

Nader gebruik en koppelen van gegevens voor gezondheidsonderzoek zonder toestemming

Aanbevelingen voor zorgaanbieders,
zorgverzekeraars en onderzoeksinstellingen



UMC Utrecht

Colofon

2022 © UMC Utrecht

Deze aanbevelingen zijn tot stand gekomen als onderdeel van het DaLi project. De wijze waarop de aanbevelingen tot stand zijn gekomen is beschreven op pagina 6 van dit document. De aanbevelingen gaan uit van de op 20 september 2022 geldende wet- en regelgeving. Het DaLi consortium bedankt de leden van de Denktank en de deelnemers aan de interviews en de focusgroepen voor hun belangrijke bijdrage.



Het DaLi project is mede mogelijk gemaakt door de bijdrage van Health~Holland, Top Sector Life Sciences & Health.

Inhoudsopgave

INTRODUCTIE	4
I. Preambule	5
II. Doelgroep en reikwijdte	5
III. Methode totstandkoming aanbevelingen	5
IV. Juridisch kader	6
 AANBEVELINGEN VOOR DE PRAKTIJK	 7
1. Algemene aanbevelingen	9
2. Wettelijke grondslag	9
3. Aanvraag- en beoordelingsprocedures	11
4. Passende waarborgen	12
 ONDERLIGGEND ONDERZOEK EN RESULTATEN	 15
Onderliggend onderzoek	16
Resultaten	16
I. Het systematische literatuuronderzoek	16
II. Het kwalitatieve onderzoek	17
III. De Technische verkenning	19
 Bijlage	 24



INTRODUCTIE

I. Preambule

Gegevens die routinematig in de zorg worden geregistreerd worden momenteel niet altijd optimaal benut voor medisch-wetenschappelijke doeleinden. Dit terwijl het koppelen van databases met gezondheidsgegevens veel kansen biedt voor gezondheidsonderzoek. Hierbij kan in het bijzonder gedacht worden aan gegevens die bij zorgaanbieders en zorgverzekeraars geregistreerd worden, bijvoorbeeld in elektrische patiëntendossiers of systemen met declaratiegegevens. Met de gedetailleerde informatie die beschikbaar wordt door het koppelen van gegevens kan niet alleen meer inzicht verkregen worden in zowel intramurele als extramurele patiënten en hun klinische resultaten, ook kan deze informatie ingezet worden voor learning healthcare systemen, value based healthcare als ook voor het doen van voorspellend onderzoek naar onder andere hart- en vaatziekten.

II. Doelgroep en reikwijdte

De aanbevelingen in dit document richten zich tot zorgaanbieders, zorgverzekeraars en onderzoeksinstituten -en de aldaar werkzame personen-, die betrokken zijn bij het nader gebruiken en koppelen van routine zorggegevens voor gezondheidsonderzoek. De aanbevelingen richten zich op scenario's waarin een onderzoeker of onderzoeksinstituut gegevens van verschillende zorgaanbieders en/of zorgverzekeraars wil koppelen voor gezondheidsonderzoek, waarbij toestemming vragen voor dit nadere gebruik geen reële mogelijkheid is. Het ontbreken van toestemming van de persoon van wie de gegevens afkomstig zijn brengt met zich mee dat een andere juridische grondslag voor het nader gebruik en de koppeling gevonden moet worden en de inachtneming van passende waarborgen aan belang wint.

De aanbevelingen in dit document moeten gelezen worden als uitwerking van of aanvulling op bestaande wet- en regelgeving, voor zover de bevindingen in het DaLi onderzoek daartoe aanleiding hebben gegeven. De aanbevelingen hebben echter geen volledig karakter, met dit document wordt niet gepoogd te voorzien in een systematische uitwerking van alle relevante (wettelijke) normen.

III. Methode totstandkoming aanbevelingen

Bij het tot stand komen van dit aanbevelingendocument is gebruik gemaakt van de reflectieve evenwichtsmethode. Dit is een in de normatieve wetenschappen beproefde aanpak, waarin men heen en weer gaat tussen inzichten uit de theorie, de praktijk en normatieve uitgangspunten waarop gereflecteerd wordt tot een coherent beeld ontstaat.

Figuur 1. De methode van het reflectieve evenwicht

Op theoretisch en normatief vlak is er voor deze studie informatie verzameld door middel van het uitvoeren van een technische verkenning, een juridische verkenning en een systematisch literatuur- en richtlijnenonderzoek (Stap 1). Om praktijkervaringen en meningen van belanghebbenden in kaart te brengen is een kwalitatieve studie uitgevoerd. Het doel van deze kwalitatieve studie was tweeledig; enerzijds het identificeren van de belangrijkste juridische en ethische belemmeringen die men in de praktijk ervaart bij het koppelen van gegevens voor gezondheidsonderzoek, anderzijds het verkennen van mogelijke oplossingsrichtingen voor deze ervaren belemmeringen. Hierover is informatie verzameld door middel van focusgroepen en diepte-interviews met verschillende belanghebbenden onder wie zorgaanbieders, wetenschappers, juristen, data verzamelaars/ beheerders en beleidsmakers (Stap 2). Vervolgens is door middel van een deliberatief proces gereflecteerd op de inzichten die in de theorie en praktijk zijn opgedaan. Deze reflectie heeft niet alleen binnen het onderzoeksteam plaatsgevonden, de leden van het consortium en de Denktank van het DaLi project hebben meermaals input gegeven op de bevindingen (Stap 3). Ook bij de vertaling van de bevindingen, waaronder de geïdentificeerde belemmeringen en oplossingsrichtingen, naar concrete aanbevelingen vond reflectie plaats en werd input verkregen vanuit het onderzoeksteam, het consortium en de Denktank (Stap 4).

