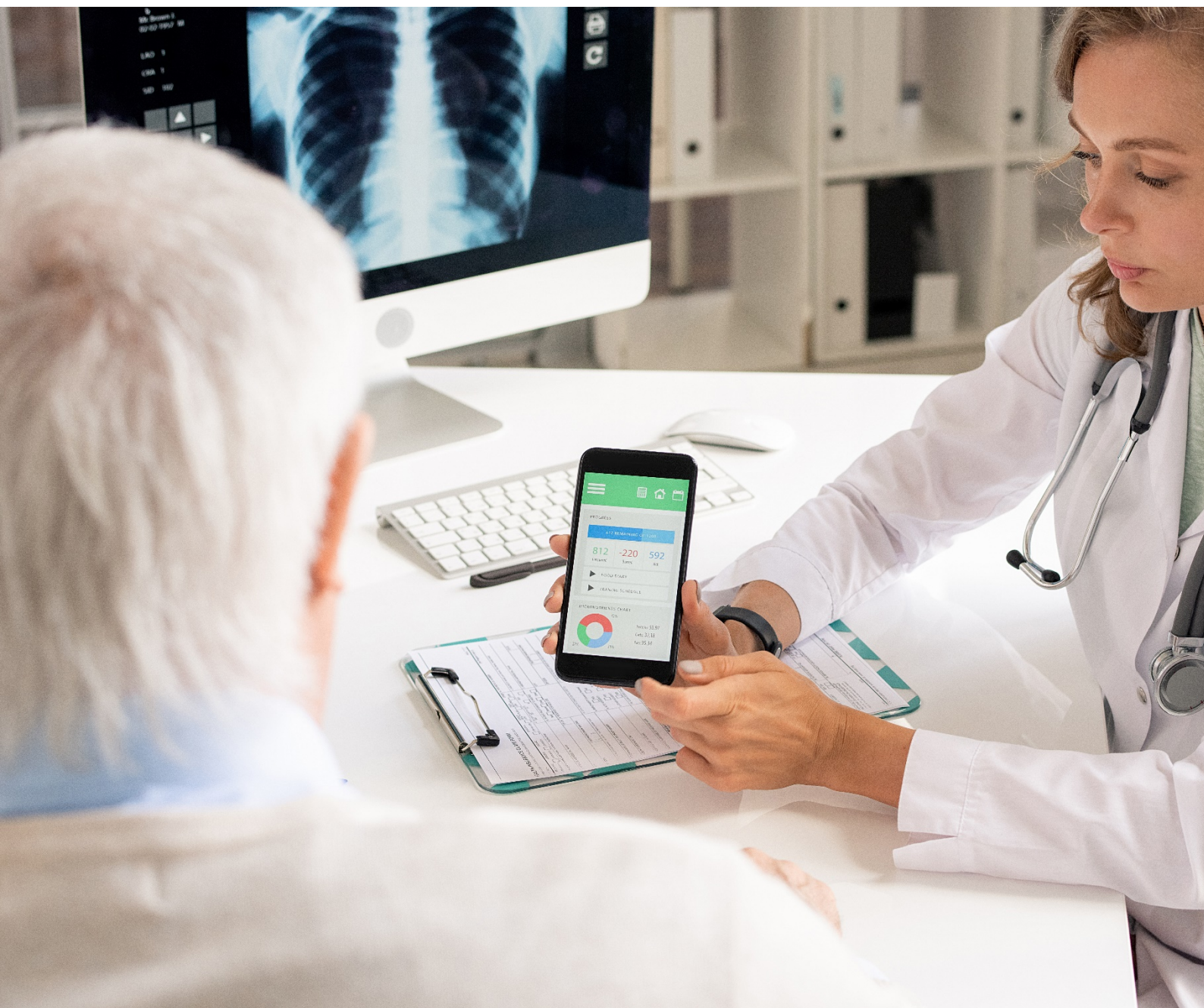


Datasolidariteit voor gezondheid

Verbeterpunten met oog voor ieders belang



Auteurs

Joost Gerritsen en Petra Verhoef

Illustraties

Rathenau Instituut

Foto omslag

Shutterstock

Bij voorkeur citeren als:

Rathenau Instituut (2020). *Datasolidariteit voor gezondheid – Verbeterpunten met oog voor ieders belang*. Den Haag (auteurs: Gerritsen, J. & P. Verhoef).

Voorwoord

Wat we met een arts bespreken of laten meten aan ons lichaam, is zeer persoonlijke informatie. Onze wetgeving ziet er gelukkig streng op toe dat die gegevens vertrouwelijk worden behandeld. De vele digitale gegevens uit medische dossiers bieden ook kansen om de volksgezondheid te verbeteren. Bijvoorbeeld door te onderzoeken welke behandelingen COVID-19 patiënten het meest gunstige herstel geven. Daarom vindt de overheid ‘datasolidariteit’ belangrijk: het beschikbaar stellen van je medische gegevens voor onderzoek.

In de wetgeving is onderzoek met gegevens uit patiëntdossiers in grote lijnen goed geregeld, maar er zijn knelpunten. Onderzoekers vinden wetten soms lastig te interpreteren of met elkaar in tegenspraak, zeker bij internationaal onderzoek. En van gezondheidsgegevens die met nieuwe technologie worden verzameld, zoals patiëntportalen en apps, is niet altijd duidelijk of die onder het medisch beroepsgeheim vallen.

Het Rathenau Instituut zette de door onderzoekers en behandelaars ervaren knelpunten op een rij. Op basis van literatuur en de bestaande wettelijke kaders, concluderen we dat het gebrek aan uniforme wetgeving binnen de EU vraagt om op Europees niveau samen te werken aan verheldering. Daarnaast komen door nieuwe technologie met commerciële spelers fundamentele rechten onder druk te staan. Ook verdient ‘datasolidariteit’ een maatschappelijke discussie. Het gaat alle burgers aan, niet alleen patiënten die nu een behandeling ondergaan.

Met dit rapport willen we bijdragen aan een geïnformeerd politiek en maatschappelijk gesprek over het goede gebruik van digitale gegevens uit patiëntdossiers voor onderzoek dat de volksgezondheid dient. ‘Doelgericht, veilig en wetmatig gezondheidsgegevens delen en gebruiken’ blijft het devies. Dat weten we al uit ons eerder onderzoek, zoals *Opwaarderen*, *Gezondheid Centraal* en de blogserie *Gezonde Bytes*. Alleen door ons voortdurend bewust te zijn van de bijzondere status van medische gegevens, kan met respect voor mensen onderzoek worden gedaan.

Dr. ir. Melanie Peters

Directeur Rathenau Instituut

Samenvatting

Gebruik van digitale gegevens uit medische dossiers ten behoeve van onderzoek is een mooi streven, maar geen sinecure. Het verwerken en gebruiken van digitale medische gegevens vraagt per definitie om veel zorgvuldigheid. Het gaat om persoonlijke gegevens die normaliter tussen hulpverlener en patiënt blijven. Niet voor niets geldt in het medische domein en zorgdomein strikte wetgeving.

De Nederlandse overheid vindt het belangrijk dat de digitale gegevens uit medische dossiers volop worden benut. Met het credo 'datasolidariteit' wil het ministerie van Volksgezondheid, Welzijn en Sport (VWS) dat data uit medische dossiers van burgers beschikbaar komen voor onderzoek waarmee de volksgezondheid is gediend. Dergelijk onderzoek kan bijvoorbeeld worden gebruikt om de effectiviteit van bevolkingsonderzoeken te evalueren of om klinische beslissystemen te ontwikkelen en te trainen. Ook bedrijven, die bijvoorbeeld met medische apparatuur allerlei digitale gegevens verzamelen van patiënten, wordt in het kader van datasolidariteit gevraagd, om de door hen verzamelde digitale data te delen voor onderzoek.

Onderzoek met bestaande data uit medische dossiers

De gevraagde datasolidariteit heeft betrekking op onderzoek met reeds bestaande gegevens uit medische dossiers. Dit onderzoek kan worden gedaan door onderzoekers binnen het ziekenhuis waar de dossiers worden bewaard, of door onderzoekers uit andere ziekenhuizen, onderzoeksinstituten (denk aan het RIVM) of bedrijven. Het zijn onderzoeken waarbij geen handelingen (het verzoek om bloed te laten afnemen of vragenlijsten in te vullen) of gedragsregels (nuchter blijven) worden opgelegd aan deelnemers. De gegevens zijn immers al vastgelegd in een medisch dossier van deze mensen, die zorg of een behandeling hebben ontvangen van een hulpverlener, zoals een arts, fysiotherapeut of logopedist.

Dergelijk onderzoek met bestaande gegevens valt *niet* onder de Wet medisch-wetenschappelijk onderzoek met mensen (WMO, waarbij onder andere veiligheid en ethische aspecten vooraf worden getoetst door een onafhankelijke deskundigencommissie), maar onder de bepalingen van de Wet op de geneeskundige behandelingsovereenkomst (WGBO), naast de wetgeving over persoonsgegevens zoals de Algemene Verordening Gegevens (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). Dit type onderzoek wordt daarom niet-WMO oftewel **nWMO-onderzoek** genoemd. De wetgever heeft middels de WGBO, AVG en UAVG getracht de juiste afwegingen te maken tussen de belangen van het wetenschappelijk onderzoek en statistiek

enerzijds en het belang van de bescherming van persoonsgegevens en de persoonlijke levenssfeer anderzijds.

Het nWMO-onderzoek kan op de ‘traditionele’ manier worden verricht, bijvoorbeeld door een epidemiologische analyse van gegevens met statistische software. Maar het nWMO-onderzoek kan ook om *big data* analyses gaan met behulp van specifieke algoritmes of met nieuwere technieken zoals *machine learning*, een vorm van kunstmatige intelligentie (*artificial intelligence*, AI) waarbij de computer zelf patronen in de data herkent of leert te herkennen.

Datasolidariteit vraagt om duidelijke voorwaarden

Niet alleen onderzoekers, maar ook technologiebedrijven hebben, buiten de behandelrelatie om, interesse in de gegevens. De bedrijven ontwikkelen bijvoorbeeld de patiëntportalen, kunstmatige intelligentie of apps die bij de behandeling of zorg worden ingezet. De grootste van deze bedrijven bevinden zich buiten de EU, bijvoorbeeld in de Verenigde Staten. Data uit medische dossiers helpen hen om hun product of service te verbeteren. Maar deze gegevens raken daarmee mogelijk ook buiten het medische domein. Met goede voorwaarden moet het voor derden mogelijk zijn om met digitale gegevens uit medische dossiers waardevol onderzoek te doen. De WGBO, AVG en UAVG geven hier de uitgangspunten voor. Alle betrokken partijen bij nWMO-onderzoek hebben eigen verantwoordelijkheden.

Van zorgprofessionals die de gegevens beschikbaar kunnen maken voor onderzoek, wordt gevraagd te werken vanuit de uitgangspunten van de wet. Beroepsgroepen kunnen de toepassing van de wet verhelderen. Van onderzoekers en de nieuwe spelers wordt gevraagd dat ze de bijzondere status van deze gegevens respecteren en met zorgprofessionals en andere belanghebbenden de goede vragen formuleren en waardevolle inzichten en toepassingen ontwikkelen. Samenwerken met de medische professionals (de hulpverlener in de behandelrelatie of ingewijde experts) is belangrijk: context ligt immers vaak niet besloten in digitale medische gegevens. Ook de kwaliteit van de gegevens en de relevantie ervan voor beantwoording van de onderzoeksvragen, kunnen het beste door medische professionals en onderzoekers samen worden beoordeeld.

De uitdaging bij het opstellen en toepassen van wetgeving rond hergebruik van gegevens uit medische dossiers voor onderzoek of ontwikkeling, ligt dus in het zorgvuldig afwegen van de belangen, rechten en plichten van de **patiënt** (of cliënt), de **hulpverlener** (arts of andere hulpverlener in de behandelrelatie, bevoegd om de gegevens beschikbaar te maken) en de **onderzoeker** (of ontwikkelaar). De afweging van belangen wordt gemaakt tegen een achtergrond van kansen op verbetering of bescherming van de volksgezondheid, mogelijk gemaakt door het

nWMO-onderzoek. Onderzoekers, hulpverleners en andere medische professionals, zullen doel en gebruikte methode van ieder nWMO-onderzoek zorgvuldig moeten beoordelen.

Uitdagingen en knelpunten van datasolidariteit

Het Ministerie van VWS, de zorgsector, onderzoekers en behartigers van patiëntenbelangen signaleren problemen bij het gebruik van bestaande gegevens uit medische dossiers voor onderzoek naar het verbeteren van gezondheid en zorg van burgers (nWMO-onderzoek). In de Tweede Kamer zijn meermalen vragen gesteld, omdat (veronderstelde) wettelijke beperkingen bij gebruik van deze medische data het ontwikkelen van producten in de zorg zou belemmeren. In de media mengen juristen zich in het debat, maar ook opiniemakers en onderzoekers.

De volgende problemen vormden de aanleiding voor ons onderzoek:

- Hulpverleners en onderzoekers ervaren **problemen bij het interpreteren en toepassen van de wetgeving** rond het gebruik van data uit medische dossiers voor nWMO-onderzoek, bij nationaal en vooral bij internationaal onderzoek. Die wettelijke kaders zijn ook vaak nog in beweging, vooral in het geval van internationaal onderzoek.
- Met name het **krijgen van toestemming van patiënten** – evenals het vaststellen of toestemming vragen echt nodig is – wordt als problematisch ervaren door onderzoekers. In het algemeen willen onderzoekers bij het gebruik van data uit bestaande medische dossiers zo min mogelijk gehinderd worden door obstakels als het vragen van toestemming van de patiënt. Bijvoorbeeld omdat het vragen hiervan niet wenselijk of tijdrovend is.
- **Innovaties** waarbij digitale gezondheidsgegevens worden gegenereerd of verwerkt, zoals *machine learning*, digitale portalen en apps, **lopen uit de pas met bestaande wetgeving voor nWMO-onderzoek**. Zo is onduidelijk of de gegevens die met dit soort technologie verzameld zijn, onder het medisch beroepsgeheim vallen. Dit zijn ook juist innovaties waarmee burgers zelf gegevens inbrengen in een behandelrelatie en waarvan de (verdere) commerciële ontwikkeling afhankelijk is van toegang tot veel data uit medische dossiers.
- Over de **rol van commerciële partijen** zijn vragen, bijvoorbeeld of *for profit* onderzoek met de gegevens uit medische dossiers mag plaatsvinden. Betrokken bedrijven zoeken zelf ook naar passende verdienmodellen.

Doel en centrale vraag van het onderzoek

Het Rathenau Instituut wil met dit rapport bijdragen aan **een goed geïnformeerd politiek en maatschappelijk gesprek** over het gebruik van digitale gegevens uit medische dossiers voor nWMO-onderzoek.

De **centrale vraag** in dit onderzoek luidt:

Wat zijn mogelijke oplossingen voor de knelpunten rond wet- en regelgeving, zoals die nu worden ervaren bij het doen van nWMO-onderzoek?

We formuleren de volgende **deelvragen**:

1. Is de kritiek op de huidige wetgeving bij nWMO-onderzoek terecht, of is er sprake van veronderstelde belemmeringen in plaats van werkelijke belemmeringen? Zijn er extra belemmeringen voor internationaal nWMO-onderzoek? Welke dan?
2. Welke extra kwesties doen zich voor bij nieuwe technologische ontwikkelingen – vaak gefaciliteerd door commerciële partijen – zoals kunstmatige intelligentie, zelfmetingen door patiënten met wearables en digitale communicatie tussen patiënt en hulpverlener? Mogen technologische bedrijven toegang hebben tot de gegevens uit medische dossiers, zelfs voor *for profit* onderzoek?
3. Zijn de regels rond het krijgen van toestemming van de patiënt helder genoeg of kan dat beter?

Onderzoeksmethoden en opzet van rapport

We verkregen middels *desk research* naar literatuur, nieuwsberichten, opinies van toezichthouders en de bestaande wettelijke kaders, waaronder rechtspraak, antwoord op de genoemde vragen. De gebruikte bronnen zijn gepubliceerd in de periode 1990-2020.

Dit rapport beschrijft allereerst **de wettelijke kaders** voor het doen van nWMO-onderzoek dat gebruik maakt van gegevens die afkomstig zijn uit medisch dossiers. We lichten steeds toe welke **fundamentele rechten** de basis vormen van die wettelijke kaders. We beperken ons zoveel mogelijk tot de bronnen die het juridisch kader vormen: de wet (AVG, uitvoeringswet AVG en de WGBO), gezaghebbende rechtspraak en documentatie van toezichthouders.

Met drie voorbeelden (**casussen**) schetsen we de complexiteit van het doen van nWMO-onderzoek dat is gebaseerd op gegevens die worden gegenereerd, gedeeld of geanalyseerd met nieuwe vormen van technologie, zoals kunstmatige intelligentie, zelfmetingen door patiënten met *wearables* en digitale communicatie tussen patiënt en hulpverlener. Twee **stroomdiagrammen** leiden vervolgens de hulpverleners en de onderzoekers door de verschillende wetgeving en toetsingskaders voor nWMO-onderzoek. In de tekst worden de afwegingen besproken, die gemaakt moeten worden tussen de fundamentele rechten van de patiënt – zoals het (grondwettelijk) recht van het individu op bescherming van de

persoonlijke levenssfeer –, de rechten van wetenschappers en het belang van de vooruitgang van de gezondheidszorg. Met voorbeelden uit de casussen of andere actuele voorbeelden, geven we punten aan waarop de wetgeving onvoldoende duidelijkheid biedt. Ook de internationale context komt daar aan de orde. Het vragen van **toestemming** van de patiënt, en de uitzondering op dat uitgangspunt, neemt een prominente plek in.

