JEJG en Kidos: van persoonsgegevens tot anonieme onderzoeksgegevens

Toestemming voor onderzoek

Op grond van artikel 7:458 BW (Wbgo) en artikel lid 2 Wbp mogen gegevens uit een medisch dossier zonder toestemming van een cliënt ten behoeve van statistiek of wetenschappelijk onderzoek worden verstrekt, uitsluitend wanneer:

1. Vragen van toestemming redelijkerwijs niet mogelijk is en met betrekking tot de uitvoering van het onderzoek is voorzien in zodanige waarborgen, dat de persoonlijke levenssfeer van de patiënt niet onevenredig wordt geschaad; of
2. Het vragen van toestemming gelet op de aard en het doel van het onderzoek in redelijkheid niet kan worden verlangd en de hulpverlener zorg heeft gedragen dat de gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen.

JEJG/Kidos: *Het vragen van uitdrukkelijke toestemming kost onevenredig veel inspanning (de onderzoeksgroep betreft jaarlijks ruim 16.000 leerlingen uit Amsterdam en Amstelland), bij de uitvoering wordt de persoonlijke levenssfeer van de respondenten niet geschaadt (respondenten ondervinden geen hinder van het onderzoek) en uitsluitend niet herleidbare gegevens komen beschikbaar voor onderzoek.*

Daarnaast gelden de volgende voorwaarden:

1. Het onderzoek dient een algemeen belang;
2. Het onderzoek kan niet zonder de desbetreffende gegevens worden uitgevoerd; en
3. Cliënt heeft geen uitdrukkelijk bezwaar gemaakt tegen verstrekking.

JEJG/Kidos: *Het onderzoek dient een algemeen belang (waarborgen en verbeteren kwaliteit van zorg voor jeugdigen), de verwerking van desbetreffende gegevens is noodzakelijk om over een volwaardig onderzoeksbestand te beschikken (zonder persoonsgegevens is koppeling op basis van pseudoniemen niet mogelijk, het beschikbare databestand is dan onvoldoende om openliggende vragen te kunnen beantwoorden) en alle leerlingen (en tot 16 jaar ook ouders) zijn geïnformeerd over hoe ze bezwaar kunnen maken tegen het gebruik van gegevens voor wetenschappelijk onderzoek.*

In geval van één van de uitzonderingsgronden en wanneer aan de drie bovengenoemde voorwaarden is voldaan, mag onderzoek uitgevoerd worden. Maar alleen wanneer gebruik gemaakt wordt van niet herleidbare gegevens. Volgens de Gedragscode Gezondheidsonderzoek (code goed gedrag) moet de onderzoeker die de persoonsgegevens wil verkrijgen (EGZ) dit schriftelijk vastleggen met de verstrekker (JGZ).

Wet bescherming persoonsgegevens

In Nederland wordt de privacy van personen gewaarborgd via de Wet bescherming persoonsgegevens (Wbp). In deze wet is vastgelegd hoe organisaties die persoonsgegevens verwerken dit moeten doen. Een organisatie dient een grondslag - een goede reden - te hebben om persoonsgegevens te mogen verwerken. Doel van de Wbp is dat persoonlijke gegevens alleen zichtbaar zijn voor de personen binnen een organisatie die met deze gegevens moeten werken vanuit de grondslag. Gebruik van deze persoonsgegevens buiten de 'productieomgeving' is niet toegestaan. De Wbp verplicht organisaties om een zogenaamde bewerkersovereenkomst af te sluiten zodra een organisatie als eigenaar van persoonsgegevens een andere organisatie (de bewerker) deze gegevens laat verwerken. Sinds dit jaar (2016) bestaat er ook een Europese privacyverordering: de algemene verordering gegevensbescherming.

JEJG/Kidos: *De afdeling jeugdgezondheidszorg (JGZ) mag persoonsgegevens verwerken, JGZ heeft immers een grondslag om persoonsgegevens te verwerken: doel van JGZ is het bevorderen, beschermen en beveiligen van de gezondheid en de lichamelijke en geestelijke ontwikkeling van jeugdigen in de leeftijd van 0 tot 18 jaar, zowel individuee als op populatieniveau. JGZ voert voor alle kinderen preventieve schreeningen uit: lichamelijk, cognitief en psychosociaal. De afdeling epidemiologie, gezondheidsbevordering en zorginnovatie (EGZ) heeft alleen toegang tot data zonder persoonsgegevens.*

Persoonsgegevens

Een persoonsgegeven is 'elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon'. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Direct identificeerbare gegevens - het wie - zijn van zichzelf herleidbaar tot een persoon. Dit zijn onder andere namen, adressen, telefoonnummers en BSN's. Indirect identificeerbare persoonsgegevens - het wat - zijn gegevens die in combinatie met andere gegevens herleid kunnen worden tot een persoon. Het kan hier gaan om bijvoorbeeld de combinatie van geboortedatum en postcode.