IV. Juridisch kader

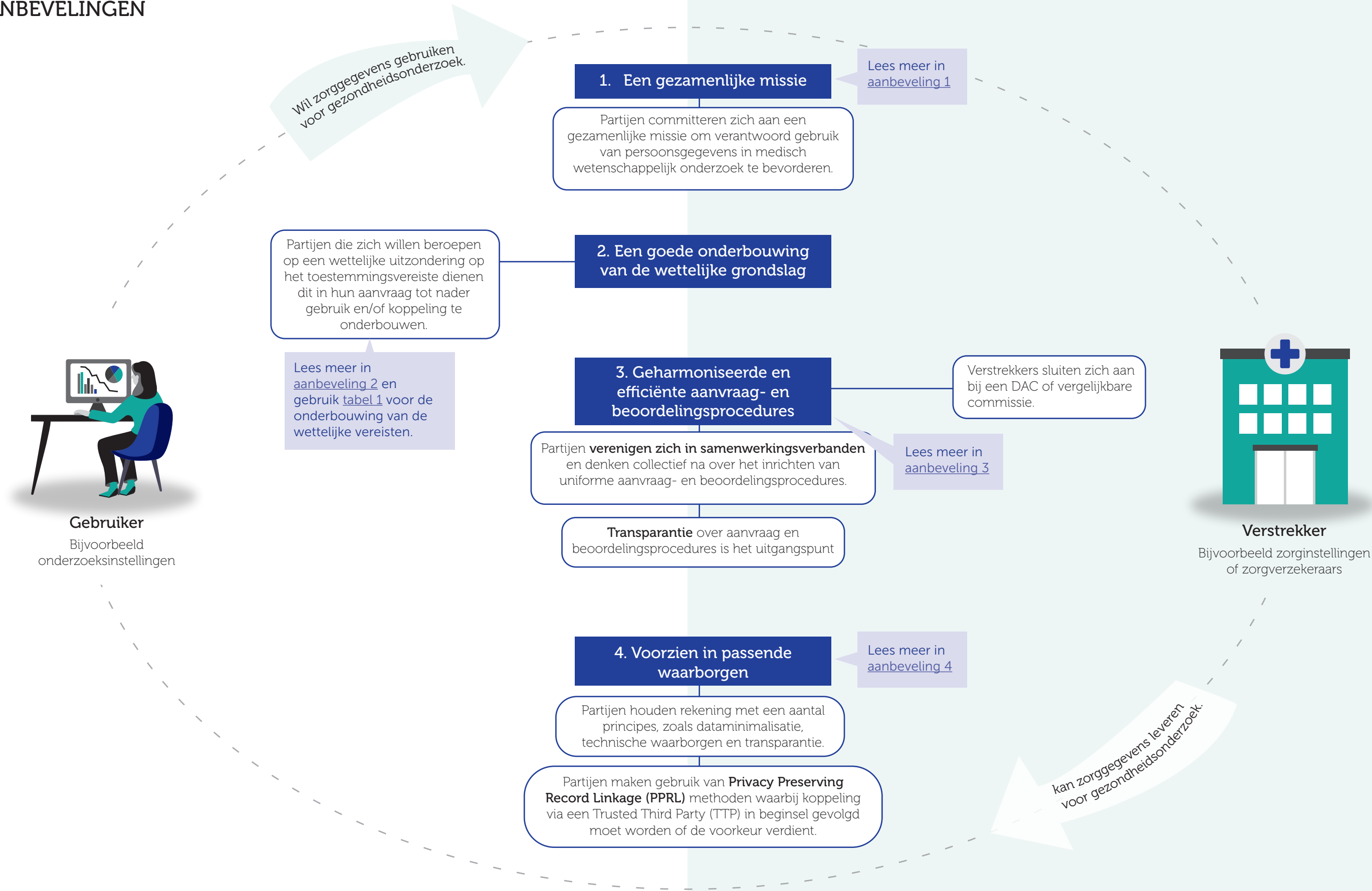
Wet- en regelgeving, richtlijnen en gedragscodes

De aanbevelingen zijn geformuleerd tegen de achtergrond van de belangrijkste in Nederland geldende wet- en regelgeving, richtlijnen en gedragscodes. Daarbij is in het bijzonder acht geslagen op relevante bepalingen uit de Algemene verordening gegevensbescherming (AVG), de Uitvoeringswet algemene verordening gegevensbescherming (UAVG), de Wet op de geneeskundige behandelingsovereenkomst (WGBO) en de Zorgverzekeringswet (Zvw). Ook relevante gedragscodes en richtlijnen werden meegenomen in deze analyse, waaronder de Gedragscode Gezondheidsonderzoek (2022) van de Stichting COREON en de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars (2021) van Zorgverzekeraars Nederland.



AANBEVELINGEN
VOOR DE PRAKTIJK

OVERZICHT
AANBEVELINGEN



1. Algemene aanbevelingen

Zorgaanbieders, zorgverzekeraars en onderzoeksinstituten -en de aldaar werkzame personen- committeren zich aan de missie om verantwoord gebruik van persoonsgegevens in medisch-wetenschappelijk onderzoek te bevorderen.

- 1.1. Zorgaanbieders, zorgverzekeraars en onderzoeksinstituten -en de aldaar werkzame personen- werken toe naar een geharmoniseerde en rechtvaardige interpretatie en toepassing van relevante wet- en regelgeving. Wat betreft de uitleg van de Algemene verordening gegevensbescherming (AVG), Uitvoeringswet algemene verordening gegevensbescherming (UAVG) en de Wet op de geneeskundige behandelingsovereenkomst (WGBO) kan de uitleg in de Gedragscode Gezondheidsonderzoek (2022) aanknopingspunten bieden.¹ Specifiek voor zorgverzekeraars bevat de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars (2021) relevante richtlijnen.
- 1.2. Het slechts voldoen aan wettelijke vereisten kan vanuit ethisch en maatschappelijk perspectief onvoldoende zijn om te komen tot een verantwoord gebruik van persoonsgegevens. Het verdient aanbeveling dat zorgaanbieders, zorgverzekeraars en onderzoeksinstituten maatregelen nemen die in lijn zijn met internationaal aanvaarde ethische principes en uitgangspunten voor gezondheidsonderzoek waarin wettelijke vereisten niet alleen uitgelegd maar soms ook uitgebreid worden. In het bijzonder kan gedacht worden aan de principes zoals geformuleerd in Guideline 12 van de CIOMS International Ethical Guidelines for Health-related Research Involving Humans (2016), de WMA Declaration of Taipei (2016) en het GA4GH Framework for Responsible Sharing of Genomic and Health-Related Data (2019).

2. Wettelijke grondslag

Aangezien iedere verwerking van persoonsgegevens gebaseerd dient te zijn op een wettelijke grondslag, moet er een basis in de wet gevonden worden voor nader gebruik en koppeling van gegevens voor wetenschappelijk onderzoek.

- 2.1. De wettelijke uitgangshouding is dat verwerking van bijzondere persoonsgegevens op basis van toestemming plaats dient te vinden;
- 2.2. Partijen die een aanvraag tot nader gebruik en/of koppeling van gegevens doen bij een verstrekker en zich willen beroepen op een uitzondering op het toestemmingsvereiste dienen in hun aanvraag voldoende aanknopingspunten te bieden voor de onderbouwing van de wettelijke uitzonderingsgrond². Hierbij moet voldaan worden aan de volgende voorwaarden:
 - 1 De verwerking van de gegevens is noodzakelijk voor het wetenschappelijk onderzoek;
 - 2 Het onderzoek dient een algemeen belang;
 - 3 Er is voorzien in passende waarborgen;
 - 4 Toestemming vragen is in redelijkheid niet mogelijk of kan niet worden verlangd.
- 2.3. Voor de beoordeling of aan de voorwaarden voor een beroep op een uitzondering op het toestemmingsvereiste is voldaan en is voorzien in passende waarborgen, dient de verstrekker een beoordelingsprocedure te implementeren. Daarbij verdient het de voorkeur dat deze beoordeling plaatsvindt door een Data Access Committee of vergelijkbare instantie (conform de aanbevelingen onder 3.2).

¹ De huidige (2022) versie van de Gedragscode Gezondheidsonderzoek kreeg (nog) geen goedkeuring van de Autoriteit Persoonsgegevens. Het document heeft dus niet de juridische zeggingskracht van een goedgekeurde AVG-gedragscode.

² Ingevolge art. 9 lid 2 sub j AVG en art. 24 alsmede par. 2c van de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars (2021).

