer niet kan koppelen aan een identificeerbare persoon, kan het patiëntnummer in zichzelf al als een pseudoniem voor de patiënt beschouwd worden. Het patiëntnummer hoeft derhalve in principe niet gepseudonimiseerd te worden. Echter, omdat de

zorgaanbieder verantwoordelijk is voor het aanleveren van gepseudonimiseerde data aan de registratiehouder is dit uiteindelijk een keuze van de zorgaanbieder.

14. **Is het verplicht om een koppelpseudoniem op te nemen?**
    Uitgangspunt is dat de registratiehouder niet over direct herleidbare gegevens beschikt. Alle aanwezige persoonskenmerken (zoals achternaam, geboortedatum, geslacht, etc.) in de dataset van de kwaliteitsregistratie worden gepseudonimiseerd. Daarnaast kunnen hieruit verschillende logische combinaties worden gevormd tot samengestelde pseudoniemen. Deze pseudoniemen zijn in principe beschikbaar voor de registratiehouder. Het is aan de registratiehouder om te bepalen welke pseudoniemen worden gebruikt en met welk doel (zoals gegevenskoppeling). Als er geen koppelingen worden gemaakt met externe bronnen of met gegevens van dezelfde patiënt die afkomstig zijn van andere zorgaanbieders, dan is het gebruik van een koppelpseudoniem niet verplicht.

    Indien koppelingen met externe bronnen en/of andere kwaliteitsregistraties op een later moment aan de orde komen, is het mogelijk voor deze doeleinden alsnog een pseudoniem samen te stellen. Ter input moeten hiervoor wel de benodigde persoonsgegevens opgevraagd worden bij de zorgaanbieders (bijv. aan de hand van het patiëntnummer).

15. **Worden alle kwaliteitsregistraties die door dezelfde registratiehouder worden onderhouden met dezelfde sleutel gepseudonimiseerd?**
    Dat is een keuze. Technisch is het mogelijk om per kwaliteitsregistratie een specifieke sleutel te hanteren. Dit vergroot de privacybescherming, doordat registraties dan onderling niet zonder tussenkomst van de TTP koppelbaar zijn. Door middel van domeinconversie via de TTP is het mogelijk om deze registraties nog steeds met elkaar te koppelen. Het staat een kwaliteitsregistratie vrij om in de DPIA te beargumenteren dat het combineren van verschillende gevoerde registraties binnen één pseudonimisatiedomein noodzakelijk/wenselijk is.

    Let wel dat hierbij het uitgangspunt moet zijn dat er domeinspecifieke pseudoniemen gebruikt worden (privacy by default). Een gegronde onderbouwing in de DPIA is hierbij vereist, waarbij een onderdeel van de argumentatie de belangenafweging tussen privacy winst en kosten van tenuitvoerlegging van de maatregelen moet bevatten. Argumenten gerelateerd aan het vergemakkelijken van koppelingen worden hierbij niet als gegrond beschouwd. Daarnaast geldt hier ook het principe van subsidiariteit waarbij het koppelen via de TTP minder privacyrisico's met zich meebrengt, en hierdoor de voorkeur betreft.

16. **Wanneer gebruik je de lokale pseudonimiseringsdienst en wanneer de webservice?**
    Als kwaliteitsregistratie is het verstandig om eerst te inventariseren van welke aanleverwijze de zorgaanbieders gebruik gaan maken. Vervolgens kun je besluiten om één van beide of beide wijzen te ondersteunen. De definitieve pseudoniemen zijn in beide gevallen identiek voor dezelfde patiënten. Het is verstandig om rekening te houden met beide aanleverwijzen. Dit biedt mogelijk ook flexibiliteit als het gaat om de verschillende gegevensstromen en de onderliggende applicaties.

17. **Hoe wordt gezorgd dat registratiehouders koppelingen kunnen maken tussen verschillende registraties? (denk aan levermetastasen bij darmkanker en openhartoperatie na dotterbehandeling)**
    De toegepaste methode voor pseudonimisering voorziet in de mogelijkheid om reeds gepseudonimiseerde gegevens te vertalen tussen verschillende registraties. Deze omzetting noemen we domeinconversie.
    Dit is relevant, omdat ook op een later moment onverwachte koppelingen tussen registraties kunnen worden gevraagd. In dat geval moet TTP in staat zijn om verschillende pseudoniemen terug te leiden naar één identiteit.