De belangrijkste **knelpunten** worden vervolgens zo concreet mogelijk op een rij gezet. Tot slot geven we **oplossingsrichtingen** voor het medische domein zelf, beleidsmakers en politici.

Belangrijkste overwegingen bij gebruik van dossiergegevens voor onderzoek

De wet- en regelgeving geeft zowel de hulpverlener als de onderzoeker een aantal overwegingen mee voor het gebruik van gegevens uit medische dossiers voor nWMO-onderzoek. We zetten ze hier op een rij, zodat knelpunten en oplossingsrichtingen beter begrijpelijk zijn.

Hulpverlener

De belangrijkste overwegingen voor de **hulpverlener**, ingegeven door de WGBO, zijn:

- Het **initiatief** tot verzoek om gegevensverstrekking behoort uit te gaan van de onderzoeker.
- **Aan de patiënt toestemming vragen is het uitgangspunt** bij nWMO-onderzoek, behalve bij eigen onderzoek door de hulpverlener.
- Toestemming moet in ieder geval **expliciet en voldoende specifiek** zijn. De patiënt moet daarbij met een redelijke mate van nauwkeurigheid kunnen overzien waartoe zijn toestemming strekt.
- Verstrekking van gegevens over patiënten of inzage in patiëntdossiers aan nWMO-onderzoekers is in bepaalde situaties **toegestaan zónder toestemming van de patiënt**, als het onderzoek valt onder de noemer van **statistisch of wetenschappelijk onderzoek**, op het gebied van de **volksgezondheid** én daarbij een **algemeen belang** dient.
- Altijd moet onderzocht worden of het inderdaad **mogelijk is om af te wijken van de hoofdregel** ‘toestemming vragen van de patiënt’. De wet omschrijft **twee situaties waarin toestemming vragen niet hoeft**. Eén van deze situaties moet aan de orde zijn, anders mag er geen verstrekking van de gegevens zonder toestemming plaatsvinden:
 - toestemming vragen is in redelijkheid niet mogelijk en/of
 - toestemming vragen kan in redelijkheid niet worden verlangd.
- De **uitzonderingen op het beginsel dat toestemming nodig is, kennen als eis** dat de te verstrekken gegevens extra beschermd worden, bijvoorbeeld door codering. Hiervan kan worden afgeweken als alle volgende punten gelden:

- direct herleidbare persoonsgegevens zijn voor het onderzoek noodzakelijk;
- toestemming is in redelijkheid niet mogelijk; en
- er wordt voorzien in zodanige waarborgen, dat de persoonlijke levenssfeer niet onevenredig wordt geschaad.
- Tot slot zijn er nog **twee belangrijke voorwaarden** waaraan moet worden voldaan om de gegevens voor nWMO-onderzoek te mogen gebruiken:
 - **Het onderzoek kan niet zonder de desbetreffende gegevens uitgevoerd worden**, bijvoorbeeld op een andere manier die minder ingrijpend is ten aanzien van de rechten en belangen van de patiënt;
 - De patiënt heeft **geen uitdrukkelijk bezwaar** gemaakt tegen de verstrekking. Hulpverleners moeten een **geen-bewaarsysteem** inrichten en hun patiënten daarover informeren. Als patiënten niet op de hoogte zijn gesteld van het feit dat de gegevens uit hun dossier voor statistiek of wetenschappelijk onderzoek gebruikt konden worden, of als er geen bezwaarmogelijkheid is geweest, dan mogen die gegevens niet worden verstrekt voor onderzoek.
- Als de gegevens worden verstrekt voor onderzoek, of als voor onderzoek inzage wordt verleend in het dossier, dan **maakt de hulpverlener hiervan aantekening in het medisch dossier**.

Onderzoeker

De belangrijkste overwegingen voor de **onderzoeker**, vooral ingegeven door de AVG en UAVG, zijn:

- Kan met zekerheid worden vastgesteld of **de hulpverlener de gegevens had mogen verstrekken**? Als dat niet het geval is, dan mogen de gegevens niet worden gebruikt.
- Verstrekkt de hulpverlener de gegevens op basis van toestemming van de patiënt of op basis van de mogelijkheid die de WGBO biedt om dat zonder toestemming te doen, te weten voor statistiek of wetenschappelijk onderzoek (zie hierboven bij 'hulpverlener')? Als de verstrekking plaatsvindt op basis van toestemming, dan is van belang dat de onderzoeker de gegevens **niet gebruikt buiten de reikwijdte van de gegeven toestemming**. Overigens geeft de wetgever van de (U)AVG, net als de WGBO-wetgever, de voorkeur aan het vragen van toestemming.
- De UAVG **heft voor de onderzoeker het verbod op** om bijzondere persoonsgegevens, zoals gezondheidsgegevens of genetische gegevens, te gebruiken zonder het vragen van toestemming, als aan bepaalde **eisen** is voldaan:
 - het gegevensgebruik moet **noodzakelijk** zijn met het oog op **wetenschappelijk onderzoek of statistische doeleinden**;
 - het onderzoek moet een **algemeen belang** dienen;
 - het **vragen van toestemming blijkt onmogelijk** of kost een **onevenredige inspanning**;

- bij de uitvoering van het onderzoek is voorzien in zodanige waarborgen dat de **persoonlijke levenssfeer** van de patiënt **niet onevenredig wordt geschaad**. Het coderen van gegevens is zo'n waarborg, maar er zijn meer maatregelen denkbaar. Ook moeten de onderzoekers zoveel mogelijk voorkomen, dat de gegevens worden gebruikt voor het nemen van maatregelen of besluiten die *tegen* een patiënt gericht zijn.
- De onderzoekers dienen erop bedacht te zijn, dat zij nog steeds een **rechtsgrond** voor het gegevensgebruik nodig hebben op basis van de AVG: de gegevens moeten worden gebruikt voor een **gerechtvaardigd (onderzoeks)doel** en onderzoekers moeten zorgen dat dit **rechtmatig** gebeurt.
- **Daarnaast dienen de onderzoekers vanzelfsprekend aan alle overige toepasselijke AVG-verplichtingen te voldoen.** Zo moeten de te gebruiken persoonsgegevens:
 - tot een minimum worden beperkt ('*dataminimalisatie*');
 - juist zijn en waar nodig worden gecorrigeerd ('*juistheid*');
 - niet langer worden bewaard in identificerende vorm gelet op de doelen waarvoor de gegevens zijn opgeslagen ('*opslagbeperking*');
 - en
 - passend beveiligd zijn ('*integriteit en vertrouwelijkheid*').

Bovendien moet voor de betrokkene, zoals de patiënt, onder meer **transparant** zijn wat er met de gegevens gebeurt. De verwerkingsverantwoordelijke – de persoon of entiteit die verantwoordelijk is voor de naleving van de AVG (lees: meestal de onderzoeker) – moet kunnen aantonen dat hij voldoet aan de AVG-principes ('*verantwoordingsplicht*').

- Daarnaast maakt de AVG duidelijk dat bij de opzet van het onderzoek het **data protection by design by default-principe** geldt: onderzoekers moeten zowel voorafgaand als tijdens het onderzoek nagaan hoe er gehandeld kan worden in lijn met de AVG.

Belangrijkste geïdentificeerde knelpunten en mogelijke oplossingen

In **hoofdzaak** zijn er de volgende **aandachtspunten voor wetgever, beroeps- en belangenverenigingen en ministeries** die om een oplossing vragen en waarvoor wij een aantal suggesties zullen doen:

- De huidige wetgeving rond nWMO-onderzoek, waarbij vooral de WGBO, AVG en Uitvoeringswet AVG van toepassing zijn, is niet zozeer belemmerend, maar moet wel op veel punten **verhelderd worden en de wetgeving moet beter op elkaar afgestemd worden.**
- Bij nWMO-onderzoek dat is gebaseerd op gegevens die worden gegenereerd of gedeeld met nieuwe vormen van technologie, ontstaat druk op fundamentele rechten, zoals de **bescherming van persoonsgegevens en de eerbiediging**

van het privéleven. Een cruciale vraag is wanneer gegevens beschermd worden onder het beroepsgeheim (en dus de WGBO-regels gevolgd moeten worden) en wanneer dit niet het geval is. Die problemen worden zichtbaar bij *quantified self*, bij gebruik van een interactief portaal tussen patiënt en hulpverlener, maar ook bij de *Personal Health Train*.

- Op de vraag **of commerciële partijen toegang mogen hebben tot de gegevens uit medische dossiers**, zelfs voor *for profit* onderzoek, is nu nog geen antwoord te geven. De ruimte voor commerciële partijen om te verdienen in het kader van nWMO-onderzoek waarvan het de bedoeling is dat het een algemeen belang moet dienen, moet **maatschappelijke worden verkend**.
- De praktijk van nWMO-onderzoek vraagt om **extra uitleg over het vragen van toestemming van patiënten, de reikwijdte van de toestemming en het onderwerp ‘geen bezwaar’** tegen gebruik van medische gegevens. Een structuur om vragen van toestemming te faciliteren en/of een (centraal) geen-bezwaarsysteem worden gemist in het veld.

Het onderzoek leverde diverse **knelpunten op per deelvraag**:

Deelvraag 1: *Is de kritiek op de huidige wetgeving bij nWMO-onderzoek terecht, of is er sprake van veronderstelde belemmeringen in plaats van werkelijke belemmeringen? Zijn er extra belemmeringen voor internationaal nWMO-onderzoek? Welke dan?*

Conclusie 1: Verheldering nodig bij AVG, UAVG en WGBO

- De **AVG** legt nWMO-onderzoek niet verder aan banden ten opzichte van de regels die golden vóór de invoering van deze verordening, maar brengt wel **nieuwe verplichtingen** met zich mee, zoals de verplichte aanstelling van een Functionaris Gegevensbescherming (FG) en het uitvoeren van een Data Protection Impact Assessment (DPIA). De **UAVG** legt nWMO-onderzoek evenmin verder aan banden, vergeleken met eerdere wetgeving.
- De **WGBO-voorwaarden** laten aan de hulpverlener een zekere **ruimte voor interpretatie**, omdat er een afweging moet worden gemaakt tussen de persoonlijke levenssfeer en het belang van het wetenschappelijk onderzoek. Het risico bestaat dat met name kleine hulpverleners die niet de ‘luxe’ hebben van **expert-ondersteuning** (denk aan een zelfstandige huisarts, diëtist of optometrist) een verzoek om gegevens voor nWMO-onderzoek veiligheidshalve afwijzen, vanwege de zorg om civiel- of tuchtrechtelijk aangesproken te kunnen worden. Kansen met gezondheidsgegevens blijven hierdoor liggen.
- De **verhouding tussen de UAVG en de WGBO** geeft aanleiding voor diverse vragen op basis van opmerkingen die zijn gedaan onder de oude Wbp-regeling in het licht van de huidige UAVG-regels, namelijk over:

- a. de **(feitelijke) onmogelijkheid om toestemming te vragen** voor het onderzoek. Volgens de WGBO-wetgever hoeft het niet feitelijk onmogelijk te zijn om toestemming te vragen, maar door de afwijkende opinie van het Europees Comité voor gegevensbescherming (EDPB) is dit niet (meer) zeker;
 - b. de plicht om het onderzoek te **publiceren** (aldus voormalig minister Bruins in 2018);
 - c. **voorwaarden van toestemming** in de WGBO die anders zijn dan de AVG-voorwaarden.
- De voorwaarde gesteld in de WGBO dat het **initiatief tot gegevensverstrekking** uit dient te gaan van de onderzoeker (en niet de hulpverlener) lijkt 'niet meer van deze tijd'.

Oplossingsrichtingen voor verheldering van wetgeving

- Beroepsorganisaties van hulpverleners zouden kunnen bijdragen aan **expert-ondersteuning voor het maken van een gewogen beslissing om gegevens ter beschikking te stellen voor onderzoek**. Algemene voorlichting kan door het Ministerie van VWS worden verzorgd, alsook door toezichthouders als IGJ en de AP. De **gedragscode** "Goed Gedrag" die momenteel herzien wordt, is eveneens een geschikte plek om hulpverleners en onderzoekers te **informer**en over hoe zij overwegingen kunnen maken in lijn met de (U)AVG en WGBO.
- De nationale wetgever dient te **verduidelijken hoe de UAVG-norm** over "het vragen van uitdrukkelijke toestemming dat onmogelijk blijkt of een onevenredige inspanning kost" **zich verhoudt tot de WGBO-normen**.
- De minister van VWS dient te verduidelijken of **publicatie inderdaad een vereiste** is voor wetenschappelijk onderzoek en of de FAIR-principes verplicht zijn op te volgen. Het vereiste van publiceren past bij het belang van openbaar maken van belangrijke inzichten, zoals verwoord in de Unesco standaard en het Nederlandse beleid ten aanzien van Open Science.
- Er dient nader onderzocht te worden of de WGBO inderdaad een ander **toestemmingsregime** heeft dan de AVG en zo ja, of dit leidt tot de conclusie dat de WGBO niet geheel AVG-proof is.
- De nationale wetgever dient te verduidelijken hoe **de eis uit de jaren '90** (initiatief tot gegevensverstrekking ligt bij onderzoeker) **anno 2020** uitgelegd dient te worden.

Conclusie 2: Verheldering nodig bij anonimiseren en pseudonimiseren

- Onder nWMO-onderzoekers bestaat het **misverstand dat anonimiseren van gegevens altijd een verplichting is**. Dit belemmert soms het onderzoek. De WGBO en de (U)AVG verlangen echter geen anonimiseren van gegevens als daardoor het onderzoek niet kan plaatsvinden, zolang het eindresultaat van het onderzoek geen herleidbare gegevens bevat.
- Het **anonimiseren** van gegevens zien sommigen onterecht als een **methode** om het onderzoek volledig te **onttrekken aan de regels van de (U)AVG**.
- Onder de AVG **worden persoonsgegevens beschermd voor en tijdens het anonimiseringsproces**. Bij de WGBO is het onduidelijk of dit ook het geval is.
- In de praktijk wordt niet altijd aan de voorwaarden van **pseudonimisering** voldaan.

Oplossingsrichtingen bij anonimiseren en pseudonimiseren

- Het Ministerie van **VWS zou een discussie kunnen faciliteren over wanneer de WGBO en de (U)AVG dienen te gelden in het licht van geanonimiseerde gegevens**. De discussie zou niet alleen hulpverleners en onderzoekers helderheid kunnen verschaffen over de (on)mogelijkheden van onderzoek met data uit medische dossiers, maar ook hun FG's en eventuele toezichts- of toetsingscommissies.
- De nationale wetgever dient te **verduidelijken of ook de WGBO en de UAVG gelden tot en met het proces van anonimiseren**. Omdat het hier een vraag betreft die deels EU-recht betreft, ligt het voor de hand dat de EDPB betrokken wordt bij de beantwoording hiervan.
- Organisaties verbonden aan hulpverleners en onderzoeksinstituten zouden **procedures voor een goede pseudonimiseringspraktijk** kunnen opstellen, voor zover zulke procedures nog niet bestaan. De (aan te passen) gedragscode kan eveneens hieraan aandacht besteden.
- Aan de oproep van de onderzoekers aan de wetgever om in de UAVG een duidelijk antwoord te geven op de vraag of, en in hoeverre en onder welke voorwaarden, gepseudonimiseerde patiëntgegevens gebruikt mogen worden bij wetenschappelijk onderzoek, bestaat ons inziens **geen dringende noodzaak**. De voorwaarden voor gebruik zijn onder meer reeds beschreven in richtlijnen van de EDPB en de (toelichtingen bij) de wet- en regelgeving als waarborgen die ervoor zorgen dat de persoonlijke levenssfeer van de patiënt niet onevenredig wordt geschaad.

Conclusie 3: Internationaal onderzoek is lastig binnen en buiten de EU

- **Binnen de EU gelden geen uniforme nationale regels voor onderzoek** met medische gegevens. Dit geldt ook voor nWMO-onderzoek. De AVG staat het immers toe dat ieder EU-land eigen wet- en regelgeving opstelt voor onderzoeken met medische data, zodat de wetgeving van de landen onderling kan afwijken. De WGBO en de UAVG bevatten de Nederlandse regeling. In EU-breed onderzoek moet dus per land worden nagegaan wat de nationale regels zijn en hoe daaraan kan worden voldaan. Dat is zeer lastig.
- Gegevensverstrekking aan landen buiten de EU wordt onder voorwaarden toegestaan door de AVG, maar er zijn **knelpunten ten aanzien van gegevensdoorgifte naar de Verenigde Staten** en mogelijk ook andere derde-landen, als met de betreffende ontvangers geen bestendige SCC's gesloten kunnen worden of andere constructies die de gegevensdoorgifte juridisch kunnen onderbouwen.