Tabel 1. Uitwerking van de wettelijke voorwaarden onder aanbeveling 2.2

1 Toestemming vragen in redelijkheid niet mogelijk

Voorbeelden van omstandigheden waaronder het vragen van toestemming in redelijkheid niet mogelijk is:

- wanneer een groot aantal deelnemers is overleden;
- wanneer communicatiegegevens onbekend of incorrect zijn en het niet mogelijk is ze te actualiseren;
- wanneer de gegevens worden verzameld in een noodsituatie.

Toestemming vragen kan in redelijkheid niet worden verlangd

Voorbeelden van omstandigheden waaronder het vragen van toestemming in redelijkheid niet kan worden verlangd zijn:

- wanneer de omvang van de groep deelnemers zo groot is dat het een onevenredige inspanning vergt van de onderzoeker(s) om de deelnemers te benaderen;
- wanneer aannemelijk is dat het benaderen van deelnemers voor hun toestemming een te grote belasting voor hen zou betekenen;
- wanneer het essentieel is dat de uitnodiging voor deelname uitsluitend de potentiële deelnemer bereikt maar er een risico bestaat dat personen in de naaste omgeving de uitnodiging zien.

2 De verwerking van de gegevens noodzakelijk is voor het wetenschappelijk onderzoek

Er dient aangetoond en onderbouwd te worden dat het onderzoek niet zonder desbetreffende gegevens uitgevoerd kan worden.

3 Het onderzoek dient een algemeen belang ³

De volgende onderdelen moeten naar voren komen bij een onderbouwing van het algemeen belang:

- Het onderzoek moet als wezenlijk doel het bevorderen en beschermen van de volksgezondheid door het op systematische wijze vergaren en bestuderen van gegevens hebben;
- Het onderzoek mag niet een uitsluitend commercieel of industrieel doel hebben;
- Het moet redelijkerwijs aannemelijk zijn dat de resultaten van het onderzoek nieuwe wetenschappelijke inzichten genereren die geldend zijn voor een populatie groter dan de directe onderzoekspopulatie;
- De onderzoekers moeten zich inspannen om hun resultaten inzichtelijk te maken voor een breder publiek dan alleen de kring van betrokken onderzoekers en betrokken patiënten;
- Over het onderzoek en de resultaten moet in de regel worden gepubliceerd, ook als de resultaten negatief zijn; en
- Er dient te worden voldaan aan de uitgangspunten van FAIR-data gebruik (Findable, Accessible, Interoperable, Reusable) ⁴.

Zorgverzekeraars hebben zich aangesloten bij de normen uit de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars (2021). Volgens 2c. van deze Gedragscode is het voor zorgverzekeraars mogelijk om gezondheidsgegevens te verstrekken voor statistiek of wetenschappelijk onderzoek dat een algemeen belang dient. Het verdient aanbeveling dat zorgverzekeraars wat betreft de interpretatie en onderbouwing van wat gezondheidsonderzoek in het algemeen belang is aansluiten bij bovenstaande toelichting.

4 Er is voorzien in passende waarborgen

Zie voor passende waarborgen onder 4. van deze aanbevelingen.

³ Deze eisen zijn gebaseerd op: Memorie van Toelichting van de WzI, Tweede Kamer, vergaderjaar 2020–2021, 35 844, nr. 3, p 35–36. Zie ook: Ministerie van VWS, 'Kamerbrief met reactie op artikel over secundair gebruik data, 1587082-195476-DICIO', www.rijksoverheid.nl, doi:10/04/kamerbrief-over-reactie-artikel-fd-over-secundair-gebruik-data, 4 oktober 2019.

⁴ Zie uitgebreider: <https://www.go-fair.org/fair-principles/>

3. Aanvraag- en beoordelingsprocedures

Zorgaanbieders, onderzoeksinstituten en zorgverzekeraars dragen zorg voor geharmoniseerde aanvraag- en beoordelingsprocedures voor nader gebruik en koppeling van gegevens ten behoeve van gezondheidsonderzoek. Het instellen van dergelijke procedures en beleid door partijen kan bijdragen aan het op een verantwoorde en efficiënte manier toegankelijk maken van gegevens voor gezondheidsonderzoek.

- 3.1. Om fragmentatie van procedures en beleid te voorkomen, dienen zorgaanbieders, zorgverzekeraars en/of onderzoeksinstituten zich te verenigen in samenwerkingsverbanden. Vanuit deze samenwerkingsverbanden wordt collectief nagedacht over het inrichten van uniforme aanvraag- en beoordelingsprocedures.
 - 3.1.1. Bij samenwerkingsverbanden die relevant zijn voor groepen van zorgaanbieders en/of onderzoeksinstituten kan bijvoorbeeld gedacht worden aan Stichting Health-RI, de Nederlandse Federatie van Universitair Medische Centra (NFU) en het Nederlands Huisartsen Genootschap (NHG).
 - 3.1.2. Voor zorgverzekeraars kan voornoemde samenwerking bijvoorbeeld een plek krijgen onder de vlag van de vereniging Zorgverzekeraars Nederland (ZN). Voorts kan Vektis in dit samenwerkingsverband een spilfunctie vervullen, gezien de centrale rol van Vektis in het samenbrengen van alle gedeclareerde zorgdata en verwerken van deze gegevens ten behoeve van zorginzichten, uitvoerings- en beleidsprocessen.
- 3.2. Partijen die verzoeken ontvangen om hun gegevens ter beschikking te stellen voor nader gebruik en/of koppeling ten behoeve van gezondheidsonderzoek sluiten zich aan bij een Data Access Committee(DAC) of vergelijkbare commissie. Dit heeft tot doel harmonisatie van toegangsprocedures en efficiëntie van toetsing te bevorderen. Vanuit ethisch perspectief is toetsing door een DAC een belangrijke institutionele waarborg, die bij kan dragen aan een onafhankelijke en evenwichtige toepassing van procedures en regels. Daarnaast kan toetsing door een DAC bijdragen aan een breder draagvlak voor het nader gebruik van gezondheidsgegevens ten behoeve van wetenschappelijk onderzoek onder zowel direct betrokkenen (patiënten, verzekerden) als indirect betrokkenen (het grotere publiek).
 - 3.2.1. Idealiter sluiten groepen van zorgaanbieders, onderzoeksinstituten en/of zorgverzekeraars zich aan bij een DAC of vergelijkbare commissie vanuit de onder 2.1 genoemde samenwerkingsverbanden.
- 3.3. Het doel, de bevoegdheden, verantwoordelijkheden, werkwijze en structuur van de DAC en diens leden worden in een door de betrokken partijen formeel erkend document neergelegd.
 - 3.3.1. Voor de invulling van een dergelijk formeel erkend document kan aangesloten worden bij de principes en algemene procedurele normen uit de Data Access Committee Review Standards Policy (2021) van de Global Alliance for Genomics and Health (GA4GH). Hierbij is in het bijzonder van belang dat de volgende onderwerpen aan de orde komen:
 - wat de samenstelling is van de DAC. Hierbij is van belang dat de benodigde expertise, achtergrond en competenties van de leden van de DAC geëxpliciteerd worden. Betrek als leden van de DAC in het bijzonder experts op wetenschappelijk, ethisch, juridisch/compliance vlak en een vertegenwoordiger van patiënten of verzekerden;
 - de mate van onafhankelijkheid van de DAC bij de beoordeling van verzoeken tot gegevenstoegang;
 - op welke gronden de betrokken partijen (eventueel) af kunnen wijken van een beslissing of advies van de DAC op verzoeken tot gegevenstoegang.