18. **Voor de koppeling met andere partijen, zoals het CBS, is het noodzakelijk om een RIN-persoon ID te kunnen maken. Daarvoor zijn een aantal variabelen nodig die ook beoogd worden voor de pseudonimiseringsdienst. Worden deze variabelen door de ziekenhuizen, naast de pseudonimisering, ook als onderdeel van de kwaliteitsregistratie als variabele aangeleverd?**
    Indien de registratiehouder deze variabele in haar kwaliteitsregistratie uitvraagt dan dient de zorgaanbieder deze variabele ook aan te leveren.

19. **Hoe kan koppeling met CBS plaatsvinden als er geen beschikking is tot identificeerbare gegevens? En zijn hier extra kosten aan verbonden?**
    Koppelen kan op basis van pseudoniemen binnen de omgeving van het CBS. De hiervoor benodigde persoonsgegevens moeten als input aan het pseudonimisatieproces worden aangeboden. Uitgangspunt is dat door centrale inkoop geen aanvullende kosten voor dergelijke verwerkingen door de pseudonimiseringsdienst worden gerekend. Hierover moet nog besluitvorming plaatsvinden.

20. **Wat is de betrouwbaarheid (sensitiviteit en specificiteit) van koppelingen?**
    Er is een aantal studies[1] gedaan naar dit onderwerp. Onderstaande afbeelding toont de sensitiviteit en specificiteit bij verschillende combinaties van identificerende gegevens ten opzichte van een gouden standaard waarbij koppeling op basis van het BSN plaatsvindt.

Resultaten

Koppel scenario	NAW pseudoniemen							Sensitiviteit	Specificiteit	Administratieve tweelingen
	geslacht	naam	geb datum	geb jaar	voorl	PC4	PC6	%	%	%
1	X	X	X		X			93,8	99,7	1,1
2	X		X				X	81,2	99,7	0
3	X	X		X				96,2	79,9	70,9
4	X	X		X	X	X		85,3	99,6	0
5	X		X		X	X		86,0	99,4	0,8
6	X	X			X	X		82,9	97,1	12,7
7	X	X	X		X	X		85,3	99,7	0
8	X	X	X					97,4	97,8	5,6

We adviseren om meerdere pseudoniemen per persoon te registreren. De tabel toont aan dat pseudoniemen waarin de postcode (deels) is verwerkt een hoge specificiteit kennen.

Zie https://www.zorgttp.nl/project/bbmrivalidatiestudiebsngegevenskoppelingen/

Nadeel is dat de postcode vaak niet stabiel is in de tijd. Door ook het pseudoniem op basis van geboortenaam, geboortedatum, geslacht en voorletter te registreren (nr. 1 in de figuur) kan bijvoorbeeld het aantal administratieve tweelingen met pseudoniem nr. 2 uit de figuur worden verminderd.

21. **Hoe zijn datavalidaties die registratiehouders nu uitvoeren, waarbij data in de kwaliteitsregistratie wordt vergeleken met data in het epd, nog mogelijk na pseudonimisering?**
    Uitgangspunt is dat de kwaliteitsregistratie slechts over gepseudonimiseerde en dus niet over direct tot de persoon herleidbare gegevens beschikt. Door te kiezen voor voor de zorgaanbieder omkeerbare pseudoniemen blijft de mogelijkheid tot validatie behouden.

22. **Vindt de encryptie plaats bij de bron (het ziekenhuis) of bij de TTP?**
    Als de zorgaanbieder het pseudonimiseren uitbesteedt aan een verwerker (TTP), dan moet dit gezien worden als pseudonimisatie onder verantwoordelijkheid van de bron (de zorgaanbieder). Pseudoniemen worden bij de TTP gegenereerd op basis van een encryptiestap. Dat is ook de essentie van het inzetten van een pseudonimisatiedienst. In zowel de lokale als de webservice vinden de eerste stappen in het pseudonimisatieproces plaats aan de bron.

23. **Blijft de bytecode hetzelfde op het moment dat de domeinhouder verandert?**
    Iedere domeinhouder ontvangt domeinspecifieke pseudoniemen.