Oplossingsrichtingen voor internationaal onderzoek

- De grensoverschrijdende knelpunten dienen grensoverschrijdend te worden aangepakt. Een **bespreking van de problematiek via de EU-privacytoezichthouders in de EDPB** ligt voor de hand, maar lost het probleem niet op. Uiteindelijk is de **EU-wetgever aan zet om een geharmoniseerd raamwerk te bewerkstelligen** voor onderzoek met gezondheidsdata. Nederland kan daarin haar stem laten doorklinken via het EU-beleid om tot een Europese onderzoeksruimte te komen, waarvan de beoogde *European Health Data Space* een onderdeel is. Omdat het probleem niet beperkt blijft tot de EU, zal ook contact gezocht moeten worden met de Raad van Europa voor internationale afspraken over gezondheidsdata.
- Daarnaast dient gekeken te worden naar **EU-brede gedragscodes** die onder de AVG erkend worden. Deze kunnen grensoverschrijdende werkwijzen opleggen aan de deelnemende partijen. Ook niet-EU partijen kunnen zich committeren aan zulke EU-brede gedragscodes. De Nederlandse overheid kan daarin, al dan niet via de daartoe bestemde EU-kanalen, een faciliterende rol spelen.
- Tot slot zouden onderzoekers ondersteund kunnen worden met de beantwoording van vragen voor het opzetten van internationaal onderzoek. Als op internationaal niveau gegevens uit medische dossiers worden verzameld voor een onderzoek, dan kan een **clearing house** nagaan of iedere datastroom voldoet aan de toepasselijke wet- en regelgeving. Voor onderzoekers zelf is dit welhaast een ondoenlijke taak. Zo'n *clearing house* zou een **initiatief van de EU kunnen zijn, aangejaagd door lidstaat Nederland**.

Deelvraag 2: *Welke extra kwesties doen zich voor bij nieuwe technologische ontwikkelingen – vaak gefaciliteerd door commerciële partijen – zoals kunstmatige intelligentie, zelfmetingen door patiënten met wearables en digitale communicatie tussen patiënt en hulpverlener? Mogen technologische bedrijven toegang hebben tot de gegevens uit medische dossiers, zelfs voor for profit onderzoek?*

Conclusie 4: Fundamentele rechten staan onder druk bij gebruik van nieuwe technologie

- Het is niet altijd eenvoudig om na te gaan **welke gegevens door het medisch beroepsgeheim worden beschermd**, bijvoorbeeld als het gaat om *quantified self* data van de patiënt, die op verzoek van de arts in de behandelrelatie worden ingebracht, of gegevens gegenereerd in een digitaal portaal, bewaard in een PGO of ‘bezocht’ door een *Personal Health Train*.
- Bij plannen voor bijzondere beleidsmaatregelen, zoals het introduceren van de CoronaMelder-app, moet helder zijn **welke gegevens door het beroepsgeheim zijn beschermd, in welke fases van de gegevensverwerkingen en door wie**. Als dit niet helder is, heeft die onduidelijkheid gevolgen voor de rechten van burgers of de mogelijkheden voor onderzoekers, en daarmee mogelijk voor het algemeen belang. Onderzoekers kunnen bijvoorbeeld niet met zekerheid vaststellen of de lokaal opgeslagen data van de CoronaMelder-app en de hieruit voorvloeiende gegevens over de afspraak met de teststraat, behandeld moeten worden volgens de WGBO of alleen de (U)AVG.
- Door wetgeving vooral in te zetten als **instrument** om politieke beleidsdoelen te realiseren, komt deze losser te staan van de **normatieve uitgangspunten** en opvattingen die binnen het recht relevant zijn. De relatie tussen middel en doel wordt dan al snel uit het oog verloren. Op basis van de wet voor de CoronaMelder kunnen GGD-hulpverleners en onderzoekers bijvoorbeeld moeilijk vaststellen wanneer welke data beschermd worden door het beroepsgeheim, zoals de app-data of de gegevens over de afspraak met de teststraat, laat staan achterhalen welke belangenafwegingen hieraan ten grondslag liggen.
- Het is bij **onderzoeken met AI**, zoals die met *machine learning* of *natural language processing*, niet altijd helder of nWMO-onderzoek dat voldoet aan de WGBO-eis ‘statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid, ten behoeve van het algemeen belang’ aan de orde is. Waar ligt bijvoorbeeld het **onderscheid tussen wetenschappelijk onderzoek met AI en het (verder) ontwikkelen en optimaliseren van een AI-toepassing in de zorg?**
- Commerciële partijen die gegevens uit medische dossiers voor eigen doeleinden willen gebruiken of een vergaande zeggenschap hebben over de te verwerken gegevens uit medisch dossiers, **kunnen belangen hebben die niet vallen onder de ‘algemeen belang’-eis**, zodat de WGBO hen geen ruimte

biedt om zonder toestemming gegevens uit medische dossiers te mogen gebruiken. Als hulpverleners dit niet scherp in de gaten houden, kunnen gegevens onbedoeld zonder toestemming worden vrijgegeven.

- Bij de totstandkoming van de WGBO is niet aan de orde gekomen of commerciële partijen betrokken bij onderzoek dat een ‘algemeen belang’ dient, **de vruchten mogen plukken** van de verwerkingen van gegevens uit medische dossiers. De vraag is of hulpverleners het verdienen aan gegevens uit medische dossiers mogen toelaten, **zonder dat de patiënt daarvoor toestemming heeft gegeven**. Zo ja, onder welke voorwaarden? Zo nee, waarom niet?

Oplossingsrichtingen bij gebruik van nieuwe technologie (van commerciële partijen)

- De wetgever dient de keuzes die zij wil maken – bijvoorbeeld nWMO-onderzoek doen met gegevens verzameld met de CoronaMelder-app – te **expliciteren en te plaatsen in de context van de relevante kernwaarden en rechtsbeginselen**, waarmee rechten van burgers worden gewaarborgd en hen bescherming wordt geboden. Die verankerende beginselen omvatten onder meer publieke gezondheid, individuele vrijheid als de bescherming van persoonsgegevens en eerbiediging van het privéleven, en wetenschapsvrijheid.
- De wetgever dient in het bijzonder uitleg te geven **wanneer gegevens onder het beroepsgeheim vallen**, bijvoorbeeld in het kader van de CoronaMelder-app, en wat dat betekent in het licht van de verankerende beginselen.
- De Autoriteit Persoonsgegevens zou kunnen toelichten wat de **reikwijdte is van ‘verwerkingen ten behoeve van wetenschappelijk onderzoek of met een statistisch oogmerk’ en of de ontwikkeling van AI-tools op basis van dossierdata mogelijk is zonder toestemming**. Het ligt voor hand om de EU-privacytoezichthouders, verenigd in de EDPB, hierbij te betrekken. De begrippen ‘wetenschappelijk onderzoek’ en ‘statistiek’ moeten namelijk autonoom uitgelegd worden binnen de Europese rechtsorde.
- Dit onderwerp verdient een **brede maatschappelijke discussie**. Kamerleden kunnen daarin een voorzet doen, bijvoorbeeld door relevante partijen uit te nodigen voor rondetafelgesprekken. Die partijen zijn in ieder geval patiënten, beroepsbeoefenaren, onderzoekers, technologie-aanbieders en sponsors van onderzoeken.
- Naar aanleiding van deze brede maatschappelijke discussie, kan de wetgever **overwegen om de WGBO-wetgeving aan te passen**.

Deelvraag 3: *Zijn de regels rond het krijgen van toestemming van de patiënt helder genoeg of kan dat beter?*

Conclusie 5: Praktijk vraagt uitleg over toestemming, reikwijdte en 'geen bezwaar'

- Het **'geen-bezwaarsysteem'** wordt in veel ziekenhuizen **gebruikt om nWMO-onderzoek te faciliteren, maar dat gebeurt soms op de verkeerde manier:** als de patiënt geen bezwaar heeft geuit, dan mogen de gegevens worden gebruikt door onderzoekers. De ziekenhuizen gaan voorbij aan het uitgangspunt dat 'geen bezwaar' pas aan de orde komt, als eerst is vastgesteld dat er geen toestemming gevraagd *hoeft* te worden.
- 'Kleine' hulpverleners, zoals tandartsen, apothekers of optometristen zouden gebaat kunnen zijn bij een **centraal geen-bezwaarsysteem**.
- De wens blijft bestaan om slechts een **'globale toestemming'** voor wetenschappelijk onderzoek of statistiek te hoeven vragen, bijvoorbeeld in gevallen waarbij onderzoekers de omvang en reikwijdte van hun onderzoek niet volledig kunnen formuleren. De Europese privacytoezichthouders – verenigd in de EDPB – geven de voorkeur aan het vragen van **toestemming in fases**. Hierop bestaat **kritiek**.

Oplossingsrichtingen voor aspecten rond toestemming

- Er moet geïnvesteerd worden in **voorlichting om de verwarring rond 'geen bezwaar' en 'toestemming vragen' weg te nemen** bij hulpverleners aan wie wordt gevraagd gegevens ter beschikking te stellen voor nWMO-onderzoek. Beroepsorganisaties van de hulpverleners, het Ministerie van VWS en de Autoriteit Persoonsgegevens hebben de taak hier voorlichting over te geven.
- Nader onderzoek zou moeten uitwijzen of **in de praktijk de bezwaarmogelijkheid afdoende wordt gefaciliteerd en of patiënten voldoende op de hoogte zijn van hun rechten**. Als dat niet het geval is, dan kan overwogen de *best practice* van het Amsterdam UMC breed toe te passen in de zorg. Die *best practice* betreft het bieden van een extra mogelijkheid aan patiënten om bezwaar aan te tekenen – los van de algemene bezwaarprocedure – als het vragen van toestemming in redelijkheid niet kan worden verlangd. Deze praktijk kan bijvoorbeeld verankerd worden in de WGBO of in de gedragscode die momenteel wordt herzien.
- Daarnaast kan **nader onderzoek uitwijzen of een centraal 'geen-bezwaarsysteem' een oplossing kan zijn voor eventueel geconstateerde uitvoeringsproblemen**. Een dergelijk systeem kan, vergelijkbaar met het donorregister, patiënten in de gelegenheid stellen om hun bezwaar kenbaar te maken. Onderzoekers en hulpverleners zouden die status eenvoudig kunnen opvragen, hetgeen hun administratieve lasten kan doen verminderen.

- De nationale wetgever of de AP (en/of de EDPB) zouden de onduidelijkheid kunnen wegnemen door **concreet de vraag te beantwoorden of de “uitdrukkelijke toestemming” uit de AVG hetzelfde is als de “uitdrukkelijke toestemming” uit de UAVG of de “toestemming” uit de WGBO**. Als de begrippen hetzelfde zijn, dan ligt het voor de hand de ‘gefaseerde toestemming’ van de EDPB te volgen, maar als de begrippen van elkaar verschillen, dan dient uitleg te worden gegeven wat hiervan de gevolgen zijn.

Tot slot

Ons rapport kan bijdragen aan een geïnformeerd gesprek over **hoe** de huidige juridische kaders het nWMO-onderzoek mogelijk bemoeilijken en **wat** daarvoor de oplossingen zijn. Om de knelpunten rond wet- en regelgeving, zoals die nu worden ervaren bij het doen van nWMO-onderzoek, op te lossen zijn de eerste stappen die gemaakt moeten worden:

- het verhelderen van de wet- en regelgeving binnen Nederland en binnen Europa;
- het ondersteunen van kleinere hulpverleners bij de nWMO-vraagstukken;
- het organiseren van een brede toestemmingsmogelijkheid en/of van een centraal bezwaarregistratiesysteem; en
- het voeren van een maatschappelijke discussie over verdienopties van bedrijven met nWMO-onderzoek.

Goede afwegingen over het beschikbaar maken of gebruiken van medische gegevens zijn belangrijke verantwoordelijkheden voor hulpverleners en onderzoekers, nu de hoeveelheid van digitale medische data en vraag naar nWMO-onderzoek, waaronder *big data* analyse, gestaag toeneemt. **Nut en doel** van nWMO-onderzoek moeten steeds goed worden beoordeeld, alvorens de hulpverlener overgaat tot verstrekken van gegevens uit medische dossiers. *Big data* analyses leiden maar al te vaak tot triviale conclusies die geen handelingsperspectief bieden. Analyses met kleinere datasets, evenwel met data van goede kwaliteit, kunnen belangrijkere inzichten geven voor de volksgezondheid dan het hypothesevrij *crunchen*. Kleinschalige data-analyse geeft tevens veel meer garanties, dat data niet buiten de context waarbinnen ze zijn verzameld of tot schade van patiënten worden gebruikt.

Alle spelers bij nWMO-onderzoek moeten zich voortdurend bewust blijven van hun verantwoordelijkheden. Ook de overheid, die onder druk soms belangrijke maatschappelijke doelen wil bereiken met nWMO-onderzoek. Daarbij raken cruciale zaken als bescherming van het beroepsgeheim op de achtergrond, zeker als daar nieuwe digitale technologie bij wordt gebruikt, zoals apps. Gevoelige persoonlijke gegevens raken met de nieuwe technologie en nieuwe spelers maar al

te gemakkelijk buiten het medische domein. En in wiens handen komen de conclusies van het onderzoek? Wat wordt ermee gedaan, en is dat in het belang van de patiënten? Is de institutionele context waarin de inzichten of ontwikkelde technologie terecht komen voldoende meegenomen? Alleen door zich voortdurend de bijzondere status van deze gegevens te realiseren, kan met respect voor mensen onderzoek en innovatie worden gedaan. Pas dan kan datasolidariteit realiteit worden.

Inhoud

Voorwoord.....	3	
Samenvatting	4	
Inleiding	23	
1	Gebruik van medische data in het licht van fundamentele rechten	34
1.1	Medisch dossier	34
1.2	Geheimhoudingsplicht.....	36
1.2.1	Beroepsgeheim en afgeleid beroepsgeheim.....	36
1.2.2	Naleving geheimhoudingsplicht.....	38
1.3	Fundamentele rechten	40
1.3.1	Bescherming van persoonsgegevens	40
1.3.2	Eerbiediging van het privéleven.....	45
1.3.3	Recht op vrijheid van informatiegaring en wetenschapsvrijheid	47
1.4	Tot slot	48
2	Technologie daagt wetgeving uit bij nWMO-onderzoek.....	49
2.1	Casus 1: machine learning	49
2.2	Casus 2: quantified self	51
2.3	Casus 3: digitale portalen.....	53
2.4	Tot slot	54
3	Gids langs bepalingen voor gebruik van medische data.....	55
3.1	Verstrekking van gegevens uit behandelrelatie	55
3.1.1	Hoofregel: toestemming vragen.....	57
3.1.2	Uitzondering: geen toestemming nodig voor gebruik van gegevens, mits voldaan aan de voorwaarden.....	61
3.1.3	Situatie gelegen bij de patiënt: toestemming vragen is in redelijkheid niet mogelijk.....	65
3.1.4	Situatie gelegen in de aard van het onderzoek: toestemming in redelijkheid niet te verlangen	68
3.1.5	Eerste voorwaarde: het onderzoek kan niet zonder desbetreffende gegevens worden uitgevoerd.....	71
3.1.6	Tweede voorwaarde: de patiënt heeft geen uitdrukkelijk bezwaar gemaakt tegen de verstrekking	71
3.2	Gegevensgebruik door de onderzoekers	75

3.2.1	Onderzoeker ontheven van verbod om bijzondere persoonsgegevens te gebruiken.....	75
3.2.2	Onderzoeker moet altijd rekening houden met overige AVG- verplichtingen.....	78
3.3	Internationaal onderzoek: datadoorgifte buiten EU	79
3.4	Tot slot	81
4	Knelpunten die datasolidariteit in de weg staan.....	83
4.1	Wetgeving voor nWMO-onderzoek in een notendop	84
4.2	Knelpunten en hun oorzaken	87
4.2.1	Knelpunten die hun oorzaak in de (internationale) wetgeving vinden	88
4.2.2	Knelpunten die samenhangen met nieuwe technologie en de toetreding van commerciële spelers in het zorgdomein	95
4.2.3	Knelpunten die spelen rond het vragen van toestemming aan patiënten	102
4.3	Voorbeelden van datasolidariteit in Europa	104
4.4	Tot slot	106
5	Conclusies en oplossingsrichtingen.....	108
5.1	Huidige wetgeving rond nWMO-onderzoek is niet zozeer belemmerend, maar moet wel helderder	110
5.1.1	Verheldering nodig bij AVG, UAVG en WGBO	110
5.1.2	Verheldering nodig bij anonimiseren en pseudonimiseren ...	112
5.1.3	Internationaal onderzoek is lastig binnen de EU	113
5.2	Fundamentele rechten vaker in de knel bij gebruik van nieuwe technologie in nWMO-onderzoek.....	114
5.3	De praktijk vraagt om extra uitleg over toestemming, de reikwijdte ervan en ‘geen bezwaar’	116
5.4	Tot slot	117
	Referenties	120
	Lijst met gebruikte afkortingen.....	129
	Bijlage 1: Verwerking van gezondheidsgegevens en genetische gegevens	131
	Bijlage 2: Verhouding tussen de (U)AVG en de WGBO.....	135
	Bijlage 3: Toestemming volgens de AVG	138

Bijlage 4: Stroomdiagram ‘Data-inzage of -verstrekking voor nWMO- onderzoek door <i>hulpverlener</i>’	142
Bijlage 5: Stroomdiagram ‘Gebruik data voor nWMO-onderzoek door <i>onderzoeker</i>’	143

Inleiding

Medische dossiers bevatten belangrijke persoonlijke gegevens die zijn verzameld binnen de behandelrelatie van patiënt (of cliënt) en arts (of andere hulpverlener). Het gaat om vaststellingen door de arts, onderzoeksresultaten van het lab, digitale meetgegevens die direct afkomstig zijn van medische apparatuur en soms ook digitale gegevens die door de patiënt op verzoek van de arts zelf buiten de ziekenhuismuren zijn geregistreerd. Bijvoorbeeld met behulp van een draagbaar ECG apparaat. Ook kan een patiënt zelf gegevens hebben ingebracht, zoals gemeten lichaamstemperatuur in de afgelopen dagen. De gegevens helpen de arts om zo goed mogelijk een diagnose te stellen of een behandelplan te maken. Juiste zorg voor de patiënt staat daarbij centraal.