- 3.4. Transparantie over aanvraag- en beoordelingsprocedures, waaronder de werkwijze, rollen en verantwoordelijkheden van een DAC, is het uitgangspunt. Transparantie over de uitkomst van de beoordeling van verzoeken en uitgaves van gegevens wordt tevens aanbevolen.
- 3.4.1. De betrokken partijen moeten richting hun patiënten, verzekerden en/of andere belanghebbenden een duidelijke en openbaar toegankelijke verklaring publiceren over de wijze waarop zij een verantwoorde toegang tot gegevens voor gezondheidsonderzoek geborgd hebben.
 - 3.4.2. Informatie over het aanvraagproces en de criteria op basis waarvan verzoeken tot nader gebruik en koppeling van gegevens beoordeeld worden moeten openbaar zijn. Toegang tot deze informatie dient gemakkelijk verkrijgbaar te zijn, bijvoorbeeld via een openbare website.
 - 3.4.3. Samenvattingen van goedgekeurde verzoeken tot toegang inclusief de beoordeling van deze verzoeken worden in begrijpelijke bewoordingen openbaar gemaakt. Bij voorkeur via de websites van de bij de DAC aangesloten zorgaanbieders, zorgverzekeraars en/of onderzoeksinstituten.
 - 3.4.4. Ook afgekeurde verzoeken, inclusief gemotiveerde afwijzing, worden -al dan niet op verzoek- toegankelijk gemaakt voor betrokkenen en andere belangstellenden met als doel om lering te trekken uit de afwijzingen.

4. Passende waarborgen

Zorgaanbieders, zorgverzekeraars en onderzoeksinstituten voorzien in passende waarborgen voor nader gebruik en koppelen van gegevens. Als voorzien is in passende waarborgen kan een beroep gedaan worden op bepalingen uit de AVG, UAVG en WGBO die meer ruimte laten voor gezondheidsonderzoek zonder toestemming.

- 4.1. Bij het inrichten van passende waarborgen voor nader gebruik en koppelen van gegevens houden zorgaanbieders, zorgverzekeraars en onderzoeksinstituten in ieder geval rekening met de volgende uitgangspunten/principes:
- 4.1.1. **Dataminimalisatie:** verwerk alleen gegevens die nodig zijn voor het beantwoorden van de onderzoeksvraag of het bereiken van de onderzoeksdoelstellingen;
 - 4.1.2. **Technische waarborgen:** identificeer en implementeer passende technische waarborgen (zie onder 4.2.);
 - 4.1.3. **Herleidbaarheid:** het is verboden om gecodeerde gegevens tot direct identificeerbare gegevens te herleiden, tenzij daar uitdrukkelijke toestemming voor is gegeven door de persoon van wie de gegevens afkomstig zijn;
 - 4.1.4. **Noodzakelijkheid:** verwerk direct identificerende persoonsgegevens alleen wanneer dit noodzakelijk is voor het onderzoek. Indien van toepassing; bewaar communicatiegegevens gescheiden van onderzoeksgegevens;
 - 4.1.5. **Toegankelijkheid:** zorg dat alleen personen die noodzakelijkerwijs betrokken zijn bij het onderzoek toegang hebben tot de gegevens. Verwerk de gegevens in een omgeving die door de organisatie als veilig is beoordeeld;
 - 4.1.6. **Verwerk conform normen:** sluit zo veel mogelijk aan bij NEN-normen en andere

relevante normen omtrent gegevensbescherming in de zorg.

- 4.1.7. **Transparantie:** wees zo transparant mogelijk over (o.a.); de verstrekking van de gegevens, toegang tot gegevens, de wijze van opslag van gegevens en getroffen andere beveiligingsmaatregelen. Publiceer e.e.a. bij voorkeur op een openbare website.
 - 4.1.8. **Informatievoorziening:** informeer de onderzoekspopulatie als mede het bredere publiek zo veel mogelijk over het soort wetenschappelijk onderzoek waarvoor de gegevens gebruikt zijn en over de uitkomsten ervan.
 - 4.1.9. **Betrokkenheid en participatie:** betrek de onderzoekspopulatie als mede het bredere publiek bij beslissingen over de verwerking en verschaft ze waar mogelijk inspraak over de manier waarop de gegevens verwerkt worden.
- 4.2. Zorgaanbieders, zorgverzekeraars en onderzoeksinstituten maken gebruik van *Privacy Preserving Record Linkage (PPRL) methodes* om gegevens uit verschillende bestanden te koppelen op individueel niveau. Hierbij kunnen de vijf hoofdstappen uit **Figuur 2.** doorlopen worden.
- 4.2.1. De vorm die de voorkeur verdient of in beginsel gevolgd moet worden voor het tot stand brengen van een koppeling is de Trusted Third Party (TTP) (zie figuur 3).
 - 4.2.1.1. Bij koppeling van gegevens op individueel persoons niveau van meerdere verstrekkers *bij een van deze verstrekkers* verdient codering via een TTP de voorkeur.⁵
 - 4.2.1.2. Als meerdere verstrekkers gegevens verstrekken die op individueel persoons niveau gekoppeld moeten worden *bij de onderzoeksinstituten*, dan moet voor de koppeling in beginsel een TTP ingeschakeld moeten worden. Gemotiveerd afwijken van dit uitgangspunt kan indien op een andere manier een vergelijkbaar niveau van bescherming en reproduceerbaarheid wordt bereikt.⁶

Figuur 2. Vijf hoofdstappen in het PPRL proces ⁷



⁵ Zie ook: 2.6.5. Gedragscode Gezondheidsonderzoek

⁶ Zie ook: 2.2.4 Gedragscode Gezondheidsonderzoek

⁷ Zie voor een uitgebreidere uitleg van het stappenplan onder Deel C: De technische verkenning.

Figuur 3. Mogelijke koppelvormen

DIRECTE KOPPELING

Zonder een beveiligde omgeving



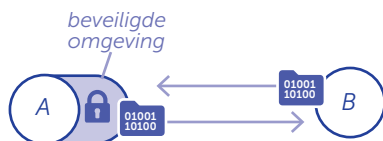
Voordelen:

- Makkelijk te bewerkstelligen.
- Gaat uit van gelijkwaardigheid tussen partijen.
- Beide partijen hebben voordeel van de koppeling.

Nadelen:

- Minst veilig voor PPRL.

Met een beveiligde omgeving



Voordelen:

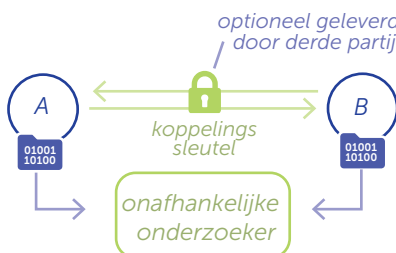
- Volledige controle voor de aanbieder.
- Biedt enige mogelijkheid tot dataverkenning voordat de koppeling tot stand komt.
- Makkelijke en dynamische mogelijkheden voor privacy en afschermen.