24. **Waarom worden geen aparte pseudoniemen gemaakt van bijvoorbeeld de gegevens geboortenaam, geboortedatum en postcode?**
    Een pseudoniem per variabele hanteren gaat ten koste van de privacy van de betrokkene. Als je de postcode los pseudonimiseert dan kun je per postcode nagaan wie op deze postcode bekend zijn. Voor goede pseudonimisering wordt rekening gehouden met de criteria linkability, inference en singling-out uit de AVG. Door samengestelde pseudoniemen te hanteren neemt de kans op herleiding af zonder het onderscheidend vermogen te verliezen.

25. **Pseudonimisering betreft niet alleen encryptie maar ook voorbewerking, bijvoorbeeld bij patiëntnamen dient rekening gehouden te worden met verschillende aanleveringen door ziekenhuizen doordat anders wordt omgegaan met diakrieten, koppeltekens, etc. Hoe wordt hier mee omgegaan?**
    De service normaliseert de input conform geen vast schema waarnaar in de presentatie wordt verwezen. Namen worden bijvoorbeeld genormaliseerd door diakritische tekens te vervangen door de basisletter. Jansen/janssen wordt niet herkend als het over dezelfde persoon gaat.

26. **Hoe ga je om met pseudonimisatie van historische data als het ziekenhuis in de afgelopen jaren gefuseerd is of bijvoorbeeld een nieuw systeem heeft gekregen en dus ook de historische data niet meer beschikbaar heeft?**
    Conversiescenario's waarbij de oorspronkelijke input aanwezig is kunnen met de beoogde service worden afgehandeld. Als de historische data niet meer beschikbaar is dan kan enkel op basis van waarschijnlijkheidskoppelingen met reeds aanwezige data-elementen onderzocht worden voor welk deel van de data conversie mogelijk is. Koppelen op basis van pseudoniemen die input nodig hebben die niet langer beschikbaar is, is niet mogelijk.

27. **Welke aanpassingen moeten gedaan worden voor het omzetten van een tijdelijk pseudoniem naar een definitief pseudoniem?**
    Het omzetten van een tijdelijk naar een definitief pseudoniem vraagt om interactie met de pseudonimisatiedienst als gebruik wordt gemaakt van de webservice. De eerste interactie is tussen zorgaanbieder en de service om een tijdelijk pseudoniem te verkrijgen. De tweede tussen de kwaliteitsregistratie en de service om een definitief pseudoniem te verkrijgen. Documentatie waarin de interactie met de pseudonimisatieservice is beschreven wordt beschikbaar gesteld.

    Voor de lokale service vinden de pseudonimisatiestappen plaats binnen de pseudonimisatieketen die door de pseudonimisatiedienst beschikbaar wordt gesteld. Die keten bestaat uit de lokale verzendmodule, de centrale module TTP en de lokale ontvangst/afhaalmodule.

28. **Vindt omkeerbaarheid plaats middels hashing?**
    Nee. Hashing maakt wel onderdeel uit van de methodebeschrijving voor het maken van onomkeerbare pseudoniemen. Voor omkeerbare pseudoniemen wordt gebruikgemaakt van encryptie.

29. **Kan een pseudoniem over de tijd heen altijd omkeerbaar blijven?**
    Omkeerbare pseudoniemen kunnen worden ontsleuteld door geautoriseerde gebruikers.

30. **Is het mogelijk om van gegevens die we eerder hebben verzameld een pseudoniem te maken en wat is daarvoor nodig? Of moet die actie via de ziekenhuizen lopen?**
    Het is mogelijk om van eerder verzamelde gegevens pseudoniemen te maken mits de daarvoor benodigde input beschikbaar is of gemaakt kan worden. Als bijvoorbeeld pseudoniemen op basis van Naam, geboortedatum, geslacht en voorletter worden gemaakt dan dienen deze gegevens bij de oorspronkelijke bron of bij de kwaliteitsregistratie beschikbaar gemaakt te worden.

4. DPIA

31. **Moet de patiëntnaam opgenomen worden in de DPIA indien alleen de pseudoniemen worden ontvangen en de naam niet in de registratie voorkomt?**
    Beschrijf in de dpia welke gegevens als **input** voor het proces worden genomen en wat er na pseudonimisering als **output** overblijft bij de kwaliteitsregistratie. Bijvoorbeeld; geboortenaam, geboortedatum, geslacht en voorletter als input. In de output een pseudoniem op basis van deze gegevens en eventueel de geaggregeerde, gecodeerde of zelfs ongewijzigde input. Ga daarbij uit van noodzakelijkheid, proportionaliteit en subsidiariteit.