Gegevens in medische dossiers zijn zeer persoonlijke gegevens die normaliter tussen hulpverlener en patiënt blijven. Niet voor niets geldt in het medische domein en het zorgdomein strikte wetgeving om fundamentele rechten te borgen, zoals het recht op de bescherming van persoonsgegevens en het recht op de eerbiediging van het privéleven. Op deze manier worden **patiënten beschermd** tegen bijvoorbeeld profilering door overheden of stigmatisering door werkgevers.

Digitalisering in het medische domein

Vrijwel alle medische dossiers, maar ook vaak de communicatie tussen arts en patiënt, zijn tegenwoordig in digitale vorm. Ook de zich snel ontwikkelende technologie van voortdurend meten van lichaamsfuncties genereert steeds meer digitale gezondheidsgegevens in de dossiers. Het Rathenau Instituut heeft eerder veel onderzoek gedaan naar de gevolgen van digitalisering van gezondheidsgegevens in het medische domein (Rathenau Instituut 2014, 2016, 2017, 2018a, 2018b, 2019a, 2019b, 2020a t/m 2020e). De inzichten laten zien dat verwerken, delen en gebruiken van digitale medische gegevens om veel zorgvuldigheid vraagt. Het verandert het systeem van medische zorg, geeft ook niet-patiënten een risicoprofiel en er komen derden in het spel; naast onderzoekers ook techbedrijven. Die hebben grote interesse in de digitale gegevens. Voor onderzoek of andere doelen. Fundamentele rechten kunnen onder druk komen te staan. Een greep uit de lessen noemen we in het kader hieronder.

Kader **Lessen over digitalisering in het medische domein**

Digitalisering beïnvloedt het systeem van medische zorg en volksgezondheid. Digitalisering leidt tot een 'looping effect' waarbij de virtuele omgeving de medische praktijk gaat sturen, zo zagen we in het rapport *Opwaarderen* (Rathenau Instituut, 2017). Dat wil zeggen: digitalisering van gezondheidsgegevens zal leiden tot verandering van het zorgproces en andere rollen van zorgprofessionals. Digitalisering vraagt daarmee om een nieuwe verdeling van verantwoordelijkheden, maar het is nog onduidelijk welke verdeling precies.

In ons onderzoek *Doelgericht digitaliseren* (Rathenau Instituut 2018a) benoemden we dat het gebruiken van big data altijd moet worden gedaan met een duidelijk **doel** en oog voor de (in dit geval: medische) **context**. Breng de algoritmen (lees: de onderzoekers) naar de data en niet andersom. Zo blijven de data in een veilige omgeving waarin de waarden die daar gelden door professionals geborgd zullen blijven.

Consequenties die aan gegevensanalyse worden verbonden, bijvoorbeeld de besluiten die worden genomen aan de hand van klinische beslissystemen, moeten onbevooroordeeld zijn (Rathenau Instituut 2020a). Het is belangrijk dat zoveel mogelijk betrouwbare gegevens van diverse patiënten op een verantwoorde en rechtmatige manier worden gebruikt om bijvoorbeeld beslissystemen gebaseerd op artificial intelligence¹ (AI) te ontwikkelen en te trainen. Goede data gebruiken bij ontwikkeling van AI is daarom cruciaal, zo leerden we van experts in de blogserie *Gezonde Bytes over AI in de zorg* (Rathenau Instituut 2020b).

Het is belangrijk dat onderzoekers **transparant zijn over wat er met de data van individuen gebeurt**: wie gebruikt de data voor wat? De commerciële partijen die de digitale gegevens uit medische dossiers willen gebruiken moeten **duidelijkheid geven over het verdienmodel**. In 2014 riep het Rathenau Instituut de overheid al op om transparantie over het verdienmodel verplicht te stellen bij health apps (Rathenau Instituut 2014). Ook het onderzoek van het rapport *Gezondheid Centraal* (Rathenau Instituut 2019a) laat zien dat transparantie bij veel apps nog ontbreekt, en dat voor gebruikers inzichtelijk moet zijn wat er met de eigen gegevens gebeurt, en wie eraan verdient. De **overheid** heeft een rol te spelen bij het

verhelderen van de status en verantwoordelijkheden van de nieuwe spelers.

*Onderzoek op basis van gegevens uit medische dossiers, bijvoorbeeld om AI-tools binnen de zorg te ontwikkelen, moet bij voorkeur gebeuren in een **cocreatie van ontwikkelaars met gebruikers (patiënten) en hulpverleners** in de gezondheidszorg. Niet 'steeds meer data aan elkaar koppelen' moet centraal staan, maar het gericht verbeteren van de (grip op) gezondheid van patiënten. Veel technologie is kwalitatief niet aan de maat en doet niet wat het belooft. Daarmee werkt deze niet voor professionals en dient dus ook niet het belang van patiënten (Rathenau Instituut 2019a). Het op elkaar betrekken van het 'ecosystem of innovation' en het 'ecosystem of trust' is dus belangrijk (Rathenau Instituut 2020c).*

***Waak voor asymmetrie in macht tussen overheid en burger.** AI-toepassingen van (gezondheids)gegevens kunnen gebruikt worden om gedrag te beïnvloeden en te voorspellen. Hulpverleners en onderzoekers moeten ervoor waken dat gebruik van medische data van individuen voor onderzoek niet leidt tot een asymmetrie in macht. Het vraagt om bescherming van burgers tegen profilering door overheid en stigmatisering door hulpverleners en werkgevers (Rathenau Instituut 2020a).*

Onderzoek met digitale data uit medische dossiers

Door de voortschrijdende digitalisering kunnen de persoonlijke gegevens uit medische dossiers eenvoudiger worden **hergebruikt voor onderzoek of voor het weergeven van statistieken**. De 'goudmijn' aan digitale dossiergegevens is momenteel verspreid over diverse zorginstellingen zoals ziekenhuizen en huisartsenposten. Tegelijkertijd brengen steeds meer partijen gegevens bij elkaar of bieden zij samen toegang tot gegevens. Toegang tot méér gegevens biedt in potentie meer of betere inzichten ten opzichte van een kleinere dataset.

1 "Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)." (8 april 2019). <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>.

Onderzoekers zijn zeer geïnteresseerd in de digitale gegevens die zich bevinden in de medische dossiers. Ze kunnen er onderzoek mee doen waarvan het voorstel niet vooraf hoeft te worden beoordeeld door een onafhankelijke deskundigencommissie in het kader van de Wet medisch-wetenschappelijk onderzoek met mensen (WMO). De onderzoekers leggen immers geen handelingen of gedragsregels op aan deelnemers. Denk aan het verzoek om bloed af te laten nemen of nuchter te blijven. Onderzoek met dergelijke bestaande gegevens valt onder de bepalingen van de Wet op de geneeskundige behandelingsovereenkomst (WGBO) en de wetgeving over persoonsgegevens, zoals de Algemene Verordening Gegevens (AVG) en de Uitvoeringswet AVG (UAVG). Het onderzoek met bestaande gegevens uit medische dossiers wordt daarom niet-WMO-onderzoek oftewel **nWMO-onderzoek** genoemd (zie kader).

Dienen van volksgezondheid, maar ook bedrijfsbelangen

Het nWMO-onderzoek wordt verricht ten behoeve van de volksgezondheid en medische wetenschap. Voorbeelden van instituten die data over volksgezondheid analyseren en statistieken publiceren, zijn het RIVM en koepelorganisaties van huisartsen. De gegevens kunnen zorgen voor levensreddende inzichten. Zo hebben onderzoekers van *Hospital Clinic* in Barcelona op basis van medische gegevens een AI-tool gemaakt die de behandeling van patiënten met ernstige COVID-19 verbetert, met lagere sterftecijfers tot gevolg (Garcia-Vidal et al. 2020).

Naast onderzoekers willen ook commerciële partijen, zoals ontwikkelaars van digitale beslissystemen voor gebruik in de zorg, graag gegevens uit medische dossiers analyseren of hierover beschikken. De bedrijven ontwikkelen bijvoorbeeld de patiëntportalen, AI-tools of apps die bij de behandeling of zorg worden ingezet. De grootste van deze bedrijven bevinden zich buiten de Europese Unie (EU), bijvoorbeeld in de Verenigde Staten. Data uit medische dossiers helpen hen om hun product of service te ontwikkelen of te verbeteren, maar ze raken daarmee ook gemakkelijk buiten het medische domein. Bedrijven kunnen zelf op hun beurt ook veel digitale data in handen hebben, bijvoorbeeld verzameld met de door hen ontwikkelde professionele meetapparatuur in het ziekenhuis.

De gegevens in medische dossiers zijn dus niet alleen waardevol voor inzichten over de volksgezondheid, maar ook voor partijen die dienstverlening exploiteren met behulp van medische gegevens. Consultancyfirma EY schatte vorig jaar in, dat de patiëntgegevens in beheer bij de Britse *National Health Service* (NHS) een jaarlijkse waarde vertegenwoordigen van omgerekend 5,5 miljard Euro, gebaseerd op 55 miljoen dossiers van patiënten (EY 2019). Naar verluidt heeft Google met de NHS een overeenkomst om vijf jaar aan dossiergegevens te ontvangen van diverse ziekenhuizen (Lomas 2019). De waarde van deze datadeal blijft vooralsnog geheim.

Kader **Verschil WMO en nWMO-onderzoek**

Wat zijn de verschillen tussen WMO en nWMO onderzoek? Een WMO-onderzoek bestaat uit medisch wetenschappelijk onderzoek waarin de deelnemers, patiënten maar ook gezonde mensen, worden onderworpen aan handelingen of gedragsregels opgelegd krijgen. Ze moeten bijvoorbeeld meerdere malen bloed laten afnemen voor biochemische analyses. Als gedragsregel dienen ze 's ochtends nuchter te arriveren voor het onderzoek. Kenmerkend aan WMO-onderzoek is, dat er op een of andere manier inbreuk wordt gemaakt op de lichamelijke en/of psychische integriteit van de deelnemer. WMO-onderzoek moet vooraf worden getoetst door een onafhankelijke deskundigencommissie. De WMO bepaalt of dit moet gebeuren door (één van de) erkende medisch-ethische toetsingscommissies (METC's) of de Centrale Commissie Mensgebonden Onderzoek.

De nWMO-onderzoeken waarop dit rapport zich richt, zijn eveneens medisch-wetenschappelijk van aard, maar hiervoor worden geen handelingen of gedragsregels opgelegd aan mensen. Er worden persoonsgegevens gebruikt uit bestaande medisch dossiers. Voorbeelden zijn retrospectief epidemiologisch onderzoek of onderzoek met statussen (dossieronderzoek). Hetzelfde geldt voor niet-direct patiëntgebonden onderzoek, zoals onderzoek met weefsels uit een biobank. In deze nWMO-gevallen hoeft de patiënt niets te doen of te laten, terwijl bij WMO-onderzoek de deelnemer zelf bij het onderzoek is betrokken.

Het is niet altijd eenvoudig vast te stellen of een onderzoek onder de WMO valt of niet. Zo is het invullen van een vragenlijst door een patiënt geen WMO-plichtig onderzoek, maar dit kan anders liggen als de patiënt wordt gevraagd vragenlijsten periodiek in te vullen. Bevolkingsonderzoeken kunnen eveneens in een grijs gebied vallen. Niet-risicovolle onderzoeken vallen doorgaans onder de WGBO en zijn daarmee nWMO-gevallen. Dit kan een bevolkingsscreening naar darmkanker zijn (RIVM 2011; RIVM 2017). Betreft het risicovol onderzoek, dan kan de WMO van toepassing zijn. Onderzoek gerelateerd aan geneesmiddelen kan, afhankelijk van de onderzoeksopzet, zowel een WMO als nWMO-onderzoek zijn. Er bestaan aanwijzingen en toetsingskaders op basis waarvan nagegaan kan worden of er sprake is van een WMO-plichtig onderzoek.²

Datasolidariteit

De Nederlandse overheid vindt het belangrijk dat de digitale gegevens uit medische dossiers volop worden benut, zoals dat gebeurt bij nWMO-onderzoek. Met het credo '**datasolidariteit**' wil het ministerie van Volksgezondheid, Welzijn en Sport (VWS) dat data uit medische dossiers van burgers beschikbaar komen voor onderzoek waarmee de volksgezondheid en medische wetenschap is gediend. Voormalig minister Bruins van het ministerie van Volksgezondheid, Welzijn en Sport (VWS) introduceerde in november 2018³ de term datasolidariteit in een Kamerbrief. In een begeleidend document, getiteld *Data laten werken voor gezondheid – Een kwestie van gewaarborgd vertrouwen*,⁴ beschrijft hij hoe (digitale) gezondheidsdata van meerwaarde kunnen zijn voor onze **eigen gezondheid, maar ook die van anderen**.

Daarbij worden onder meer *big data* analyses genoemd. Datasolidariteit gaat niet alleen burgers aan. Volgens Bruins is datasolidariteit ook van toepassing op **bedrijven**, die bijvoorbeeld met medische apparatuur allerlei digitale gegevens verzamelen van patiënten en die beschikbaar zouden kunnen maken voor onderzoek.

Ook **internationaal** is datasolidariteit actueel. Zo riepen de president van Costa Rica en de Wereldgezondheidsorganisatie (WHO) op tot solidariteit, door onder meer kennis en gegevens te delen over COVID-19 (WHO 2020). Zij verzochten landen, academici, bedrijven en onderzoeksinstituten om data te *poolen* ten behoeve van de *COVID-19 Technology Access Pool* (C-TAP).⁵ Op Europees niveau bestaat een vergelijkbaar initiatief, de COVID-19 Data Portal geheten.⁶ Andere initiatieven zijn het Amerikaanse Secure-IBD, waar hulpverleners wereldwijd gegevens over hun patiënten kunnen invoeren, met als doel kennisbundeling over COVID-19 op één centrale plaats (Marill 2020). De COVID-19 pandemie zorgt ervoor dat wereldwijd onderzoekers en hulpverleners zijn gaan samenwerken, onder meer door het uitwisselen van gegevens en kennis (Lee 2020).

2 Zie bijvoorbeeld het handboek van de Dutch Clinical Research Foundation, te raadplegen via <https://nwmostudies.nl/handboek>, of de informatievoorziening van de Centrale Commissie Mensgebonden Onderzoek, <https://www.ccmo.nl/onderzoekers/wet-en-regelgeving-voor-medisch-wetenschappelijk-onderzoek/uw-onderzoek-wmo-plichtig-of-niet>.

3 Kamerbrief van Minister Bruins voor Medische Zorg & Sport, 'Data laten werken voor gezondheid,' 15 november 2018, <https://www.rijksoverheid.nl/documenten/kamerstukken/2018/11/15/kamerbrief-over-data-laten-werken-voor-gezondheid>.

4 Rijksoverheid, 'Data laten werken voor gezondheid', 15 november 2018, <https://www.rijksoverheid.nl/documenten/brieven/2018/11/15/data-laten-werken-voor-gezondheid>.

5 <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/global-research-on-novel-coronavirus-2019-ncov/covid-19-technology-access-pool>

6 <https://www.covid19dataportal.org/>

nWMO-onderzoek vraagt om duidelijke voorwaarden

Met goede voorwaarden moet het mogelijk zijn voor derden (lees: anderen dan patiënten of hulpverleners) om met digitale gegevens uit medische dossiers waardevol onderzoek te doen voor de volksgezondheid en medische wetenschap. De WGBO, AVG en UAVG geven hier de uitgangspunten voor, zoals we in dit rapport zullen bespreken. Alle betrokken partijen hebben verantwoordelijkheden. Van **zorgprofessionals**, die de gegevens beschikbaar kunnen maken voor onderzoek, wordt gevraagd om nauwgezet te werken vanuit de uitgangspunten van de wet. Beroepsgroepen kunnen de toepassing van de wet verhelderen. Van **onderzoekers** en de **commerciële spelers** wordt gevraagd, dat ze de bijzondere status van deze gegevens respecteren en met zorgprofessionals en andere belanghebbenden de **goede vragen formuleren en waardevolle inzichten en toepassingen ontwikkelen**. Samenwerken met de medische professionals (de hulpverlener in de behandelrelatie of ingewijde experts) is belangrijk. **Context** ligt immers vaak niet besloten in digitale medische gegevens. Ook de **kwaliteit** van de gegevens en de **relevantie** ervan voor beantwoording van de onderzoeksvragen kan het beste door medische professionals worden beoordeeld.

De uitdaging bij het opstellen en toepassen van wetgeving rond hergebruik van gegevens uit medische dossiers voor onderzoek of ontwikkeling, ligt dus in het zorgvuldig afwegen van de belangen, rechten en plichten van de **patiënt** (of cliënt), de **hulpverlener** (arts, ziekenhuis of andere hulpverlener in de behandelrelatie, bevoegd om de gegevens beschikbaar te maken) en de **onderzoeker** (of ontwikkelaar). De afweging van belangen wordt gemaakt tegen een achtergrond van kansen op verbetering of bescherming van de volksgezondheid, mogelijk gemaakt door het nWMO-onderzoek. Onderzoekers, hulpverleners en andere medische professionals zullen doel en gebruikte methode van ieder nWMO-onderzoek zorgvuldig moeten beoordelen.