Nadelen:

- Individuele subject data koppeling maakt het onmogelijk om ongewenste identificatie van subjecten uit te sluiten.
- Andere partij(en) moeten hun data uploaden naar de beveiligde omgeving om toegang te krijgen tot de koppeling van de aanbieder.

KOPPELING VIA...

... een onafhankelijke onderzoeker

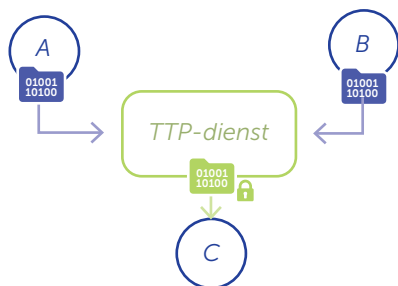


Voordelen:

- Geen partij met een direct te identificeren dataset nadat de koppelings sleutels zijn uitgewisseld.

Nadelen:

- Risico op collusie tussen onderzoekers.
- Onderzoekers zouden subjecten kunnen heridentificeren door gebruik van quasi-identificeerders of frequentie benadering.
- Als de data niet goed voorbereid zijn door de partij die de data in het bezit heeft, kan dit tot problemen leiden bij de vragende partij.

...een vertrouwde derde partij
(Trusted-third party (TTP) linkage)

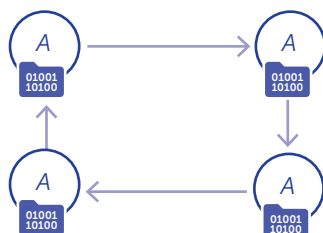
Voordelen:

- Als de koppelings sleutels vooraf uitgewisseld worden, kan geen van de partijen alle identificeerbare data in het bezit krijgen.
- Minder aanvullende PPRL methodes nodig gezien privacybescherming via TTP.

Nadelen:

- Risico op collusie tussen onderzoekers.
- Onderzoekers zouden subjecten kunnen heridentificeren door gebruik van quasi-identificeerders of frequentie benadering.
- Partijen moeten in grote mate vertrouwen op de betrouwbaarheid van de TTP koppeling en de privacy-maatregelen hiervan.

... aggregatie van meerdere partijen

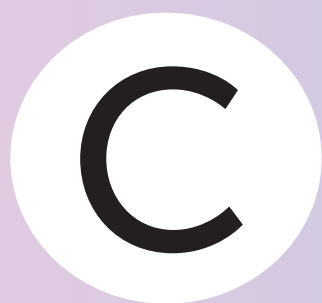


Voordelen:

- Weinig aanvullende PPRL methodes nodig omdat deze methode analyse mogelijk maakt zonder dat persoonsgegevens uitgewisseld worden.

Nadelen:

- Geen individuele subject data koppeling mogelijk.



ONDERLIGGEND
ONDERZOEK EN
RESULTATEN

Onderliggend onderzoek

De bronnen en bevindingen uit het DaLi onderzoek die gebruikt zijn om tot aanbevelingen te komen door middel van de methode van het reflectieve evenwicht zijn divers. Hieronder benoemen wij de belangrijkste bronnen en geven wij een beknopte samenvatting van de bevindingen in het DaLi project welke zijn voortgekomen uit

- I. **Het systematische literatuuronderzoek;**
- II. **Het kwalitatieve onderzoek;**
- III. **De technische verkenning.**

Resultaten

I. Het systematische literatuuronderzoek

Er heeft een systematische analyse plaatsgevonden van academische literatuur en relevante soft-law instrumenten. Het doel van dit onderzoek was om na te gaan naar welke passende en specifieke maatregelen en waarborgen in deze bronnen wordt verwezen voor het verrichten van wetenschappelijk onderzoek zonder toestemming. De review van de soft-law instrumenten en literatuur heeft geleid tot de identificatie van vijf overkoepelende thema's:

1. Toezicht en/of toetsing: Uit het literatuuronderzoek is gebleken dat het een breed gedragen opvatting is dat er een bepaalde vorm van toezicht of toetsing moet zijn wanneer zonder toestemming wetenschappelijk onderzoek met persoonsgegevens wordt verricht. Te denken valt bijvoorbeeld aan toetsing door een Medisch Ethische Toetsingscommissie (METC) of een Data Access Committee (DAC).
2. Organisatorische maatregelen: Bij de afwezigheid van toestemming kan het aanscherpen van organisatorische maatregelen en het versterken van het governance framework dienen als -aanvullende- waarborg. Met name thema's als transparantie, openheid en het afleggen van verantwoording worden veelvuldig aangehaald in de literatuur. Voorbeelden van onderwerpen waarover (meer) transparantie gewenst is zijn bijvoorbeeld beleid inzake; verstrekking van gegevens, opslag van gegevens, toegang tot gegevens, beveiligingsmaatregelen en privacybescherming.
3. Technische maatregelen: Het verbeteren van de gegevensbescherming en privacy door het toepassen van (aanvullende) technische maatregelen is gewenst bij het uitvoeren van wetenschappelijk onderzoek met persoonsgegevens zonder toestemming. Onder meer wordt in de literatuur verwezen naar technische maatregelen om veilige opslag van en toegang tot data te garanderen. Daarnaast wordt veelvuldig gerefereerd naar methodes voor de-identificatie en data minimalisatie.
4. Informatievoorziening: De plicht om te informeren gaat verder dan transparant zijn; alleen inzicht verschaffen in uw eigen beleid of dat van uw instelling is niet voldoende, het vereist dat er positieve actie wordt ondernomen en dat informatie actief wordt verspreid aan zowel betrokkenen als het grotere publiek. Voorbeelden van onderwerpen waarover kan worden geïnformeerd zijn o.a. medisch wetenschappelijk onderzoek zonder toestemming, medisch onderzoek dat door ethische comités is goedgekeurd en ook de resultaten van dergelijk door de RECs/DACs goedgekeurd onderzoek.
5. Betrokkenheid en participatie: Uit de geanalyseerde bronnen is naar voren gekomen dat

individueen maar ook het bredere publiek meer bij wetenschappelijk onderzoek betrokken moeten worden wanneer toestemming ontbreekt. Men wil niet slechts geïnformeerd worden over wat er met de gegevens gedaan wordt, men wil daadwerkelijk betrokken worden en inspraak hebben bij de beslissingen hierover. De vergroting van zeggenschap en deelname door het individu, de patiënt en/of het publiek kan bovendien tot gevolg hebben dat het vertrouwen van die groepen in de wetenschap toeneemt.

II. Het kwalitatieve onderzoek

Door middel van focusgroepen en diepte-interviews zijn meningen en inzichten van verschillende belanghebbenden verzameld. Het kwalitatieve onderzoek had het verkennen van oplossingsrichtingen voor de juridische en ethische belemmeringen die zich voordoen bij het koppelen van twee of meerdere (medische) datasets ten behoeve van gezondheidsonderzoek tot doel. Hiervoor zijn eerst de belangrijkste belemmeringen in kaart gebracht, welke in drie thema's zijn gecategoriseerd. De aangedragen oplossingen laten zich in vijf thema's onderverdelen.