Pseudonieme gegevens

Gegevens zijn anoniem, tenzij ze direct of indirect identificeerbare persoonsgegevens bevatten. Direct identificeerbare persoonsgegevens kunnen worden geanonimiseerd door 'het wie' te verwijderen of door 'het wie' te pseudonimiseren. Pseudonimiseren is een procedure waarmee identificerende gegevens met een bepaald algoritme worden vervangen door versleutelde gegevens (het pseudoniem). Het algoritme kan voor een persoon altijd hetzelfde pseudoniem berekenen, waardoor informatie over de persoon, ook uit verschillende bronnen, kan worden gecombineerd. Pseudonimiseren kan met hashing of encripting. Hashing is onomkeerbaar (eenweg), encripting is omkeerbaar (tweeweg). Het gebruik van een pseudoniem betekent niet automatisch dat de Wbp niet meer van toepassing is. Als

aan de hand van een pseudoniem een persoon uniek kan worden aangewezen in de groep (linkability), is ook het pseudoniem een persoonsgegeven.

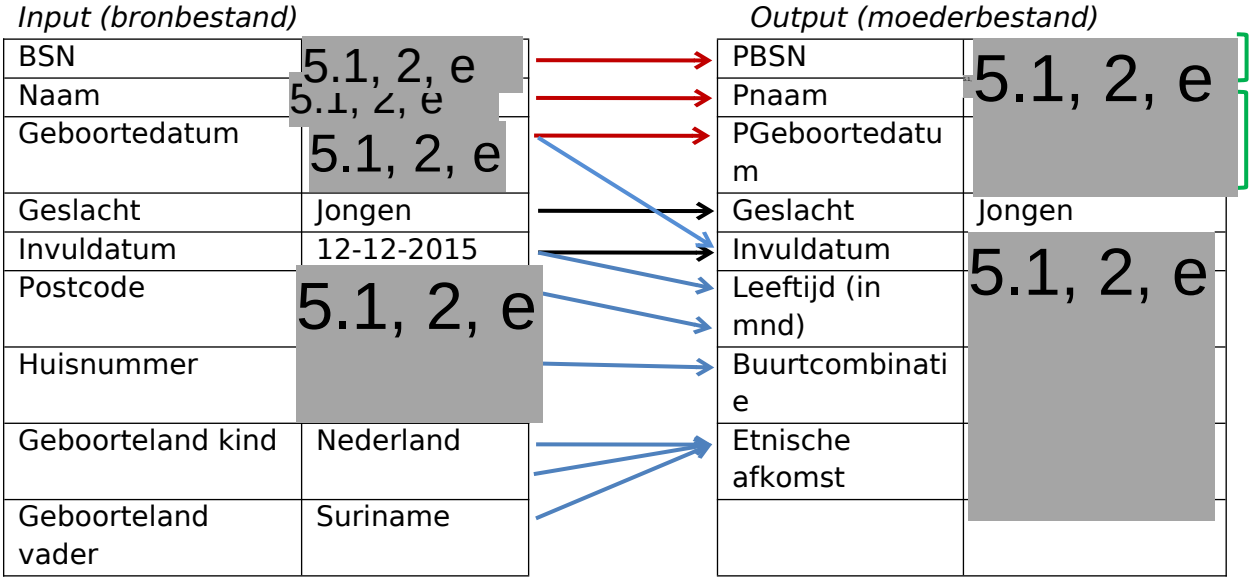
Anonieme gegevens

Om tot een anonieme dataset te komen is het ook noodzakelijk om indirecte herleidbaarheid te voorkomen. Indirecte persoonsgegevens kunnen worden geanonimiseerd door 'het wat' te verwijderen, te pseudonimiseren of op te schalen. Een geboortedatum kan bijvoorbeeld worden opgeschaald (afgerond) tot een geboortejaar of een leeftijd. Het geboorteland van kind, vader en moeder kan worden opgeschaald (gecategoriseerd) tot etnische afkomst. Let op: Door het koppelen van anonieme bestanden kan een samengesteld bestand ontstaan met zo veel 'wat' gegevens dat indirecte herleidbaarheid weer mogelijk is.