Uitdagingen en knelpunten bij nWMO-onderzoek volgens het veld

Om verantwoord hergebruik van data uit medische dossiers mogelijk te maken voor nWMO-onderzoek, is het belangrijk dat de wettelijke kaders voor het doen van onderzoek met digitale gegevens uit medisch dossiers helder zijn en dat eventuele knelpunten worden geïdentificeerd en opgelost. Dat geldt ook voor het doen van onderzoek met de data die door de patiënt zelf zijn verzameld ten behoeve van het dossier. Daarover gaat ons onderzoek.

Het Ministerie van VWS, de zorgsector, onderzoekers en behartigers van patiëntenbelangen signaleren knelpunten bij het gebruik van gegevens uit medische dossiers voor onderzoek naar het verbeteren van gezondheid en zorg van Nederlanders. Een belangrijk knelpunt gaat over de privacywetgeving, die als te streng wordt

ervaren. In de Tweede Kamer zijn vragen gesteld,⁷ omdat wettelijke beperkingen bij gebruik van deze medische data het ontwikkelen van producten in de zorg zou belemmeren, zoals de genoemde digitale beslissystemen op basis van AI. In de media mengen juristen zich in het debat, maar ook opiniemakers en onderzoekers.⁸

De volgende problemen vormden de aanleiding voor ons onderzoek:

- Hulpverleners en onderzoekers ervaren **problemen bij het interpreteren en toepassen van de wetgeving** rond gebruik van data uit medische dossiers voor nWMO-onderzoek, bij nationaal en vooral bij internationaal onderzoek. Die wettelijke kaders zijn ook vaak nog in beweging, vooral in het geval van internationaal onderzoek.
- Met name het **krijgen van toestemming van patiënten** – evenals het vaststellen of toestemming vragen echt nodig is – wordt als problematisch ervaren door onderzoekers. In het algemeen willen onderzoekers bij het gebruik van data uit bestaande medische dossiers zo min mogelijk gehinderd worden door obstakels als het vragen van toestemming van de patiënt. Bijvoorbeeld omdat het vragen hiervan niet wenselijk of tijdrovend is.
- **Innovaties** waarbij digitale gezondheidsgegevens worden gegenereerd of verwerkt, zoals *machine learning*, digitale portalen en apps, **lopen uit de pas met bestaande wetgeving voor nWMO-onderzoek**. Zo is bijvoorbeeld onduidelijk of de met dit soort technologie verzamelde gegevens onder het medisch beroepsgeheim vallen. Dit zijn ook juist innovaties waarmee burgers zelf gegevens inbrengen in een behandelrelatie en waarvan de (verdere) commerciële ontwikkeling afhankelijk is van toegang tot veel data uit medische dossiers.
- Over de **rol van commerciële partijen** zijn vragen, bijvoorbeeld of *for profit* onderzoek met de gegevens uit medische dossiers mag plaatsvinden. Betrokken bedrijven zoeken zelf ook naar passende verdienmodellen.

7 Verzoek van het lid Van den Berg (CDA) om een reactie op het artikel FD.nl d.d. 23 september 2019 Strenge privacyregels hinderen medisch onderzoek in Nederland, <https://www.tweedekamer.nl/kamerstukken/detail?id=2019Z17768&did=2019D37042>. Het Financieele Dagblad, 'Minister moet privacyprobleem bij medisch onderzoek aanpakken', 24 september 2019. Reactie Minister Bruins voor Medische Zorg & Sport, 'Kamerbrief met reactie op artikel over secundair gebruik data', 4 oktober 2019, <https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/04/kamerbrief-over-reactie-artikel-fd-over-secundair-gebruik-data>.

8 Het Financieele Dagblad, 'Strenge privacyregels hinderen medisch onderzoek in Nederland', 24 september 2019. BNR Nieuwsradio, 'Privacyregels hinderen onderzoek medische data', 23 september 2019, <https://www.bnr.nl/podcast/internet-vandaag/10390376/privacyregels-hinderen-onderzoek-medische-data>. Opinie van K. Lucassen & C. van Waesberge, 'Juist misvatting over privacyregels belet academisch-medische onderzoek', *Het Financieele Dagblad*, 29 september 2019.

Afbakening van het onderzoek

Zoals aangegeven is dit rapport gericht op nWMO-onderzoeken waarop de WGBO van toepassing is en wetgeving over persoonsgegevens zoals de AVG en de UAVG. Daarbij gaan we er telkens vanuit dat de hulpverlener (arts, maar ook een ziekenhuis) als poortwachter fungeert van de data in medische dossiers. De hulpverlener beslist of de betreffende gegevens wel of niet ter beschikking worden gesteld aan de partij die er onderzoek mee wil verrichten. De hierbij gehanteerde aanname is dat de door de hulpverlener te verstrekken gegevens vallen onder de definitie 'persoonsgegevens'.

Ons rapport gaat *niet* over burgerplatforms, zoals MiDATA⁹ en PatientsLikeMe.¹⁰ Hierbij nemen patiënten zelf het besluit om hun data proactief te delen voor onderzoek. We deden hier eerder onderzoek naar bij het Rathenau Instituut (Rathenau Instituut 2019). In plaats daarvan richten we ons op reeds vanwege de behandelrelatie verzamelde gegevens in het medisch dossier ('primair gebruik'), die later hergebruikt worden voor onderzoek, ook wel 'secundair gebruik' genoemd.

Hoewel we diverse malen stilstaan bij AI-tools die ontwikkeld zijn met behulp van gegevens uit medische dossiers, gaan wij niet in op andere juridische vragen die daarover kunnen rijzen. Bijvoorbeeld of dit medische hulpmiddelen zijn, of dat de geautomatiseerde beslissingen van de AI onder specifieke regels van de AVG vallen. Die toepassingen gaan het onderwerp 'nWMO-onderzoek' te buiten. Tot slot stippen we in dit rapport aan dat medische dossiers genetische gegevens kunnen bevatten. Het Rathenau Instituut publiceert dit najaar een uitgebreid rapport over dit type gegevens. Daarom gaan wij niet diep in op alle juridische aspecten van genetische gegevens. Deze komen in het andere rapport aan bod.

Doelstelling en onderzoeksvragen

Het Rathenau Instituut wil met dit rapport bijdragen aan **een goed geïnformeerd politiek en maatschappelijk** gesprek over het gebruik van digitale gegevens uit medische dossiers voor nWMO-onderzoek.

De **centrale vraag** in dit onderzoek luidt:

Wat zijn mogelijke oplossingen voor de knelpunten rond wet- en regelgeving, zoals die nu worden ervaren bij het doen van nWMO-onderzoek?

We formuleren de volgende **deelvragen**:

1. Is de kritiek op de huidige wetgeving bij nWMO-onderzoek terecht, of is er sprake van veronderstelde belemmeringen in plaats van werkelijke

9 <https://www.midata.coop/en/home/>.

10 <https://www.patientslikeme.com/>.

- belemmeringen? Zijn er extra belemmeringen voor internationaal nWMO-onderzoek? Welke dan?
2. Welke extra kwesties doen zich voor bij nieuwe technologische ontwikkelingen – vaak gefaciliteerd door commerciële partijen – zoals kunstmatige intelligentie, zelfmetingen door patiënten met wearables en digitale communicatie tussen patiënt en hulpverlener? Mogen technologische bedrijven toegang hebben tot de gegevens uit medische dossiers, zelfs voor *for profit* onderzoek?
 3. Zijn de regels rond het krijgen van toestemming van de patiënt helder genoeg of kan dat beter?

Onderzoeksmethoden en opzet van rapport

We verkregen middels *desk research* naar literatuur, nieuwsberichten, opinies van toezichthouders en de bestaande wettelijke kaders, waaronder rechtspraak, antwoord op de genoemde vragen. De gebruikte bronnen zijn gepubliceerd in de periode 1990-2020.

Op 1 september 2020 is het onderzoek inhoudelijk afgerond, met uitzondering van de recente ontwikkelingen naar aanleiding van de *Schrems II*-uitspraak van het Hof van Justitie EU over de internationale doorgifte van data. Naar aanleiding van die uitspraak heeft de European Data Protection Board op 10 november 2020 richtlijnen in consultatie gebracht en die actualiteit is in het rapport opgenomen.

Dit rapport beschrijft in **hoofdstuk 1** allereerst de wettelijke kaders voor het doen van nWMO-onderzoek dat gebruik maakt van gegevens die afkomstig zijn uit medisch dossiers. We lichten steeds toe welke fundamentele rechten daarbij de basis vormen. Over onderzoek met medische gegevens is veel geschreven. We beperken ons zoveel mogelijk tot de bronnen die het juridisch kader vormen: de wet, gezaghebbende rechtspraak en documentatie van toezichthouders. Dus: de AVG, de UAVG, de WGBO en *soft law*, zoals gedragscodes en beroepsrichtlijnen. We merken op dat, als in enkelvoud gesproken wordt van de (U)AVG, we doelen op zowel de AVG als de UAVG.

Hoofdstuk 1 geeft op veel plaatsen het spanningsveld weer tussen enerzijds de fundamentele rechten en belangen van de patiënt en anderzijds de rechten en belangen van de onderzoekers, steeds bij het gebruik van de data voor preventie, behandeling en zorg. De rechten en belangen van de patiënt zijn deels wettelijk vastgelegd in de plichten van de hulpverlener en de onderzoekers, deels op andere manieren geborgd.

In **hoofdstuk 2** signaleren we met drie voorbeelden (casussen) de knelpunten die ontstaan bij de wens om nWMO te doen met data uit medische dossiers, waarbij

nieuwe technologie een rol speelt. Kunstmatige intelligentie, zelf-registratie van gezondheidsparameters door patiënten en digitale communicatie tussen patiënt en arts blijken interessante kansen te bieden, maar passen niet naadloos in de bestaande juridische kaders.

In **hoofdstuk 3** leiden we hulpverleners en onderzoekers door de verschillende wetgeving en toetsingskaders die van toepassing zijn bij nWMO-onderzoek. Hulpverleners wordt gevraagd om de data af te staan; onderzoekers vragen de data op. We doen dit met twee stroomdiagrammen. Met voorbeelden uit de casussen of andere actuele voorbeelden geven we punten aan waarop de wetgeving onvoldoende duidelijkheid biedt. Ook de internationale context komt daar aan de orde. Het vragen van toestemming van de patiënt, en de uitzondering op dat uitgangspunt, neemt in dit hoofdstuk een prominente plek in.

Hoofdstuk 4 geeft op basis van de inzichten uit de eerste drie hoofdstukken antwoord op de drie deelvraagstellingen. Het is een synthese van het spanningsveld tussen de fundamentele rechten van de patiënt, de rechten van wetenschappers en het belang van de vooruitgang van de gezondheidszorg. De belangrijkste knelpunten worden in dit hoofdstuk schematisch op een rij gezet, per deelvraagstelling.

In **hoofdstuk 5** volgen de conclusies en oplossingsrichtingen voor het medische domein, beleidsmakers en politici.

1 Gebruik van medische data in het licht van fundamentele rechten

In Europa zijn de meeste gezondheidssystemen gebaseerd op fundamentele rechten en daarvan afgeleide regels en voorwaarden. Dat is onontbeerlijk voor een betrouwbare en toegankelijke gezondheidszorg voor iedereen. Dit hoofdstuk geeft allereerst een uitleg van 'het medisch dossier'. Dat dossier bevat immers de gegevens die vertrouwelijk behandeld moeten worden. Daarna bespreekt het hoofdstuk achtereenvolgens de geheimhoudingsplicht van de hulpverlener ten aanzien van de dossiergegevens en de fundamentele rechten van de patiënt en de onderzoeker. Dit zijn: het recht op toegang tot de gezondheidszorg, het recht op de bescherming van persoonsgegevens, recht op de eerbiediging van het privéleven en het recht op de wetenschapsvrijheid.

1.1 Medisch dossier

Een behandelrelatie ontstaat zodra een hulpverlener geneeskundige handelingen verricht bij de patiënt. Dit zijn alle verrichtingen die erop gericht zijn om een patiënt van een ziekte te genezen of hem/haar hiervoor te behoeden. Denk aan beoordeling van de gezondheidstoestand, voorlichting vanwege een concrete hulpvraag, advisering, maar ook aan nazorg.

De hulpverlener is op grond van de **Wet op de Geneeskundige Behandelovereenkomst (WGBO)** verplicht een dossier in te richten met betrekking tot de behandeling van de patiënt. Hij houdt in het dossier aantekeningen bij van de gegevens over de gezondheid van de patiënt en de uitgevoerde verrichtingen. In het dossier kunnen ook andere gegevens worden opgenomen, als dit nodig is voor een goede hulpverlening aan de patiënt.

De **dossierplicht** is één van de belangrijkste verplichtingen van de hulpverlener. Het maakt een goede behandeling van de patiënt mogelijk en is onder meer van belang als de behandeling wordt overgedragen aan andere hulpverleners en bij toekomstige behandelingen. Het dossier speelt ook een belangrijke rol bij de beoordeling van de behandeling achteraf.

Diverse wettelijke bepalingen bevatten voorschriften over 'gegevens uit het dossier'. Soms bestaat de indruk dat het gaat om één dossier dat wordt bewaard op één plek, maar in de praktijk is dat meestal niet het geval. Het volledige medische

dossier ligt verspreid over alle plaatsen waar de patiënt behandeld is geweest, meestal in digitale vorm in elektronisch patiëntendossiers (EPD's) maar ook in fysieke, papieren, vorm, opgeslagen in dossierkasten. Al deze gegevens, die in diverse behandelrelaties zijn verzameld, maken onderdeel uit van het medisch dossier (zie kader).

Kader **Inhoud medisch dossier**

Het 'medisch dossier' bevat alle informatie over de behandeling en de begeleiding van de patiënt die noodzakelijk is voor een goede hulpverlening en andere relevante gegevens. Bijvoorbeeld diagnoses, onderzoeksresultaten, beoordelingen door behandelende artsen en verrichte behandelingen of ingrepen.¹¹ Persoonlijke werkaantekeningen, zoals eigen indrukken, vermoedens en vragen van de hulpverlener, dienen buiten het medisch dossier te worden gehouden.

Desgevraagd voegt de hulpverlener een door de patiënt afgegeven verklaring toe aan het dossier. Bijvoorbeeld een zienswijze van de patiënt die afwijkt van de hulpverlener. Als gegevens zijn verstrekt over de patiënt omwille van statistiek of wetenschappelijk onderzoek, dan wordt hiervan een aantekening gemaakt in het dossier.

De hulpverlener bewaart het dossier 20 jaar, gerekend vanaf het tijdstip waarop de laatste wijziging in het dossier heeft plaatsgevonden. Het dossier kan ook langer worden bewaard als dit redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit. Na het verloop van de bewaartermijn dient de hulpverlener het dossier te vernietigen. Dit kan ook eerder, als de patiënt hierom heeft verzocht.

Soms vindt er een gegevensuitwisseling plaats, bijvoorbeeld tussen de huisarts en het ziekenhuis. Er bestaat vooralsnog geen landelijke, overkoepelende dataverzameling van alle gegevens. Wel zijn er **Persoonlijke Gezondheidsomgevingen** (PGO's) in ontwikkeling.¹² Dit zijn een soort digitale persoonlijke datakluisen waarin verschillende soorten informatie over gezondheid

11 Overweging 63 AVG.

12 Voor een overzicht van PGO's met een MedMij-label, zie: <https://www.medmij.nl/pgo/>.

zijn verzameld. Bijvoorbeeld over behandelingen, medicijngebruik, onderzoekuitslagen of data zelfgemeten met apps en *wearables*. De bedoeling is dat burgers met PGO's, van geboorte tot hun dood, inzage en controle kunnen houden op hun eigen gezondheidsgegevens (Rathenau Instituut 2019). Overheid en PGO-ontwikkelaars verwachten dat PGO's zorgen voor een actieve deelname aan de eigen zorg, zodat burgers proactief en preventief kunnen werken aan de eigen gezondheid, onder andere door zelf gegevens over hun gezondheid te genereren, en op basis van deze gegevens beslissingen te nemen over hun eigen zorgproces en gezondheid. De toekomst zal uitwijzen of deze verwachting uitkomt.

1.2 Geheimhoudingsplicht

Als onderzoekers gegevens nodig hebben uit medische dossiers of anderszins inlichtingen over de patiënt willen gebruiken, dan komt het beroepsgeheim van de hulpverlener (of hulpverleners) die het dossier onder zich houdt in beeld. Dit beroepsgeheim, 400 jaar voor Christus voor het eerst geformuleerd door Hippocrates, is in Nederland sinds 1865 wettelijk erkend – weliswaar in aangepaste vorm. Dat is niet zonder reden. De geheimhoudingsplicht van de arts dient zowel het individuele (privacy)belang van de patiënt, als een algemeen belang.

Het algemene belang houdt in, dat niemand zich weerhouden hoeft te voelen om zich tot de gezondheidszorg te wenden, bijvoorbeeld vanwege de vrees dat informatie over zijn of haar aandoening kenbaar raakt bij anderen. Geheimhouding is nodig, niet alleen voor zieken die uit schaamte of angst voor uitsluiting geneeskundige hulp zouden vermijden, maar ook omdat vroege opsporing van bijvoorbeeld besmettelijke ziekten de algemene gezondheid van de bevolking ten goede komt (Van Veen 2004, p. 27). Naast een individueel belang is er dus ook een breder maatschappelijke belang om vertrouwelijkheid te waarborgen, zodat niemand zich gehinderd voelt om medische hulp in te roepen. Kortom, hoe meer mensen zich melden bij de dokter, des te beter dat is voor de volksgezondheid.