Geïdentificeerde belemmeringen bij koppeling en nader gebruik van gegevens:

1. De heersende onduidelijkheid over de interpretatie van het huidige wettelijke kader.

Volgens de deelnemers aan het kwalitatieve onderzoek is momenteel niet duidelijk hoe de wettelijke bepalingen die het verwerken van persoonsgegevens ten behoeve van wetenschappelijk onderzoek regelen geïnterpreteerd moeten worden. Deze onduidelijkheid resulteert in uiteenlopende wetsinterpretaties. Bovendien bestaat er een angst voor het verkeerd interpreteren van de AVG (en andere relevante wettelijke bepalingen) met onder andere boetes maar ook imagoschade als mogelijke gevolgen, wat volgens meerdere deelnemers leidt tot risicomijding.

2. Het gefragmenteerde beleid ten aanzien van het verwerken van persoonsgegevens.

Het wordt als belemmerend ervaren dat instellingen hun systemen en procedures voor het verwerken van persoonsgegevens verschillend hebben ingericht. Er werd gesteld dat zorgaanbieders een groot belang hechten aan autonomie en dus graag hun eigen beleid bepalen. Geïnterviewden wezen op een gebrek aan centrale regie. Er geen sprake van eenheid van taal en techniek, er wordt geen/te weinig gebruik gemaakt van (inter)nationale standaarden. Door deze uiteenlopende systemen en procedures wordt de uitwisseling en samenwerking niet geoptimaliseerd, en de kans op miscommunicatie tussen verschillende instellingen zelfs vergroot. Een genoemde verklaring hiervoor is de marktwerking in de zorg, welke transparantie en uitwisseling zou belemmeren.

3. Het moeten voldoen aan veeleisende wettelijke vereisten.

Door sommigen wordt het huidige wettelijke kader en de vereisten waar men aan moet voldoen bij het verwerken van persoonsgegevens voor wetenschappelijk onderzoek als veeleisend en belemmerend ervaren. Het toestemmingsvereiste werd het meest aangehaald als belemmerend. Daarnaast werd onder meer gesteld dat het lastig kan zijn een rechtmatige wettelijke grondslag te vinden voor het maken van een koppeling of het nader gebruiken van (bijzondere) persoonsgegevens. Ook wordt het als lastig ervaren dat doelbinding aangetoond dient te worden, bijvoorbeeld in situaties waar op het moment van datacollectie de nu relevante onderzoeksvraag nog niet bestond. Ook refereerde men naar wettelijke vereisten als transparantie, dataminimalisatie en het moeten beperken van de herleidbaarheid. Bovendien werd gesteld dat er niet voldoende budget is binnen de zorg om te kunnen voldoen aan de wettelijke eisen, welke hoge kosten met zich meebrengen.

Geïdentificeerde oplossingsrichtingen voor koppeling en nader gebruik van gegevens:

1. Het uitvaardigen van gezaghebbende interpretaties van de wet.

Meerdere deelnemers waren van mening dat het uitvaardigen van gezaghebbende interpretaties van de wet kan bijdragen aan het wegnemen van verschillende belemmeringen die momenteel de koppeling van persoonsgegevens voor onderzoeksdoeleinden in de weg staan. Gedragscodes, praktische richtsnoeren, professionele samenvattingen en wetenschappelijke documenten werden voorgesteld als geschikte middelen om deze gezaghebbende interpretaties over te brengen.

2. Het intensiveren van communicatie, harmonisatie en samenwerking.

Onderlinge communicatie en samenwerking, zowel binnen instellingen als tussen instellingen, moeten bevorderd en geoptimaliseerd worden aldus verschillende deelnemers, bijvoorbeeld door het uitwisselen van *best practices*. Ook werd geopperd dat instellingen/gegevensverwerkers hun procedures voor het verzamelen, opslaan en uitwisselen van gegevens standaardiseren, bijvoorbeeld met behulp van templates. Gepleit werd voor de oprichting van een centraal orgaan of een onafhankelijke instantie die de regie hierover kan voeren.

3. Het bevorderen van vertrouwen en transparantie.

Een belangrijke factor voor succesvolle gegevensuitwisseling en -koppeling is vertrouwen. Zowel het vertrouwen tussen instellingen onderling als het vertrouwen tussen instellingen en het individu/de patiënt dient vergroot te worden. Een belangrijke manier om vertrouwen te vergroten is door transparanter te zijn. Onder meer over het onderzoeksbeleid, welk type onderzoek wordt uitgevoerd, welk type (patiënt)gegevens er wordt gebruikt, wat wordt gedaan om de gegevens te beschermen en de gevolgen van dit alles zijn voor de patiënt.

4. Het aanscherpen van technische en organisatorische maatregelen.

Ook het optimaliseren van verscheidene organisatorische en technische beveiligingsmaatregelen voor het veilig opslaan en verwerken van (bijzondere) persoonsgegevens kan mogelijk helpen de geïdentificeerde belemmeringen te verminderen. Gedacht kan worden aan training van het personeel, zowel op het gebied van data-science als op juridisch/ethisch vlak. Daarnaast werden maatregelen als het gebruik van een TTP en verschillende encryptie methodes geopperd.

5. Het aanpassen van wet- en regelgeving.

Door verschillende deelnemers werd gepleit voor wijziging van de wet. Volgens hen zou de overheid het initiatief moeten nemen tot een verruiming van de wettelijke grondslag voor wetenschappelijk onderzoek/het algemeen belang. Ook dient volgens geïnterviewde de wettelijke taakomschrijving van de zorgverzekeraar verruimd te worden om het gebruik van zorgdeclaratiedata voor wetenschappelijk onderzoek te kunnen bevorderen. Daarnaast werd meermaals de wens geuit om het toestaan van het gebruik van het BSN bij wetenschappelijk onderzoek wettelijk te verankeren.

De set van geïdentificeerde belemmeringen en mogelijke oplossingsrichtingen die het kwalitatieve onderzoek heeft voortgebracht heeft ons inzichten gegeven in de problemen in de huidige praktijk en heeft laten zien waar volgens verschillende belanghebbenden ruimte is voor verbetering. Een aantal van de oplossingsrichtingen pogen wij in dit aanbevelingsdocument verder uit te werken, anderen liggen buiten het bereik van dit project maar geven wel aanleiding voor verder onderzoek en/of actie vanuit de politiek.

III. De Technische verkenning

De doelstelling van de technische verkenning was het bieden van een leidraad voor onderzoekers in *Privacy-Preserving Record Linkage* (PPRL)-methoden. Het combineren van datasets is van groot belang omdat het de leerervaringen voor de gezondheidszorg en de samenleving vergroot, maar het behoud van privacy kan een uitdaging zijn. PPRL-methoden kunnen helpen bij het combineren van gegevens terwijl de privacy van individuen beschermd wordt. PPRL methoden zijn nog in ontwikkeling en de verwachting is dat in de toekomst de methoden nog verder verbeteren. Tabel 3 geeft een overzicht van de huidige modellen, maar het verdient de aanbeveling om bij toekomstige projecten na te gaan of er nieuwe methoden ontwikkeld zijn.