Als de gecombineerde dataset van alle 'wie' en 'wat' niet meer (indirect) herleidbaar (anoniem) is, valt deze niet meer onder de Wbp. Anoniem betekent volgens de Wbp niet tot personen herleidbare informatie of het herleiden kost onevenredig veel tijd en inspanning. De Autoriteit Persoonsgegevens (AP), voorheen het College Bescherming Persoonsgegevens (CBP), heeft gesteld dat via pseudonimisering anonieme gegevens kunnen worden bereikt indien aan vier voorwaarden is voldaan:

1. Er wordt vakkundig gebruik gemaakt van pseudonimisering, waarbij de eerste versleuteling van gegevens plaatsvind bij de aanbieder van de gegevens;
2. Er zijn technische en organisatorische maatregelen getroffen om ongewenste herhaalbaarheid van de versleuteling te voorkomen (dat het niet mogelijk is dat iemand miljoenen BSN nummers door de hash-applicatie haalt en dan wellicht een treffer vindt (pseudoniem));
3. De verwerkte gegevens zijn niet (indirect) identificerend;
4. De werkwijze (1 t/m 3) wordt periode ge-audit, beschreven en gepubliceerd.

JEJG/Kidos: *Het bronbestand met alle originele gegevens wordt door JGZ met behulp van de hash applicatie omgezet in een moederbestand. In het moederbestand zijn direct identificeerbare gegevens (BSN, naam en geboortedatum) vervangen door pseudoniemen. Indirect identicifeerbare gegevens (geboortedatum, postcode, huisnummer en geboortelanden) zijn opgeschaald. In het moederbestand zijn de gegevens niet langer identificeerbaar tot individuen. Zie afbeelding 1.*



Geboorteland moeder	Suriname

→ Pseudonimiseren
→ Opschalen
] Uniek persoon

Afbeelding 1. Vertaling van JEJG bronbestand naar JEJG moederbestand.

Afbeelding voor Kidos nog toevoegen!

De moederbestanden worden gekoppeld en beheerd door een datamanager van de afdeling JGZ. Onderzoekers van de afdeling EGZ kunnen via de datamanager een databestand met anonieme gegevens opvragen via een datacontract. In het datacontract staat aangegeven welke onderzoeksvraag beantwoord dient te worden met de data en welke variabelen uit het databestand nodig zijn om deze onderzoeksvraag te beantwoorden. De datamanager stelt een bestand samen met de variabelen uit het datacontract: het werkbestand. Onderzoekers krijgen op die manier uitsluitend anonieme gegevens uit het moederbestand die strikt noodzakelijk zijn voor het betreffende onderzoek. Het werkbestand kan dus per onderzoek(er) verschillen. De datamanager checkt of geen indirecte herleidbaarheid mogelijk is door een combinatie van verschillende gegevens.

Acties GGD

1. Pseudonimiseer op basis van hashing (eenweg) in de productieomgeving van de zorgverlener (JGZ). Zorg dat de hashing voldoet aan de NEN-normen beschreven in NPR-ISO/TS 25237 (Medische informatica-Pseudonimisatie).
2. Voorkom dat ongeauthoriseerd personeel toegang krijgt tot de hashfunctie. Neem maatregelen om het kraken van het hashprogramma te voorkomen.
3. Zorg dat de gegevens in de moeder- en werkbestanden voldoende zijn opgeschaald. Geef nooit werkbestanden aan onderzoekers (derden) die pseudoniemen (koppelgegevens) bevatten.
4. Onderzoekers verrichten geen handelingen met de bestanden bedoeld om tot herleiding van betrokkenen te komen.
5. Alle betrokken leven de Gedragscode in zijn geheel na.
6. Laat een privacywerkgroep elk jaar een audit uitvoeren. Beschrijf de werkwijze helder en plaats het document op relevante openbare websites.

Bij gepseudonimiseerde gegevens gelden verschillende opvattingen. Als de gegevens in theorie niet herleidbaar zijn, door wie dan ook, zijn het geen persoonsgegevens (absolute benadering). Als de gegevens in de praktijk niet herleidbaar zijn, met alle middelen die redelijkerwijs gebruikt kunnen worden, dan zijn het geen persoonsgegevens (risicobenadering). Door nieuwe technieken kan de herleidbaarheid toenemen. De herleidbaarheid dient dan ook met regelmaat te