1.2.1 Beroepsgeheim en afgeleid beroepsgeheim

De geheimhoudingsplicht voor medische beroepsbeoefenaren wordt op twee plaatsen in de wet beschreven. De **Wet op de Beroepen in de Individuele Gezondheidszorg** (Wet BIG) verplicht geheimhouding voor de daarin genoemde beroepsbeoefenaren in de individuele gezondheidszorg (zie Tabel 1). Daarnaast stelt de eerder genoemde WGBO geheimhouding verplicht voor hulpverleners die een contractuele behandelrelatie met een patiënt (of cliënt) zijn aangegaan. Deze relatie ontstaat zodra een hulpverlener geneeskundige handelingen verricht bij de

patiënt, in opdracht van de patiënt zelf of een ander. In juridisch jargon wordt dit een geneeskundige behandelingsovereenkomst genoemd, kortweg 'behandelrelatie'. Onder 'hulpverlener' vallen zowel individuele beroepsbeoefenaren (denk aan artsen) als rechtspersonen, zoals ziekenhuizen en andere zorgaanbieders. Omwille van de leesbaarheid wordt in dit rapport telkens verwezen naar 'hulpverlener'.

Tabel 1 **Beroepsbeoefenaren volgens de Wet BIG**

Artikel 3-beroepen	Artikel 34-beroepen	Artikel 36a-beroepen (experimenteerberoepen)
Apotheker	Apothekersassistent	Klinisch technoloog
Arts	Diëtist	BSc Medisch Hulpverlener
Fysiotherapeut	Ergotherapeut	Geregistreerd mondhygiënist (sinds 1 juli 2020)
Gezondheidszorgpsycholoog	Huidtherapeut	
Orthopedagoog-generalist	Klinisch fysicus	
Physician assistant	Logopedist	
Tandarts	Mondhygiënist	
Verloskundige	Oefentherapeut	
Verpleegkundige	Optometrist	
	Orthopist	
	Podotherapeut	
	Radiodiagnostisch laborant	
	Radiotherapeutisch laborant	
	Tandprotheticus	
	Verzorgende in de individuele gezondheidszorg (VIG-er)	

Naast de **wettelijke geheimhoudingsplicht**, kan een medewerker van een zorginstelling, bijvoorbeeld een secretariaal medewerker of schoonmaker, **contractueel gebonden zijn aan geheimhouding**. Dit wordt meestal vastgelegd in het arbeidscontract. Ook kan geheimhouding voortvloeien uit **beroepscode**s voor personeel in de zorg. In dit verband is belangrijk om te weten dat er zoiets als

een *afgeleid* beroepsgeheim bestaat. Het **afgeleid beroepsgeheim** geldt voor alle personen die beroepsmatig op de hoogte raken van behandelgegevens van de patiënt. Het gaat niet alleen om (dokters)assistenten, maar ook om bijvoorbeeld bestuurders, secretariële medewerkers, bewakingspersoneel, ICT-medewerkers en schoonmakers (Buijsen et al. 2012).

Tot nu toe bedoelen we met de geheimhoudingsplicht de *zwijgplicht* van de hulpverlener om alles wat aan hem door de patiënt is toevertrouwd, waaronder de gegevens in het medisch dossier. Die informatie mag in de regel niet aan anderen worden verstrekt. Dat is iets anders dan het *verschoningsrecht*, dat eveneens volgt uit de geheimhoudingsplicht. Met een beroep op dit recht hoeft een beroepsbeoefenaar in principe niet te spreken over zijn patiënt. Bijvoorbeeld tegenover de rechter als hij als getuige is opgeroepen of in het geval politie of justitie gegevens vorderen.

In dit rapport richten we ons op de zwijgplicht, omdat het verzoek om gegevensverstrekking wordt gedaan door partijen die onderzoek willen verrichten omwille van een algemeen belang. Rechters, politie en justitie vallen daarbuiten. Belangrijk te weten: onderzoekers die gegevens ontvangen van een hulpverlener hebben *geen* afgeleid beroepsgeheim en kunnen dus geen beroep doen op een zwijgplicht of verschoningsrecht.

1.2.2 Naleving geheimhoudingsplicht

Naleving van de geheimhoudingsplicht is niet vrijblijvend. Als de hulpverlener ongeoorloofd zijn geheimhoudingsplicht schendt, dan zijn daar gevolgen aan verbonden. Dit kan strafbaar zijn en er kan tuchtrechtelijk worden ingegrepen. Voor een overzicht van de gevolgen van een schending van de geheimhoudingsplicht: zie kader hierna.

Alleen al vanwege deze gevolgen is het voor hulpverleners van belang goed na te gaan of zij gegevens uit medische dossiers mogen verstrekken aan onderzoekers. De WGBO bevat hiervoor de belangrijkste voorschriften. Als **uitgangspunt geldt dat gegevens voor wetenschappelijk onderzoek of statistiek alleen met toestemming van de patiënt mogen worden verstrekt**. De WGBO kent echter een uitzondering hierop als toestemming in redelijkheid niet mogelijk is of niet kan worden verlangd. Hoofdstuk 3 biedt hulpverleners (paragraaf 3.1) en onderzoekers (paragraaf 3.2) handvatten om te beoordelen wanneer de gegevens mogen worden verstrekt.

Kader **Gevolgen overtreding geheimhoudingsplicht**

Schending van het beroepsgeheim kan worden aangekaart bij de tuchtcolleges voor de gezondheidszorg. Een tuchtcollege kan maatregelen opleggen, zoals een waarschuwing, berisping of geldboete.

Daarnaast is schending van de wettelijke geheimhoudingsplicht strafbaar volgens artikel 272 van het Wetboek van Strafrecht. Een opzettelijke schending kan worden gestraft met een gevangenisstraf tot 4 jaar of met een geldboete tot € 21.750,--. Zo trof het VUmc een schikking met het Openbaar Ministerie, nadat zij patiënten liet filmen zonder hun toestemming voor een TV-programma.¹³ Verder kan op basis van de Wet BIG de minister voor Medische Zorg bij schendingen van het beroepsgeheim bestuurlijke boetes opleggen op basis van de Wet BIG.

Toezichthouders, ten slotte, kunnen ook een rol spelen als de geheimhoudingsplicht wordt overtreden. Zo houdt de Inspectie Gezondheidszorg en Jeugd (IGJ, voorheen IGZ) toezicht op de naleving van de Wet BIG, vooral vanwege het voorkomen van risico's voor de veiligheid van de patiënt. Daarnaast kan de Autoriteit Persoonsgegevens (AP) handhaven. Als het medisch dossier persoonsgegevens bevat, en dat is al snel het geval, dan is er sprake van een 'onrechtmatige gegevensverwerking' als de gegevens worden ingezien door personen die daartoe niet bevoegd zijn. Bijvoorbeeld collega-hulpverleners die een medisch dossier inzien, zonder dat zij iets te maken hebben met de behandeling van de patiënt. Een ziekenhuis moet adequate maatregelen treffen om zulke onbevoegde toegang te voorkomen. Het HagaZiekenhuis deed dit onvoldoende, waarop de AP het ziekenhuis een boete van 460.000 euro oplegde.¹⁴ Het AP en IGJ hebben een samenwerkingsconvenant gesloten om onderling handhavingstaken te verdelen als beide toezichthouders bevoegd zijn om in te grijpen.

13 Bijzonder Strafrecht, 'VUmc en Eyeworks: stand van zaken', 7 november 2013, <https://www.bijzonderstrafrecht.nl/home/vumc-en-eyeworks-stand-van-zaken>.

14 Autoriteit Persoonsgegevens, 'Haga beboet voor onvoldoende interne beveiliging patiëntendossiers', 16 juli 2019, <https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers>.

1.3 Fundamentele rechten

De hiervoor geschetste geheimhoudingsplicht van hulpverleners en de door onderzoekers verlangde ontvangst van gegevens uit medische dossiers, moeten worden gezien in het licht van **fundamentele rechten**, ook wel grondrechten of mensenrechten genoemd. Deze rechten vormen het algemene juridische kader waarin de wettelijke voorschriften zijn opgenomen van bijvoorbeeld de WGBO, AVG en UAVG. Voor onderzoek met medische gegevens spelen met name de volgende rechten een rol: de **bescherming van persoonsgegevens**, de **eerbiediging van het privéleven** en de **wetenschapsvrijheid**. De rechten worden hieronder besproken zodat verhelderd wordt, waarom de wettelijke regels bestaan en binnen welke kaders mogelijk nieuwe regels moeten passen.

Het ‘medisch beroepsgeheim’ is op zichzelf geen fundamenteel recht, maar hangt wel samen met het fundamentele **recht op toegang tot gezondheidszorg**. Vergelijkbaar met de overwegingen genoemd in paragraaf 1.2, is het idee dat zonder juridische verankering van het beroepsgeheim hulpbehoevenden zich afgeschrikt kunnen voelen om persoonlijke informatie te delen die nodig is voor een goede behandeling, of zich ontmoedigd kunnen voelen om medische hulp te zoeken.

Daarmee brengen ze de eigen gezondheid en de maatschappij in gevaar, bijvoorbeeld in het geval van overdraagbare ziektes als COVID-19. Van de staat Nederland wordt daarom verwacht dat zij voorzieningen voor de gezondheidszorg zo inricht, dat deze geheimhouding tussen patiënt en arts waarborgen (Ministerie VWS 2016). Zo moet volgens het Straatsburgse Mensenrechtenhof – het hoogste rechtcollege dat beslist over klachten op basis van het **Europees Verdrag voor de Rechten van de Mens (EVRM)** – nationale wetgeving voldoende waarborgen bieden omwille van de vertrouwelijkheid van gezondheidsgegevens (ECrHR 2019, alinea 178). Nederland heeft dat in de Wet BIG en de WGBO geregeld.

1.3.1 Bescherming van persoonsgegevens

Het EU-Grondrechtenhandvest¹⁵ bevat een algemeen recht op bescherming van persoonsgegevens. Dit wordt ook wel het gegevensbeschermingsrecht genoemd. Op basis van dit fundamentele recht moeten gegevens eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene (hier: de patiënt) of op basis van een andere gerechtvaardigde wettelijke grondslag (ook wel

15 Voluit “Handvest van de Grondrechten van de Europese Unie”, te raadplegen via: <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A12012P%2FTXT>. Het Handvest werd in de EU juridisch bindend met de inwerkingtreding van het Verdrag van Lissabon in december 2009.

‘rechtsgrond’ genoemd). Een ‘eerlijke verwerking’ betekent dat er een behoorlijke belangenafweging heeft plaatsgevonden bij verwerking van gegevens zodat deze niet ongerechtvaardigd, schadelijk, discriminerend of misleidend is. Ook heeft iedereen het recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.

Onder ‘betrokkene’ dient degene te worden verstaan op wie de gegevens betrekking hebben. In dit rapport wordt met de ‘betrokkene’ de patiënt bedoeld. Het **fundamentele recht op gegevensbescherming** is uitgewerkt in de AVG waarop in Nederland de **Autoriteit Persoonsgegevens** (AP) toezicht houdt.¹⁶

De juridische bronnen van het ‘gegevensbeschermingsrecht’ trachten regels te stellen op basis waarvan persoonsgegevens **zorgvuldig gebruikt** mogen worden. Het is dus niet zo dat persoonsgegevens altijd geheim moeten blijven, of dat het op voorhand altijd ‘verboden’ is deze te gebruiken. Slechts in enkele gevallen wordt gegevensgebruik vergaand aan banden gelegd, bijvoorbeeld als er sprake is van gezondheidsgegevens. Dit komt hieronder aan de orde. Eerst zetten we de begrippen ‘persoonsgegevens’ en ‘bijzondere persoonsgegevens’ uiteen.

Persoonsgegevens algemeen

De AVG is van toepassing op de geautomatiseerde **verwerking van persoonsgegevens**. De AVG bepaalt daarmee de plichten van de partijen die persoonsgegevens verwerken, waaronder de onderzoekers of ontwikkelaars die met de gegevens nWMO-onderzoek willen doen. Een ‘verwerking’ betreft alle denkbare handelingen die ten aanzien van persoonsgegevens verricht kunnen worden. Bijvoorbeeld de verzameling, analyse of opslag van persoonsgegevens. De vernietiging of anonimisering van persoonsgegevens vallen eveneens onder de noemer van ‘verwerking’. Ook persoonsgegevens die aanvankelijk niet-geautomatiseerd zijn geregistreerd, maar die bestemd zijn om later te worden opgenomen in een ‘bestand’ (of dat al zijn) zijn ‘verwerkingen van persoonsgegevens’. Denk aan de pen-en-papier aantekeningen van een arts die later in een elektronisch patiëntendossier opgenomen zullen worden. In dit rapport worden de termen ‘verwerking’ en ‘gebruik van gegevens’ of ‘gegevensgebruik’ als synoniemen gehanteerd.¹⁷

Persoonsgegevens worden gedefinieerd als **alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon**.¹⁸ Dit is een brede definitie. Als identificeerbaar wordt beschouwd een natuurlijke persoon, zoals een

16 Op internationaal niveau is naast de AVG het Dataprotectieverdrag uit 1981 relevant, dat in 2018 gemoderniseerd is. Dit verdrag lijkt op de AVG, maar is minder gedetailleerd. Een belangrijk verschil is dat het Dataprotectieverdrag door meer landen wordt onderschreven dan de AVG. De AVG is van toepassing op 27 EU-landen en de landen van de EER (Liechtenstein, Noorwegen en IJsland), terwijl het Dataprotectieverdrag wordt onderschreven door 55 landen.

17 Dit alles volgt uit de AVG, in het bijzonder de artikelen 2 lid 1, 4 leden 2 en 6 AVG.

18 Artikel 4 lid 1 AVG.

patiënt, die direct of indirect kan worden geïdentificeerd. De indirecte identificatie is aan de orde als identificatie mogelijk is met behulp van indicatoren zoals een naam, een patiëntnummer, locatiegegevens of elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van de natuurlijke persoon.

Als iemand zonder al te veel moeite en met legale middelen een set gegevens kan combineren of koppelen, en daarmee een persoon kan identificeren, dan zijn de betreffende gegevens voor diegene persoonsgegevens. Volgens de AP kunnen gegevens als *anoniem* worden beschouwd als voor welke partij dan ook, met inzet van (voor het beoogde doel) redelijke middelen, het onwaarschijnlijk is dat hieruit personen worden geïdentificeerd (AP 2020). Daarbij dient volgens de AP rekening te worden gehouden met toekomstige situaties en ontwikkelingen die re-identificatie mogelijk zouden kunnen maken (AP 2019). Anonimisering zorgt er dus voor dat, in tegenstelling tot pseudonimisering, gegevens niet meer te herleiden zijn naar individuen. Anonimisering is daarmee onomkeerbaar. Robuust onomkeerbaar anonimiseren is niet eenvoudig. Zelfs de enkele afbeelding van een afgezet been kan in de juiste omstandigheden een persoonsgegeven zijn.¹⁹ Ook datasets zoals *machine learning* training data, waarover meer in paragraaf 2.1, kunnen soms tot personen herleidbare informatie bevatten, door toepassing van technieken zoals *model inversion* (Veale et al. 2018).

Voor de hulpverlener zijn de gegevens in een medisch dossier al snel persoonsgegevens. De hulpverlener kan zelfs ogenschijnlijk anonieme gegevens, zoals een röntgenfoto, relateren aan een persoon op basis van bijvoorbeeld een patiëntnummer. Dit zou ook voor de onderzoeker gelden, naar gelang de dataset die hij ontvangt. In dit rapport gaan we er vanuit dat de onderzoekers (meestal digitale) gegevens ontvangen die geheel of gedeeltelijk persoonsgegevens bevatten. Hierop is dus de AVG van toepassing.

Bijzondere persoonsgegevens

Zoals aangegeven bij de introductie van deze paragraaf, 'verbiedt' de AVG over het algemeen niet het gebruik van persoonsgegevens. Er geldt één belangrijke nuance hierop, te weten: het gebruik van zogeheten 'bijzondere categorieën van persoonsgegevens'. Hieronder vallen **gezondheidsgegevens en genetische gegevens** (zie onderstaand kader). Deze bijzonder gevoelige gegevens verdienen specifieke bescherming, omdat de context van de verwerking significante risico's kan meebrengen voor de fundamentele rechten en vrijheden van de betrokkenen. Het gebruik van deze 'bijzondere gegevens' is verboden, tenzij de wet voorziet in een opheffing van dit verbod. De **verbodsopheffingen** staan genoemd in de AVG

19 NOS, 'Foto geamputeerd been Albanees zonder toestemming op pakjes tabak', 18 juli 2019, <https://nos.nl/artikel/2294033-foto-geamputeerd-been-albanees-zonder-toestemming-op-pakjes-tabak.html>.

en sommige daarvan zijn uitgewerkt in nationale wetgeving, zoals de **Uitvoeringswet AVG (UAVG)**. Zie voor een opsomming hiervan Bijlage 1, Tabel 5.