Middels deze verkenning pogen we een overzicht te bieden van beschikbare methoden en een stapsgewijze benadering van PPRL te ontwikkelen. Deze stap-voor-stap benadering werd ontwikkeld door het extraheren en interpreteren van belangrijke stappen en patronen welke zijn geïdentificeerd door middel van een systematische review. Door middel van het doorlopen van dit stappenplan bieden we een gestructureerde aanpak om onderzoekers te helpen transparante en kwalitatief hoogwaardige PPRL uit te voeren.

Het ontwikkelde stappenplan is opgebouwd uit vijf stappen:



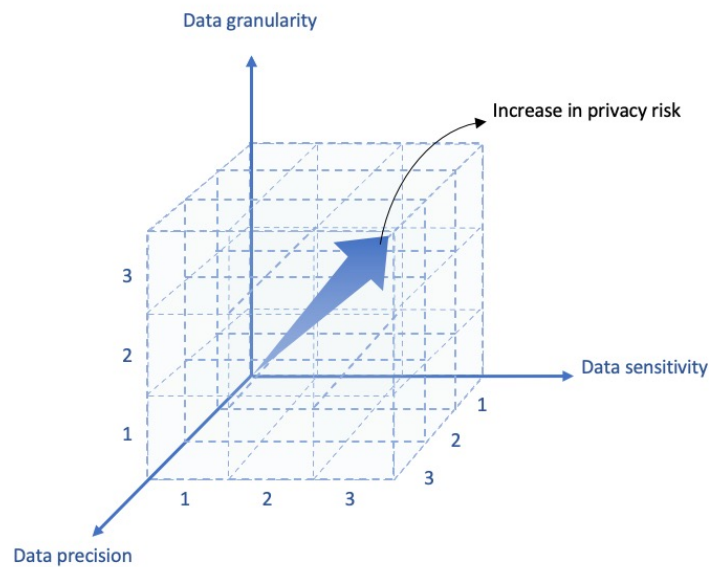
1. De eerste stap in het PPRL-proces is de beoordeling van de privacy-risiconiveaus van de afzonderlijke te koppelen datasets en die van de ontstane dataset na koppeling. Om de privacy-risico's te bepalen, stellen wij voor een privacy-risicoscore te maken voor de informatie in de te koppelen datasets aan de hand van een matrix met granulariteit, gevoeligheid en precisie van de gegevens als assen (figuur 4). Hierbij geldt doorgaans de regel; hoe gedetailleerder de data hoe groter je risico. Aangezien het vaak moeilijk is risiconiveaus voor deze factoren formeel te kwantificeren, hebben we een normatief scoresysteem ontwikkeld om informatie te rangschikken op basis van privacy-risicofactoren die in de literatuur het meest worden genoemd (tabel 2). Om een privacy-risicoscore te verlagen kunnen onderzoekers de data groeperen (waardoor de gegevens minder fijnmazig zijn), gevoelige eigenschappen uitsluiten (waardoor de gegevens minder gevoelig zijn), en exacte gegevenswaarden verhullen (waardoor de gegevens minder nauwkeurig zijn).

2. De tweede stap in het PPRL-proces is het kiezen van een vorm voor koppeling en het opstellen van een bijbehorend partijprotocol. Partijprotocollen beschrijven hoe de bij een PPRL-zaak betrokken partijen willen samenwerken en gegevens met elkaar willen delen. De verschillende partijprotocollen weerspiegelen ook het niveau van vertrouwen tussen de partijen (zie tabel 3).

Naast het de facto aantal partijen dat bij het PPRL-proces betrokken is, wordt onderzoekers aangeraden rekening te houden met drie verschillende modellen die de mate van vertrouwen tussen de partijen weerspiegelen.

 - **Honest-but-curious (HBC)** - gaat ervan uit dat partijen een bepaald protocol volgen en toch nieuwsgierig zijn om meer te weten te komen over de gegevens van de andere partij. Dit model is gebaseerd op vertrouwen en wordt verondersteld door de meeste PPRL-methoden.
 - **Accountable computing/covert** - gaat ervan uit dat partijen zich aan het protocol houden door protocolinteracties te registreren. Dit vereist de invoering van verantwoordingsmaatregelen naast koppelings- en privacybewarende maatregelen.
 - **Kwaadaardig** - gaat ervan uit dat partijen zich willekeurig zullen gedragen en het protocol zullen breken wanneer dat in hun voordeel is. Protocollen volgens dit model moeten gebruik maken van een TTP of van zeer complexe PPRL-methoden.
3. De derde stap is de keuze van de PPRL-methode die het meest geschikt is voor de gegeven situatie. Belangrijk om rekening mee te houden is dat bij elke koppeling van bestanden een afweging moet worden gemaakt tussen de kwaliteit van de koppeling en de bescherming van de privacy van de betrokkenen. Deze afweging komt vooral tot uiting in de methode die wordt gekozen.

In figuur 3 wordt een overzicht van de verschillende PPRL-methodes en een beknopte beschrijving van de methodes weergegeven.
4. De vierde stap is het kiezen van eventuele aanvullende methoden ter bescherming van de persoonlijke levenssfeer om de privacy van de betrokkenen verder te beschermen. Extra privacy verbetering kan op twee manieren worden toegepast: door waardegeneralisering en door het versluieren van waarden. Methoden voor waardegeneralisering richten zich op het beperken van de hoeveelheid gegevens die wordt vrijgegeven door gegevens te groeperen. De bekendste methode hierin is de differentiële privacymethode.
5. De laatste en vijfde stap is de evaluatie na afloop van de kwaliteit, de privacy en de benodigde rekenkracht van het koppelingsproces die voortvloeien uit de in de vorige stappen gemaakte keuzes. Evalueer hoe goed je de datasets aan elkaar hebt kunnen koppelen; evalueer hoe goed je de data verborgen hebt; evalueer hoeveel computerkracht je nodig hebt voor het benodigde privacy beschermingsniveau. (E.g. bij zeer grote datasets kan het voorkomen dat je niet voldoende computerkracht hebt om de benodigde beveiliging te kunnen bieden). Op deze manier poogt de onderzoeker objectief te beoordelen of het beveiligen goed is gegaan en wat er de volgende keer eventueel beter of anders moet.

Figuur 4. Privacy-risiconiveaus**Tabel 2. Privacy risicoberekening**

As	Score	Omschrijving
Granulariteit van de gegevens	1	Zowel persoonsgegevens als gegevensattributen zijn alleen gekoppeld op groeps- of propensity score-niveau
	2	Ofwel de persoonsgegevens ofwel de gegevensattributen zijn gegroepeerd
	3	Zowel de persoonsgegevens als de gegevensattributen zijn gekoppeld op een individueel niveau
Gevoeligheid van de gegevens	1	Geen van de gelinkte gegevens worden aangemerkt als gevoelig
	2	Een deel van de gelinkte gegevens worden aangemerkt als gevoelig
	3	Alle gelinkte gegevens worden aangemerkt als gevoelig
Precisie van de gegevens	1	Alle gegevensattributen zijn bij benadering gelijk aan hun oorspronkelijke waarden; geen gegevensattributen zijn gekoppeld aan hun oorspronkelijke exacte waarden
	2	Sommige van de gegevensattributen zijn bij benadering gelijk aan hun oorspronkelijke waarden; geen gegevensattributen zijn gekoppeld aan hun oorspronkelijke exacte waarden
	3	Geen van de gegevensattributen zijn bij benadering gelijk aan hun oorspronkelijke waarden; geen gegevensattributen zijn gekoppeld aan hun oorspronkelijke exacte waarden
Totaal score:	...	