32. **Essentiële punten die voorheen onderdeel van het reguliere proces van gegevensverwerking waren moeten nu "afgedekt" worden in de DPIA. Hoe wordt de zorgvuldigheid in het totale proces gewaarborgd en is voorzien in procedures wanneer registratiehouders door onduidelijkheden informatie missen?**
    Er is een extra eis dat de registratiehouder moet beschikken over een gekwalificeerde functionaris voor de gegevensbescherming (FG). Die eis is er niet voor niets. De FG heeft een duidelijke wettelijk rol onder de AVG. Met betrekking tot de DPIA is die rol:

- Advies geven
  - Of een DPIA nodig is (ja, want in dezen wettelijk bepaald)
  - Hoe de DPIA moet worden uitgevoerd
  - Welke maatregelen nodig zijn om risico's te beperken
- Toezicht houden
  - Controleren of de DPIA goed en volledig is uitgevoerd
  - Nagaan of de aanbevelingen daadwerkelijk worden opgevolgd
- Onafhankelijk
  - Advies geven zonder beïnvloeding
  - Organisatie moet het advies serieus wegen

De FG voert de DPIA niet zelf uit, dat blijft de taak van de verwerkingsverantwoordelijke. Door de wettelijke rol en de kwaliteitseisen die aan de FG zijn gesteld, mogen wij ervan uitgaan dat de zorgvuldigheid van het proces is gewaarborgd.

33. Hoe zorgen we dat alle registratiehouders de kans krijgen om alle onderdelen van de DPIA goed te verwerken in de beoogde tijdsplanning? Inclusief afstemming met bijvoorbeeld de eigen FG en/of privacycommissie?

De verantwoordelijkheid voor het pseudonimiseren is in de Wkkgz toegewezen aan de zorgaanbieder ofwel de verstrekker van de gegevens.

Wat moet de registratiehouder dan in zijn DPIA beschrijven?

De registratiehouder moet in zijn DPIA aangeven welke persoonsgegevens nodig zijn voor een goede werking van de kwaliteitsregistratie.

Voorbeelden:

- Voor *[doel]* het kunnen volgen van een patiënt in de tijd over een keten van zorgverleners of voor het kunnen *[doel]* koppelen van gegevens van een patiënt die afkomstig zijn uit verschillende bronbestanden, heb ik *[beveiligingsmaatregel]* pseudoniemen van combinaties van de volgende gegevens nodig:
  - Geboortenaam of eerste vier letter geboortenaam
  - Geboortedatum
  - Initialen
  - Postcode
  - Lokaal patiëntennummer

  De zorgaanbieder zal die gegevens in diverse combinaties (onomkeerbaar) laten pseudonimiseren door de pseudonimiseringsdienst.

- Voor het *[doel]* uitvoeren van validaties en kwaliteitscontroles zijn gegevens nodig die de zorgaanbieder in staat stellen een patiënt te identificeren, maar die voor de registratiehouder niet te herleiden zijn tot een identificeerbare persoon. Het gaat hierbij om:
  - Patiëntnummer
  - AGB-code van de zorgaanbieder

De zorgaanbieder levert het patiëntnummer – dat uniek is binnen de eigen registratie (AGB-code) – [*informatiebeveiligingsmaatregel*] gepseudonimiseerd aan bij de registratiehouder.

Voor de registratiehouder is dit patiëntnummer, zonder aanvullende gegevens uit het epd, direct een onomkeerbaar pseudoniem. Voor de zorgaanbieder blijft het omkeerbaar, omdat via het eigen epd de koppeling met de identiteit van de patiënt behouden blijft.

Als aanvullende beveiligingsmaatregel kan de zorgaanbieder ervoor kiezen om het patiëntnummer, in combinatie met de AGB-code, door een pseudonimiseringsdienst te laten verwerken. In dat geval is het pseudoniem voor de zorgaanbieder óók omkeerbaar uitsluitend via die dienst.