Kader **Gezondheidsgegevens en genetische gegevens**

Gegevens over gezondheid vallen in de bijzondere categorieën van persoonsgegevens. De term ‘gezondheidsgegevens’ moet breed worden opgevat. Het gaat om alle persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, bijvoorbeeld ziekte of handicap. Hieronder vallen ook gegevens over verleende gezondheidsdiensten, waarmee informatie over de gezondheidstoestand wordt gegeven.²⁰

Het gaat niet alleen om informatie over iemands gezondheidstoestand in het verleden, zoals de medische voorgeschiedenis, en het heden. Het gaat ook om de toekomst. Denk aan informatie over ziekterisico’s. Patiëntnummers of andere cijfers, symbolen of kenmerken die als uniek identificatiemiddel in de gezondheidszorg worden gebruikt, zijn eveneens gezondheidsgegevens. Andere voorbeelden zijn: informatie uit testen of onderzoeken van lichaamsdelen of lichaamseigen stoffen, waaronder genetische gegevens en biologische monsters.²¹

Genetische gegevens vallen – naast gezondheidsgegevens – ook onder de noemer ‘bijzondere categorieën van persoonsgegevens’. Genetische gegevens zijn gegevens die verband houden met iemands overgeërfd of verworven genetische kenmerken en die informatie verschaffen over de fysiologie of de gezondheid van die persoon.²² Bijvoorbeeld informatie uit chromosoomanalyse of een DNA-analyse.²³

20 Artikel 4 lid 15 AVG.

21 Voorbeelden ontleend aan overweging 35 AVG.

22 Artikel 4 lid 15 AVG definieert genetische gegevens als: “persoonsgegevens die verband houden met de overgeërfd of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon.”

23 Overweging 34 AVG.

Aangenomen mag worden dat de informatie die de hulpverlener verzamelt in een medisch dossier (medische geschiedenis, uitslagen, etc.) bijzondere persoonsgegevens zijn.

Voor de toepassing van de **AVG maakt het niet uit wat de bron van de gezondheidsgegevens is geweest**. Gezondheidsinformatie is bijvoorbeeld informatie over de klinische behandeling, of de fysiologische of biomedische staat van de patiënt, ongeacht of deze informatie direct is geregistreerd door de arts of afkomstig is van een medisch hulpmiddel.²⁴ **Gezondheidsgegevens buiten het medisch dossier worden ook beschermd door de AVG**. Denk aan gezondheidsdata gemeten met een bloeddruk-app als onderdeel van *quantified self*. In de hoofdstukken 2 en 4 beschrijven we dat *quantified self*-gegevens echter **niet zomaar worden beschermd door het beroepsgeheim** van de hulpverlener.

Voor hulpverleners en onderzoekers is het van belang te onderkennen dat (niet-gevoelige) persoonsgegevens kunnen **'verkleuren'** naar gezondheidsgegevens. Dat 'verkleuren' gebeurt als ogenschijnlijk niet-gevoelige gegevens worden gekoppeld of gerelateerd aan andere data, waardoor de gezondheidsstatus of gezondheidsrisico's van iemand worden blootgelegd. Bijvoorbeeld de kennis dat een persoon een verhoogd risico heeft op een hartaanval, gebaseerd op de variabiliteit in hartritme gemeten over een bepaalde periode met een biomonitor op de mobiele telefoon. Verkleuring van informatie kan ook optreden als de niet-gevoelige informatie in een bepaalde context wordt gebruikt. Bijvoorbeeld informatie over wanneer iemand naar een door COVID-19 getroffen gebied is gereisd, mede op basis waarvan een hulpverlener een diagnose stelt (EDPB Guidelines 03/2020).

Verhouding (uitvoeringswet) AVG en WGBO

De regels van de **WGBO en de (U)AVG vallen goeddeels samen of vullen elkaar aan**. De verhouding tussen beide wetten kan worden getypeerd als aanvullend, en op enkele punten als afwijkend, zoals weergegeven in Bijlage 2 (Tabel 7). De (U)AVG dient in samenhang te worden gezien met de wettelijke voorschriften in de WGBO over gegevensverstrekking en het medisch beroepsgeheim.²⁵ Zo is het denkbaar dat de (U)AVG een bepaald gebruik van persoonsgegevens door bijvoorbeeld een onderzoeker toestaat, maar dat het beoogde gegevensgebruik alsnog geen doorgang kan vinden vanwege het medisch beroepsgeheim van de hulpverlener.

Daarom moet het beoogde gebruik van gezondheidsgegevens **eerst worden getoetst aan de regels voor doorbreking van het medisch beroepsgeheim**. Blijkt hieruit dat de verstrekking van gezondheidsgegevens niet in strijd is met het

24 Voorbeelden ontleend aan overweging 35 AVG.

25 Memorie van Toelichting Uitvoeringswet AVG, p. 95.

beroepsgeheim, dan kan vervolgens worden getoetst aan de voorwaarden van de (U)AVG. Hoofdstuk 3 beschrijft hoe die toets kan plaatsvinden.

1.3.2 Eerbiediging van het privéleven

Artikel 8 van het EVRM bepaalt dat iedereen recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Het EU-Grondrechtenhandvest bevat een vergelijkbare bepaling.²⁶ Dit **recht op bescherming van het privéleven** – ook wel de **persoonlijke levenssfeer** genoemd – is breed. Het wordt ook wel ‘privacy-recht’ genoemd. Het hoeft niet om persoonsgegevens te gaan. Zo kan een patiënt in zijn privacy worden aangetast als hij zonder toestemming wordt geobserveerd door co-assistenten. Telefoongesprekken en videoregistraties vallen ook onder de bescherming, ongeacht of hiermee persoonsgegevens worden verwerkt. Het afnemen en bewaren van DNA-gegevens en vingerafdrukken vallen ook onder het recht op eerbiediging van het privéleven.

Hoewel het privacy-recht **niet specifiek is gericht op de bescherming van persoonsgegevens**, kan het informatie zoals medische gegevens wel beschermen (ECrHR 2015, Hoofdstuk VII, B).²⁷

De **WGBO** noemt enkele malen de ‘**persoonlijke levenssfeer**’. Zo blijft inzage aan de patiënt in het eigen medisch dossier achterwege voor zover dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander, bijvoorbeeld als het over biologisch ouderschap gaat.²⁸ Dit geldt ook als gegevensverstrekking uit het dossier zou plaatsvinden op basis van toestemming van de patiënt.²⁹ De persoonlijke levenssfeer dient ook in acht te worden genomen als gegevensverstrekking of inzage in het dossier plaatsvindt vanwege statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid.³⁰ Hoofdstuk 3 zet uiteen hoe deze eis in de praktijk kan worden ingevuld, bijvoorbeeld door anonimisering of het coderen van de gegevens uit het medisch dossier. In al deze gevallen dient stil te worden gestaan bij het recht op eerbiediging van het privéleven, waarbij persoonsgegevens een rol kunnen spelen.

26 Artikel 7 van dit Handvest luidt: “Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.”

27 Het Straatsburgse Mensenrechtshof (EHRM) dat beslist over EVRM-zaken heeft nooit een algemeen recht op de bescherming van privégegevens erkend. Wel erkent het EHRM dat de bescherming van persoonsgegevens, waaronder medische informatie, van fundamenteel belang is om de bescherming van artikel 8 EVRM te kunnen genieten.

28 Artikel 7:456 BW.

29 Artikel 7:457 lid 1 BW. Dit geldt ook voor dossiers van overleden patiënten. Zie artikel 7:458a lid 4 BW.

30 Dergelijk onderzoek mag alleen worden uitgevoerd op een manier waarop de persoonlijke levenssfeer van de patiënt niet onevenredig wordt geschaad. Artikel 7:458 lid 1 sub a BW.

Voorwaarden waaronder rechten beperkt mogen worden

Het recht op eerbiediging van het privéleven en de bescherming van persoonsgegevens hebben met elkaar gemeen, dat ze **niet absoluut** zijn. Dat wil zeggen dat deze rechten **onder voorwaarden beperkt mogen worden**. Als landen bijvoorbeeld wetgeving willen opstellen waarin de vertrouwelijkheid van medische informatie in het geding is, zoals een wettelijke plicht voor de arts om gegevens te verstrekken aan derden, dan moet die wet voldoen aan de voorwaarden die artikel 8 EVRM daaraan stelt. Dit betekent onder meer dat de wet in overeenstemming moet zijn met de eisen van **proportionaliteit** ('staat de beoogde inbreuk in verhouding tot het te dienen doel van de wet?') en **subsidiariteit** ('kan de inbreuk op het fundamentele recht op een minder ingrijpende manier plaatsvinden?'). De betreffende wet moet daarnaast **noodzakelijk** zijn in een democratische samenleving. Bijvoorbeeld omdat de wet het belang dient van de patiënt, of nodig is voor de veiligheid van ziekenhuispersoneel (ECrHR 2019, alinea 179).

Een wet die erop gericht is om het beroepsgeheim te doorbreken, moet dus aan kwaliteitseisen voldoen, waarbij de **belangenafwegingen kunnen verschillen per wetsvoorstel**. Het belang om de vertrouwelijkheid te blijven waarborgen, weegt bijvoorbeeld extra zwaar als het gaat om medische informatie waarvan de openbaarmaking ervan verstrekende gevolgen kan hebben. Denk aan de onthulling van HIV-informatie. Dit kan vergaande gevolgen hebben voor het privé- en familieleven van de betreffende persoon en voor zijn of haar sociale en professionele situatie. Bijvoorbeeld vanwege risico's op stigmatisering en sociale uitsluiting als deze informatie bekend raakt (ECrHR 2019, alinea 179). Het is aan de wetgever en het parlement de afweging te maken tussen de rechten van patiënten en onderzoekers, tegen de achtergrond van het publieke gezondheidsbelang.

Andere in het recht beschermde belangen die soms zwaarder kunnen wegen dan het beroepsgeheim, zijn de persvrijheid, volksgezondheid en het belang van het publieke debat, de waarheidsvinding in het strafproces (Buijsen et al. 2012). **Het recht op de vrijheid van informatiegaring en wetenschapsvrijheid** van onderzoekers is ook zo'n belang (zie paragraaf 1.3.3).

Het Straatsburgse Mensenrechtenhof heeft overigens erkend dat **het gebruik van persoonlijke informatie op basis van toestemming een 'legitiem doel'** is in de zin van artikel 8 EVRM, mits de informatie wordt gebruikt overeenkomstig de verleende toestemming. Dus **naast een wet kan ook de toestemming van een patiënt legitimeren dat de geheimhouding wordt doorbroken**. In Nederland is dat geregeld in de WGBO.

1.3.3 Recht op vrijheid van informatiegaring en wetenschapsvrijheid

In de voorgaande paragrafen hebben we gezien dat betrokkenen, zoals patiënten, fundamentele rechten genieten met betrekking tot eerbiediging van het privé-leven en gegevensbeschermingsrecht. We hebben ook gezien, dat deze rechten onder voorwaarden beperkt kunnen worden door rechten die soms zwaarder kunnen wegen. Bijvoorbeeld vanwege het recht op de vrijheid van meningsuiting en van informatie, dat de vrijheid omvat kennis te nemen en te geven van informatie of ideeën, zonder inmenging van enig openbaar gezag en ongeacht grenzen.³¹ Of in verband met de erkenning dat wetenschappelijk onderzoek vrij moet zijn, waarbij de academische vrijheid dient te worden geëerbiedigd.³² We duiden deze rechten kortweg aan als '**wetenschapsvrijheid**'.

De literatuur onderscheidt **drie elementen van de wetenschapsvrijheid**: studievrijheid, onderzoeksvrijheid en openbaarmakingsvrijheid (Ploem 2004). Daarbij is in bijvoorbeeld nWMO-onderzoek de wetenschapsvrijheid alleen van betekenis als een gegevensverwerking tot doel heeft een bijdrage te leveren aan het algemeen belang, door vermeerdering van wetenschappelijke kennis (Ploem 2004).

De wetenschapsvrijheid heeft te maken met het belang van het kunnen gebruiken van (medische) gegevens voor wetenschappelijk onderzoek (Ploem 2004). Zulk onderzoek dient de technische en wetenschappelijke vooruitgang binnen de samenleving en uiteindelijk de volksgezondheid. De AVG-wetgever erkent bijvoorbeeld dat onderzoekers door gegevenskoppeling waardevolle kennis kunnen verwerven over veel voorkomende medische aandoeningen, zoals hart- en vaatziekten, kanker en depressie.³³

Omdat de wetenschapsvrijheid evenmin een absoluut karakter heeft, kan ook zij beperkt worden vanwege andere rechten en belangen, waaronder die van patiënten. Er vindt dus een belangenafweging plaats tussen de conflicterende rechten. De WGBO-wetgever heeft die afweging in de jaren '90 gemaakt bij het opstellen van de voorschriften voor gegevensverstrekking voor onderzoek en statistiek (hoofdstuk 3).

31 Artikel 11 lid 1 EU-Grondrechtenhandvest.

32 Artikel 13 EU-Grondrechtenhandvest.

33 Overweging 157 AVG.

1.4 Tot slot

Wetenschappelijk onderzoek is noodzakelijk voor de ontwikkeling van de geneeskunde en de gezondheidszorg. Voor zulke onderzoeken wordt regelmatig gebruik gemaakt van gegevens uit medische dossiers. Dat heet nWMO-onderzoek. De privacybelangen van de patiënt, vervat in het recht op eerbiediging van zijn privéleven en de bescherming van persoonsgegevens, zijn mogelijk in het geding, met name als de onderzoeksgegevens herleidbaar zijn tot de patiënt. De wetgever heeft middels de WGBO, AVG en UAVG getracht de juiste afwegingen te maken tussen de belangen van het wetenschappelijk onderzoek en statistiek enerzijds en het belang van de bescherming van persoonsgegevens en de persoonlijke levenssfeer anderzijds. In het volgende hoofdstuk schetsen we een aantal technologische ontwikkelingen die interessante gegevens en medische mogelijkheden bieden, maar tegelijkertijd de wetgeving uitdagen.

2 Technologie daagt wetgeving uit bij nWMO-onderzoek

In hoofdstuk 1 zijn de belangrijkste juridische kaders uiteengezet die relevant zijn bij het beschikbaar maken van data uit medische dossiers en het gebruiken daarvan door onderzoekers ten behoeve van statistisch of wetenschappelijk onderzoek. Dit wordt samengevat als nWMO-onderzoek. Het hoofdstuk gaf een uitleg van onderliggende rechten, de manier waarop de verschillende wetten zich tot elkaar verhouden, voorwaarden waaronder uitzonderingen kunnen worden gemaakt en de afweging van belangen daarbij.

Hoofdstuk 2 omvat drie casussen die schetsen dat er door allerlei nieuwe (digitale) ontwikkelingen in het medische domein extra uitdagingen zijn voor het juridisch toetsen bij het gebruik van gegevens uit medische dossiers ten behoeve van nWMO-onderzoek. Deze voorbeelden laten zien dat data steeds vaker op andere manieren worden verzameld dan door de hulpverlener, bijvoorbeeld door de patiënt zelf met behulp van sensoren en apps. Of er worden gegevens verzameld in het kader van internationale wetenschappelijke samenwerkingen, of met data-verwerkende bedrijven (vaak de aanbieders van health apps of meetapparatuur). Daarnaast wordt het steeds lastiger om de grens tussen 'algemeen belang' en 'commercieel belang' vast te stellen als er commerciële partijen een rol hebben, zoals bij ontwikkelingen gebaseerd op AI. Private partijen kunnen met hun technologie belangrijke bijdragen leveren in de publieke sector, maar moeten ook geld verdienen om te kunnen bestaan. Bij iedere casus worden kansen en belangenafwegingen geschetst voor de gezondheid van de patiënt tegen de achtergrond van de kansen voor de volksgezondheid. Ook worden juridische uitdagingen bij nWMO-onderzoek alvast geïllustreerd. In hoofdstuk 3 komen we daar in detail op terug.

2.1 Casus 1: machine learning

Tegenwoordig zijn medisch dossiers veelal digitaal beschikbaar. Hiermee worden de daarin opgenomen patiëntdata technisch steeds gemakkelijker ontsloten en toegankelijk gemaakt voor anderen dan de hulpverlener. Dit biedt allerlei technische mogelijkheden voor onderzoek en computergestuurde diagnostiek. Bijvoorbeeld met behulp van kunstmatige intelligentie (*artificial intelligence*, AI) waaronder *machine learning*.

Hulpverleners en onderzoekers, ook van bedrijven, proberen door middel van software de dossiers elektronisch te doorzoeken en te analyseren. Bijvoorbeeld met betrekking tot behandelingen van ernstige bloedvergiftiging. Met algoritmen wordt vervolgens onderzocht wat de beste behandeling is voor de patiënt, door gegevens te gebruiken van patiënten met dezelfde aandoening die eerder zijn behandeld. Zoals historische informatie over het gebruik van dosering en antibiotica, hoe de patiënten daarop reageerden en wat de uitkomst van de behandelingen was.³⁴ Daarnaast wordt bijvoorbeeld beeldherkenning toegepast om foto's te analyseren met de bedoeling om tumoren te herkennen. Naar verluidt is een door Google ontwikkeld algoritme meer succesvol in het herkennen van ziektes dan een patholoog.³⁵ In Amerika wordt *machine learning* toegepast bij de ontwikkeling van software dat repetitief en herhaalbaar werk verricht, zodat radiologen meer tijd vrij hebben om zich te richten op niet-repliceerbaar werk in de laatste diagnosefase en bijzondere gevallen.³⁶ In Groningen onderzoekt men de mogelijkheden om op basis van *big data* en *AI* een model te ontwikkelen dat voorspelt welke kinderen een verhoogd risico hebben op astma.³⁷

Het gaat telkens om het gebruik van gegevens die routinematig worden vastgelegd en hergebruikt worden voor onderzoek. Op de Intensive Care worden bijvoorbeeld vitale functies van patiënten gemonitord en geregistreerd, dat neerkomt op ongeveer 30.000 datapunten per dag. Een datapunt is een waarde van een lichaamsfunctie op een bepaald moment van een bepaalde patiënt.³⁸ Voor een onderzoek stelt het Amsterdam UMC 1 miljard datapunten beschikbaar, voornamelijk uit bewakingsapparatuur van ongeveer 20.000 patiënten maar ook medicatiegegevens.³⁹ De gegevens staan in de database AmsterdamUMCdb genaamd, een afgeschermd portal van het online archiveringssysteem DANS.⁴⁰ Het is de bedoeling dat artsen en wetenschappers vanuit de hele wereld met deze *big data* algoritmes ontwikkelen met *AI*-technieken als *machine learning*.