Tabel 3. Overzicht beschikbare PPRL-methodes

Partij protocollen	Methode	Koppel methode	Omschrijving	Voordelen	Nadelen
>=2	Willekeurige koppelingssleutels	Exacte overeenstemming (deterministisch)	Verwijder identificeerbare informatie en vervang deze door een willekeurig gegenereerde koppelingssleutel. Koppelingssleutels kunnen worden verstrekt door een derde partij (bv. GUID, EUPID, of een computeralgoritme als Mainzelliste)	Gemakkelijk uit te voeren	- Subjecten kunnen vaak nog worden geïdentificeerd aan de hand van unieke combinaties van attributen - Datasets moeten worden geharmoniseerd voordat koppelingssleutels worden gegenereerd - Kwetsbaar voor frequentieaanvallen
	(Beveiligde) hash-linkage sleutel / hash-encoding	Exacte overeenstemming (deterministisch)	Eenrichtings hashfunctie zoals SHA om gegevens te "coderen en te vergelijken". Kan worden gebruikt om unieke koppelingssleutels te maken van ID's om datasets aan elkaar te koppelen of om gegevensattributen te verbergen.	Gemakkelijk uit te voeren	- Subjecten kunnen vaak nog worden geïdentificeerd aan de hand van unieke combinaties van kenmerken - Verschil van één karakter tussen datasets zal resulteren in verschillende hashes - Kwetsbaar voor frequentieaanvallen - Kwetsbaar voor dictionary-aanvallen
	Gecodeerde statistische koppelingssleutel (ESLK)	Exacte overeenstemming (deterministisch)	Koppelingssleutel is met eenrichtingshashes afgeleid van componenten van ID-attributen (bv. achternaam + voornaam + geboortedatum wordt XXXZZYYYMMDD).	Relatief gemakkelijk uit te voeren	- Beperkte privacybescherming - Kwetsbaar voor frequentieaanvallen
	(Veldniveau) Bloom filter codering	Benaderende overeenstemming (probabilistisch)	Bit arrays van n-grammen van ID's in Bloom filters resulterend in gecodeerde hashes waarmee gegevens bij benadering aan elkaar kunnen worden gekoppeld. Traditionele Bloom-filters werden ontwikkeld voor het coderen van strings, maar tegenwoordig bestaan Bloom-filters ook voor numerieke gegevens.	Maakt gegevenskoppeling bij benadering mogelijk	Kwetsbaar voor cryptografische/decoderingsaanvallen
	(Recordniveau) samengestelde Bloom-filters / cryptografische langetermijnsleutels	Benaderende overeenstemming (probabilistisch)	Samengestelde Bloom-filters zijn Bloom-filters op basis van meerdere ID-componenten om de privacy beter te beschermen.	- Maakt gegevenskoppeling bij benadering mogelijk - Sterkere bescherming tegen cryptografische aanvallen	Nog steeds kwetsbaar voor cryptografische aanvallen (maar minder dan traditionele Bloom-filters)
	Op Markovketens gebaseerde Bloom Filter	Benaderende overeenstemming (probabilistisch)	Op Markovketen gebaseerde Bloom-filters zijn ook Bloom-filters maar maken gebruik van Markovketens om de privacy beter te beschermen.	- Maakt gegevenskoppeling bij benadering mogelijk - Sterkere bescherming tegen cryptografische aanvallen	Computationeel kostbaar
	Garbled circuits	Exacte overeenstemming (deterministisch)	Garbled circuits zijn gebaseerd op logistieke circuits waarin één gebruiker een "slot" maakt rond een "sleutel" die uit de gegevens van de andere partij wordt gemaakt.	Veilige, nauwkeurige gegevenskoppeling	- Ongelijke relatie tussen partijen - Niet schaalbaar, vereist een nieuw circuit voor elke koppeling
>=2 w/ TTP	Ontkoppeling van gegevens	Exacte overeenstemming (deterministisch)	Eigenaars van datasets sturen gegevens met identificeerbare gegevens naar TTP, die gegevens koppelt en vervolgens ID's verwijdert	Traditionele koppeling van bestanden kan worden toegepast om datasets te koppelen	- Vereist TTP - Datasets moeten soortgelijke identifiers bevatten om koppeling mogelijk te maken - Kwetsbaar voor collusie
>=3	Meer-partij Bloom filters	Benaderende overeenstemming (probabilistisch)	Meer-partij Bloom filters maken een benaderende match van gegevens tussen meer dan twee partijen mogelijk.	Koppeling tussen meerdere partijen is mogelijk	Kwetsbaar voor cryptografische/decoderingsaanvallen
	Encryptiesystemen / veilige meerpartijtoegang (SMC)	Exacte overeenstemming (deterministisch)	Berekent een functie over verschillende partijen, zodanig dat geen enkele partij de informatie van de andere partijen te weten komt, maar allen de eindresultaten ontvangen. Meest gebruikt: - Beveiligd scalair product - Beveiligde verzameling intersectie - Beveiligde verzameling unie	Maakt gegevenskoppeling met precisie mogelijk, terwijl gegevens van individuele partijen geheim blijven	Computationeel kostbaar



Bijlagen

Bijlage 1

Definitielijst

Bijzondere persoonsgegevens	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, het lidmaatschap van een vakbond blijken, alsmede genetische gegevens, biometrische gegevens, gegevens over gezondheid, gegevens met betrekking tot iemands seksuele gedrag of seksuele gerichtheid. (afgeleid van art 9 lid 1 AVG)
Data Access Committee (DAC)	Een orgaan bestaande uit een of meer leden die verantwoordelijk zijn voor het toezicht op de toegang tot gegevens voor onderzoek dat volgt op het hoofddoel waarvoor de gegevens zijn verzameld, wanneer interne en/of externe aanvragers daartoe een verzoek indienen.
Gezondheidsonderzoek	Wetenschappelijk onderzoek gericht op het beantwoorden van vragen op het gebied van ziekte, gezondheid en gezondheidszorg.
(Juridische) grondslag	Een wettelijke basis die een verwerking van persoonsgegevens rechtvaardigt.
Koppeling	Koppeling van gegevens op individueel persoonsniveau afkomstig van twee of meer verstrekkers voor gezondheidsonderzoeksdoeleinden
Nader gebruik	Verdere verwerking van persoonsgegevens voor wetenschappelijk onderzoek (afgeleid van art. 5.1b AVG)
Routine zorggegevens	Gegevens die routinematig verzameld worden in de zorg door zorgaanbieders en zorgverzekeraars
Verstrekker	De zorgverzekeraar of zorgaanbieder die persoonsgegevens ten behoeve van wetenschappelijk gezondheidsonderzoek aan een onderzoeker en/of onderzoeksinstelling verstrekt. Een verstrekker is verwerkingsverantwoordelijke of handelt namens een verwerkingsverantwoordelijke.