- Om [*doel*] leeftijd van een patiënt te kunnen berekenen heb ik:
  - het geboortejaar nodig
    - De zorgaanbieder dient dan het geboortejaar als extra variabele aan te leveren
  - Idem: [*doel*] om leeftijd van baby's te kunnen berekenen heb ik de geboortedatum onversleuteld nodig
    - In een dergelijke situatie verwacht je in de DPIA dan ook een omschrijving van maatregelen om het zo ontstane risico op identificatie te verkleinen

- De registratiehouder dient eventueel ook te beschrijven welke extra risico's er ontstaan door het koppelen van gegevens uit meerdere bronnen:
  - Een vergroot risico op indirecte herleidbaarheid als gevolg van de grote hoeveelheid gegevens die bij elkaar gebracht worden.
  - De (extra) maatregelen die getroffen zijn om die risico's te mitigeren
    - Bijv.: Een organisatorische maatregel die het gebruikers van data verbiedt om die gegevens te gebruiken om de persoon te identificeren.

Wat hoeft de registratiehouder dus NIET in zijn DPIA te beschrijven?
Het beschrijven van de conversies van historische data (waarmee bedoeld wordt het pseudonimiseren van de historische data) is de verantwoordelijkheid van de zorgaanbieder. Hoe dit proces werkt/gaat werken is bekend en zal ook met de zorgaanbieders gedeeld worden, zodat zij dit kunnen beschrijven in hun DPIA. De registratiehouder hoeft dit in zijn DPIA niet te benoemen. Immers, er is bepaald dat de registratiehouder uitsluitend gepseudonimiseerde gegeven mag verwerken en dat geldt ook voor de historische gegevens.

34. In de DPIA moeten zeer uitgebreid de technische en organisatorische maatregelen voor informatiebeveiliging worden uitgewerkt, terwijl dit precies is wat er met een NEN7510 of ISO27001 wordt aangetoond. Wat is het verschil?
De DPIA moet aantonen hoe concreet de informatiebeveiliginsrisico's (zijnde privacyrisico's!) bij de verwerking *waarop die DPIA betrekking heeft*, zijn onderkend en afgedekt.

- De NEN7510 en ISO 27001 beschrijven de opzet en het onderhouden van een Information Security Management System (ISMS). Het geeft dus een raamwerk voor *het proces van informatiebeveiliging* op organisatieniveau, maar gaat niet concreet in op de risico's en maatregelen van één specifieke verwerking.
- De DPIA vraagt om verwerkingspecifieke dreigingen, kwetsbaarheden en mogelijke impact voor de betrokkenen (patiënten) in kaart te brengen en welke beveiligingsmaatregelen hier specifiek zijn genomen.

- Een toezichthouder verwacht dat in een DPIA duidelijk en toetsbaar staat beschreven welke risico's voor de betrokkenen bestaan en welke specifieke maatregelen (waaronder informatiebeveiligingsmaatregelen) genomen zijn. Alleen zeggen "wij voldoen aan NEN7510" geeft onvoldoende inzicht in of die maatregelen ook daadwerkelijk passend zijn voor deze specifieke verwerking.

35. Wat is de reden dat er een nieuwe DPIA/nieuw format DPIA aangeleverd moet worden?

Er is een expertgroep gevormd van acht personen met expertise op het gebied van privacy om samen invulling te geven aan een onafhankelijk toets van de DPIA. Deze expertgroep bestaat o.a. uit de FG's van het merendeel van de UMC's en onafhankelijk werkende FG's met ervaring in de zorg.

De DPIA moet aansluiten op de verwerking van de gegevens van een kwaliteitsregistratie. Het NOREA-model sloot onvoldoende aan bij die gegevensverwerking. De expertgroep is daarom afgestapt van dat model en overgestapt op het model dat de Rijksdienst gebruikt. Vervolgens is het model zoveel mogelijk voorzien van voorbeelden en adviezen om registratiehouders te ondersteunen bij het opstellen van de DPIA.

Dit model is overigens bedoeld als een tegemoetkoming en ondersteuning voor de registratiehouder. Indien een registratiehouder zijn eigen model wenst te hanteren dan is dat toegestaan, mits alle informatie aangeleverd wordt waarop de DPIA beoordeeld wordt. Voor de beoordeling is het toetsingskader leidend. Zowel het format voor de DPIA-rapportage als het toetsingskader voor format DPIA-rapportage zijn te vinden op www.ssc-dg.nl/documenten.

36. Heeft de DPIA betrekking op de huidige situatie of de situatie ná inwerkingtreding van de wet?

De DPIA moet betrekking hebben op de verwerking die onder de verantwoordelijkheid van de registratiehouder gaat plaats vinden. Ons inziens is alle kennis voorhanden om de DPIA van de registratiehouder goed te kunnen invullen.

37. Als een ziekenhuis per 1 januari geen gegevens kan aanleveren die aan de bron via een TTP gepseudonimiseerd zijn, betekent dit dat dataverwerkers van de registratie voor die ziekenhuizen geen data mogen verwerken?

Een ziekenhuis is verplicht om vóór verstrekking de gegevens te (laten) pseudonimiseren.

- In het onwaarschijnlijke geval dat een ziekenhuis ongepseudonimiseerde gegevens verstrekt aan een registratiehouder (of diens verwerker), dan is de registratiehouder (dus niet de verwerker!) verplicht dit als vermeend datalek te melden aan de zorgaanbieder. De verdere afhandeling berust daarna bij de zorgaanbieder.
- Indien een zorgaanbieder gepseudonimiseerde data verstrekt, maar niet via de aangewezen route, kan het probleem zijn dat die data niet gekoppeld kunnen worden met data die door een andere TTP of door de zorgaanbieder zelf gepseudonimiseerd zijn. Dit maakt die data minder bruikbaar. Wellicht dat dat in strijd is met de verplichte aanlevering van de data conform de data dictionary van de registratiehouder, maar daar staat vooralsnog geen sanctie op.

5. Financiering

38. **Worden de kosten per aan te maken pseudoniem berekend of per aanlevering? En wie gaat dit bekostigen?**
    Het nu voorliggend plan is dat alle pseudonimiseringen die binnen de Wkkgz vallen centraal gefinancierd worden. Dat betekent dat als dit plan goedgekeurd wordt, er voor zowel de zorgaanbieder als ook voor de registratiehouder geen kosten zijn, ongeacht het aantal pseudoniemen of het aantal pseudonimiseringen.

6. Algemeen/overig

39. **Mogen bestaande gepseudonimiseerde BSN gegevens bewaard worden na ingang van de nieuwe Wkkgz?**
    Een registratiehouder mag zelf bepalen of hij de oude gepseudonimiseerde BSN-gegevens bewaart of niet. Het moet dan wel zo zijn dat deze gegevens "worden bevroren" en echt niet meer worden gebruikt. Als een registratiehouder daarvoor kiest (het bewaren van de gegevens), dan leidt dit niet automatisch tot een afwijzing voor opname in het register (of een negatief advies van de DGC). Dat komt omdat Zorginstituut Nederland en de DGC kijken naar de huidige gang van zaken bij een kwaliteitsregistratie. Hierbij moet wel vermeld worden dat de AP nog steeds handhavend zou kunnen optreden en dat dit evt. gevolgen kan hebben voor de registratiehouder. Maar de afweging tussen bewaren van de gegevens of vernietigen van de gegevens is dus een keuze van de registratiehouder.

40. **Eén van de voordelen van centrale pseudonimisering die wordt gegeven is het koppelen over kwaliteitsregistraties heen. Dit is niet zonder meer mogelijk, maar moet via ZorgTTP in de toekomst. Koppelen over (kwaliteits-)registraties heen doen we nu ook al (bijv. CBS, PHARMO) via een TTP. Wat is er anders aan centrale pseudonimisering en waarom heeft dit voordelen?**
    Het verschil is dat de pseudonimiseringsdienst zo is gemaakt dat één betrouwbare partij het sleutelbeheer regelt. Daardoor kunnen in de toekomst ook nieuwe, nu nog niet bedachte koppelingen eenvoudig worden gemaakt, zonder dat het ingewikkeld wordt doordat meerdere partijen het sleutelbeheer doen. De meeste geraadpleegde experts zijn het eens met de keuze om het sleutelbeheer bij slechts één TTP te beleggen.

41. **Komen er centrale deels voor-ingevulde contracten beschikbaar?**
    ZorgTTP werkt met standaard overeenkomsten. Daarbij wordt waar mogelijk gebruikgemaakt van generieke modellen zoals die van de BOZ voor verwerkersovereenkomsten.

42. **Wat zijn de gevolgen als ziekenhuizen fuseren en een andere AGB-code krijgen**?
    Door het omkeerbare karakter van het pseudoniem op basis van patiëntennummer en AGB code is het mogelijk om historische pseudoniemen te ontsleutelen, de oude AGB-code te vervangen en opnieuw te versleutelen.

43. **Hoe is in de tijdlijn rekening gehouden met het werk aan de kant van de dataverwerkers?**
    Met dataverwerkers is rekening gehouden door ze te consulteren bij het opstellen van het programma van eisen, het uitvoeren van pilots en inventariserende gesprekken. Op basis van die ervaringen worden de ter voorbereiding te nemen stappen door dataverwerkers toegevoegd aan de tijdlijn.

44. Hoe en wanneer worden aanleverende partijen (zorgaanbieders) geïnformeerd over deze beoogde aanpak?
Op 29 september 2025 vindt een digitale informatiebijeenkomst plaatst voor de ziekenhuizen en op 15 oktober 2025 voor de klinieken.

45. In hoeverre zijn zorgaanbieders klaar voor het gepseudonimiseerd aanleveren van de gegevens?
Hier is geen algemeen antwoord op te geven. De ene zorgaanbieder zal wel klaar zijn en een andere zorgaanbieder nog niet. Bovendien hangt dit ook nog samen met de definitieve inrichting en financiering van de pseudonimiseringsdienst. Hierover verwachten wij op korte termijn besluitvorming.

46. Hoe voorkomen we dat ZorgTTP een 'single point of failure' kan worden? Daar zitten meerdere aspecten aan: Hoe is daar de capaciteit en expertise geborgd? Wat als zij bijvoorbeeld overgenomen worden door een commerciële partij of failliet gaan?
Een Single point of failure wordt in opzet voorkomen door:

1. Het werken conform een openbare methode waarin overdraagbaarheid van sleutelmateriaal is geborgd.
2. Functiescheiding tussen het maken van pseudoniemen en het werken met gepseudonimiseerde data; dit voorkomt dat er informatie bij één organisatie ligt waarmee de pseudonimisering doorbroken kan worden. De pseudonimisatiedienst beheert enkel encryptiesleutels en rechten om van die sleutels gebruik te maken. De dienst slaat geen inhoudelijke data op.
3. Het afsluiten van service levels passend bij de gevraagde beschikbaarheid, inclusief certificeringen en daarbij behorende periodieke audits.

ZorgTTP biedt naast de gebruikelijke maatregelen uit oogpunt van business continuity aanvullende maatregelen in geval van “vendor failure”:

1. ZorgTTP heeft een overeenkomst met de NCC group voor het in escrow onderbrengen van software. Opdrachtgevers kunnen desgewenst van deze regeling gebruikmaken. Hiervoor wordt een aanvullende overeenkomst gesloten;
2. ZorgTTP betaalt de in Nederland gevestigde hosting provider RAM-IT van de productiesystemen 3 maanden vooruit. Een aanvullende bepaling in de overeenkomst regelt dat deze maanden ingaan op het moment dat Stichting ZorgTTP niet langer aan haar verplichtingen voldoet. De hosting provider houdt in dat geval de productiesystemen nog 3 maanden in stand. Opdrachtgevers kunnen in deze periode maatregelen treffen om met de ontstane situatie om te gaan. Bijvoorbeeld door met de in escrow gegeven materialen elders een nieuwe omgeving op te bouwen.
3. De keuze voor de stichtingsvorm met een not-for-profit karakter voorkomt dat de organisatie kan worden overgenomen door partijen met andere belangen. Zo wordt voorkomen dat perverse prikkels ontstaan die de duurzame bijdrage aan een veilige informatiesamenleving – waar Stichting ZorgTTP naar streeft – in gevaar kunnen brengen. Onder perverse prikkels wordt o.a. verstaan:
    a. Winstmaximalisatie boven maatschappelijk belang
    b. Commerciële exploitatie van data
    c. Buitenlandse overnames waardoor toegang tot of opslag van encryptiesleutels buiten de werkingssfeer van EU wetgeving kan komen te liggen.