34 NOS Nieuws, 'Big data in de zorg, hoe werkt dat?', 31 augustus 2016, <https://nos.nl/artikel/2129192-big-data-in-de-zorg-hoe-werkt-dat.html>.

35 NOS Nieuws, 'Computer kan kanker beter herkennen dan patholoog,' 3 maart 2017, <https://nos.nl/artikel/2161091-computer-kan-kanker-beter-herkennen-dan-patholoog.html>.

36 TechCrunch, 'FDA-cleared AI-based medical triage tool goes free for customers to help busy radiology diagnostics departments', 30 april 2020, <https://techcrunch.com/2020/04/30/fda-cleared-ai-based-medical-triage-tool-goes-free-to-help-busy-radiology-diagnostics-departments/>.

37 NOS Nieuws, 'Gronings ziekenhuis zet big data in tegen astma', 20 juni 2019, <https://nos.nl/artikel/2289836-gronings-ziekenhuis-zet-big-data-in-tegen-astma.html>.

38 SmartHealth, 'Algoritme adviseert intensivist: samenwerking Pacmed en Amsterdam UMC, 25 juli 2019, <https://www.smarthealth.nl/2019/07/25/algoritme-adviseert-intensivist-samenwerking-pacmed-en-amsterdam-umc/>.

39 Amsterdam UMC, Locatie AMC, 'Amsterdam UMC stelt gegevens over IC-patiënten beschikbaar om levens te redden', 17 november 2019, <https://www.amc.nl/web/nieuws-en-verhalen/actueel/actueel/amsterdam-umc-stelt-gegevens-over-ic-patienten-beschikbaar-om-levens-te-redden.htm>.

40 Een instituut voor digitale onderzoeksgegevens van Koninklijke Nederlandse Akademie van Wetenschappen (KNAW) en Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO). Meer informatie: www.amsterdammedicaldatascience.nl.

Meer recent creëerden Nederlandse ziekenhuizen een database met gegevens van coronapatiënten.⁴¹ Dit wordt gecoördineerd door Amsterdam UMC, de Vrije Universiteit Amsterdam en het Maastricht UMC+. De bedoeling is om coronapatiënten sneller en effectiever te kunnen behandelen. De datapunten voortvloeiend uit de IC-behandeling, zoals data over hartslag, toegediende zuurstof, klachten van de patiënt en behandeling, worden verzameld via het elektronisch patiëntdossier dat individuele ziekenhuizen van patiënten bijhouden. De ziekenhuizen anonimiseren deze gegevens en brengen de informatie samen in de database. Vervolgens wordt *machine learning* toegepast. Zo kan worden nagegaan welke patiënt- en behandelingskarakteristieken het meest bepalend zijn voor succesvolle behandeling en kan worden getracht het ziekteverloop te voorspellen. Het doel hiervan is tevens om beter in te schatten welke behandelingen en welke zorgcapaciteit er nodig zijn.

De database met informatie afkomstig van coronapatiënten, is aangelegd zonder toestemming van de patiënt. In reactie op het initiatief gaf de AP aan dat toestemming van de patiënt in principe nodig is, maar dat dit anders ligt, als dit niet mogelijk is of niet van de arts kan worden verlangd, gelet op de huidige omstandigheden. Dit laatste is volgens UMC Amsterdam de reden dat geen toestemming hoeft te worden gevraagd: "Patiënten zijn vaak te ziek zijn om toestemming te verlenen en we willen de behandelaars, patiënten en hun dierbaren niet nog meer te belasten".⁴² Daarbij kunnen desgewenst patiënten bezwaar maken bij hun ziekenhuis, bijvoorbeeld door het sturen van een e-mailbericht.⁴³ De gegevens worden dan niet gebruikt voor het onderzoek.

In hoofdstuk 3 zetten we in detail uiteen wanneer toestemming nodig is en wanneer het bezwaar van patiënten van toepassing is.

2.2 Casus 2: quantified self

De hulpverlener, zoals de huisarts of ziekenhuis, en onderzoekers zijn geenszins de enige partijen die gezondheidsgegevens verzamelen of analyseren. **Het individu, als gezond persoon of patiënt, is eveneens een dataverzamelaar.** Als onderdeel van trends als *quantified self* meten mensen steeds vaker zichzelf met

41 Nu.nl, 'Nederlandse ziekenhuizen creëren database met gegevens coronapatiënten', 25 maart 2020, <https://www.nu.nl/tech/6040223/nederlandse-ziekenhuizen-creeren-database-met-gegevens-coronapatienten.html>.

42 Nu.nl, 'Nederlandse ziekenhuizen creëren database met gegevens coronapatiënten', 25 maart 2020, <https://www.nu.nl/tech/6040223/nederlandse-ziekenhuizen-creeren-database-met-gegevens-coronapatienten.html>.

43 Maastricht UMC+, 'Kunstmatige intelligentie moet helpen in de strijd tegen het coronavirus', 24 maart 2020, <https://www.mumc.nl/actueel/nieuws/kunstmatige-intelligentie-moet-helpen-de-strijd-tegen-het-coronavirus>.

het oog op hun gezondheid. Bijvoorbeeld via een *fitness tracker* die je conditie-ontwikkelingen bijhoudt of een slimme weegschaal die je gewicht, vet- en vochtpercentage en spiermassa meet en via een app informatie met de gebruiker deelt. Deze metingen worden buiten het domein van de hulpverlener verricht en vinden plaats in de relatie consument-bedrijfsleven, waarbij het bedrijfsleven bestaat uit de aanbieder van het meetinstrument inclusief eventuele partners zoals advertentiefirma's of databedrijven. Dat dit interessante gegevens zijn, blijkt bijvoorbeeld uit het feit dat Fitbit claimde op basis van gegevens over hartslag en ademsnelheid van gebruikers een besmetting met COVID-19 te kunnen voorspellen.⁴⁴

Een ander voorbeeld van gegevensverzameling **buiten het medisch domein** betreft het Amsterdamse Happitech dat de *Heart for Heart*- app aanbiedt. Hiermee verstrekt de app-gebruiker gegevens over zijn of haar hartritme. De gegevens worden geregistreerd doordat de app-gebruiker zijn vinger op de lens van de telefooncamera legt. De camera detecteert beweging van het bloed en meet zodoende de hartslag.⁴⁵ De verzamelde gegevens worden gebruikt om inzicht te verkrijgen in oorzaken van bepaalde vormen van hart- en vaatziekten en het ziektebeloop. Hulpverleners valideren de gegevens.⁴⁶ Op deze manier 'doneren' de app-gebruikers hun data ten behoeve van hartonderzoek.

Er zijn meerdere manieren waarop metingen van patiënten met *quantified self*-instrumenten worden gebruikt **in het medisch domein**. Zo worden de instrumenten actief aangeboden door bedrijven, al dan niet in samenwerking met hulpverleners. Patiënten, maar ook gezonde personen, kunnen dan vrijwillig en op eigen initiatief deelnemen aan het onderzoek door de data ter beschikking te stellen aan het onderzoek. Illustratief is de genoemde Heart for Heart-app, maar een ander voorbeeld is dat van de Radboud Universiteit in samenwerking met het Radboudumc.⁴⁷ Deze onderzoekers en hulpverleners bieden een speciaal horloge aan. Dit horloge, afkomstig van Google's zusterbedrijf Verily, maakt tijdens de dagelijkse activiteiten van de patiënt metingen van de elektriciteit van de hersenen (eeg's) en van de hartspier (ecg's). De meetgegevens worden gebruikt voor een wereldwijd onderzoek naar de ziekte van Parkinson. Patiënten moeten voor elk nieuw onderzoek opnieuw toestemming geven voor het gebruik van hun gegevens. Ze kunnen zelf bepalen welke onderzoekers toegang krijgen. Dit kunnen ook

44 <https://blog.fitbit.com/early-findings-covid-19-study/>.

45 NOS Nieuws, 'Data in plaats van geld doneren voor hartonderzoek', 12 juni 2017, <https://nos.nl/artikel/2177797-data-in-plaats-van-geld-doneren-voor-hartonderzoek.html>.

46 SmartHealth, 'HeartForHeart: onderzoek boezemfibrilleren via app en crowdfunding', 12 juni 2017, <https://www.smarthealth.nl/2017/06/12/heartforheart-happitech-crowdfunding-data/>.

47 NOS Nieuws, 'Big data-onderzoek naar Parkinson, met respect voor privacy', 30 september 2016, <https://nos.nl/artikel/2135155-big-data-onderzoek-naar-parkinson-met-respect-voor-privacy.html>.

internationale onderzoekers zijn. Na de toestemming ontvangt de betreffende onderzoeker een digitale sleutel waarmee de data kunnen worden ingezien.

Een andere manier waarop *quantified self*-data in het medisch dossier (en later in het onderzoek) terechtkomen, is als de metingen worden verricht op aanraden van de hulpverlener of buiten de behandelrelatie om. In het eerste geval vraagt de hulpverlener de patiënt bijvoorbeeld om een 'slaap-app' te gebruiken om na te gaan of er sprake is van slaapapneu. De app wordt aangeboden in de app-stores, soms zonder dat hulpverleners betrokken zijn geweest bij de totstandkoming ervan. In het tweede geval zijn de data reeds verzameld, omdat de patiënt de metingen uitvoerde vóórdát een behandelrelatie tot stand kwam. Bijvoorbeeld informatie over de dagelijkse lichaamsbeweging. De patiënt brengt de gemeten data in op verzoek van de hulpverlener, *nadat* de behandelrelatie is gestart.

De *quantified self*-data kunnen ook **buiten het medisch dossier** blijven. Bijvoorbeeld als de hulpverlener geen kopie ontvangt van de data in het dossier, maar de gemeten resultaten van de app bespreekt met de patiënt. Deze inlichtingen vallen waarschijnlijk wel onder het beroepsgeheim (lees: de zwijgplicht en het verschoningsrecht van de hulpverlener), maar voor de onderliggende app-data is dit niet vanzelfsprekend. Zijn de app-gegevens persoonsgegevens, dan worden deze 'slechts' beschermd door de (U)AVG.

2.3 Casus 3: digitale portalen

Naast *machine learning* en *quantified self* zijn er ook **digitale portalen**. Digitale portalen geven patiënten de mogelijkheid om op afstand zorg te ontvangen. De portalen zijn in opkomst, mede doordat de COVID-19 crisis persoonlijk contact tussen arts en patiënt bemoeilijkt (Spoelsta 2020).

Digitale portalen bieden patiënten een online platform, waarmee ze kunnen **informer**, **communiceren** en **monitoren**. Wanneer nodig, kan de hulpverlener interveniëren. Informeren kan bijvoorbeeld via een online bibliotheek. Via technieken als videobellen kan de patiënt communiceren met een hulpverlener. Het e-consult via videobellen zit sinds de coronacrisis enorm in de lift en grote tech-bedrijven bundelen hierbij hun krachten. Zo hebben Google Cloud en e-health leverancier Amwell onlangs een samenwerkingsovereenkomst gesloten. Amwell zal de videodiensten voor patiënten onderbrengen in de cloud van Google.⁴⁸ Daarnaast bieden portalen patiënten de mogelijkheid hun stemming, gedachten, gedrag, en

48 <https://www.icthealth.nl/nieuws/google-cloud-investeert-100-miljoen-in-e-health-platform/>

lichamelijke gesteldheid te monitoren en te delen met de hulpverlener. Dat kan bijvoorbeeld via een chatfunctie. Verder kunnen patiënten via portalen interventies aangeboden krijgen, zoals psychologische therapeutische interventies. Zodra de digitale behandeling (via filmpjes en online opdrachten) gekoppeld wordt aan een ondersteunende fysieke behandeling, dan heet dit *blended care*. *Blended care* is daarmee een combinatie van online en face-to-face behandeling (Rathenau Instituut 2019a).

Digitale portalen passen binnen de trend die **datagedreven gezondheidszorg** wordt genoemd. Dit, omdat het gebruik van het portaal zorgaanbieders belangrijke informatie oplevert om patiënten zo goed mogelijk te behandelen.

De portalen bieden, net als *quantified-self*, nieuwe databronnen voor hulpverlening en onderzoek. Zo worden via de portalen allerlei gegevens verzameld die nieuw zijn ten opzichte van de gegevensregistratie in een traditionele zorgcontext. Bijvoorbeeld de inhoud van gesprekken die zijn gevoerd via de chat-optie, maar ook gegevens over de frequentie van het gebruik van het portal door de patiënt. Deze informatie wordt ter evaluatie aan de hulpverleners teruggekoppeld, zodat zij inzicht verkrijgen in hoe, wanneer en aan wie het portal aangeboden kan worden (Rathenau Instituut 2019). Ook onderzoekers zouden deze data mogelijk willen gebruiken voor nWMO-onderzoek.

2.4 Tot slot

De drie casussen laten zien, dat technologische ontwikkelingen leiden tot andere, nieuwe manieren van medische data verzamelen en gebruiken. Sommige onderzoekers, patiënten en hulpverleners zijn voorlopers als het gaat om gebruik van deze technologie. In het volgende hoofdstuk gaan we na hoe de WGBO-voorschriften over medisch data-onderzoek toegepast kunnen worden op onder meer technologische ontwikkelingen als AI, *quantified self* en digitale portalen.

3 Gids langs bepalingen voor gebruik van medische data

In hoofdstuk 1 is reeds aangekondigd dat zowel hulpverleners als onderzoekers rekening moeten houden met de wettelijke bepalingen over gebruik van gegevens uit medische dossiers voor nWMO-onderzoek. Dit hoofdstuk zal hen langs de belangrijkste bepalingen leiden. Paragraaf 3.1 is geschreven voor de hulpverlener. Hij kan met behulp van de tekst en een stroomdiagram (zie Bijlage 4) voor de hulpverlener beoordelen of de gevraagde gegevensverstrekking, c.q. inzage in de medische dossiers, mag plaatsvinden. Als dat het geval is, verschuift de verantwoordelijkheid voor een zorgvuldige omgang met de gegevens naar de onderzoeker. Paragraaf 3.2 beschrijft waaraan de onderzoeker moet voldoen bij het gebruik van de gegevens uit de medische dossiers. Ook hij kan dit doen aan de hand van de tekst en een stroomdiagram, speciaal voor de onderzoeker (zie Bijlage 5).

Alvorens de hulpverlener nagaat of de gegevens verstrekt mogen worden, dient hij eerst te controleren of het inderdaad om nWMO-onderzoek gaat en niet om onderzoek waarvoor specifieke andere regels gelden, zoals de WMO. Zie hiervoor het tekstkader in de inleiding van dit rapport. Daarnaast kunnen de Telecommunicatiewet en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg van toepassing zijn. Zie het tekstkader in paragraaf 3.1.1.

3.1 Verstrekking van gegevens uit behandelrelatie

Wanneer een hulpverlener een verzoek krijgt van een onderzoeker om gegevens uit het medisch dossier te verstrekken, speelt direct het medisch beroepsgeheim een rol (zie paragraaf 1.2). Vrijwel alle informatie uit het medisch dossier valt onder het medisch beroepsgeheim. Het is de informatie van (of over) de patiënt waarvan de hulpverlener kennisneemt bij het uitoefenen van zijn of haar beroep. De hulpverlener ontvangt of registreert zulke informatie in het kader van de behandelrelatie met de patiënt. Dit werd uitgelegd in paragraaf 1.1.

Kader **Beschermd door het beroepsgeheim?**

Quantified self-data doen diverse vragen rijzen. Het is voor de patiënt bijvoorbeeld lang niet altijd duidelijk of, en zo ja wanneer, de data onder het medisch beroepsgeheim van een hulpverlener vallen. De data van de Heart for Heart-app (paragraaf 2.2) worden gebruikt door diverse onderzoekers en ziekenhuizen, verspreid over de hele wereld. Welke hulpverlener geldt als de aangewezen persoon die de ingebrachte data beheert in het kader van de dossierplicht? Is dit een Nederlandse hulpverlener waarop de WGBO van toepassing is? Of ontstaat er een directe relatie tussen de app-gebruiker en de onderzoekers, zodat de data in het geheel niet worden beschermd door het beroepsgeheim? Vanuit het perspectief van de patiënt zijn dit soort zaken moeilijk te doorgronden, zeker als hierover niet helder wordt gecommuniceerd (ICO 2018). Dit staat op gespannen voet met de eisen over informatievoorziening uit de WGBO en de AVG.

Vergelijkbare vragen rijzen bij het gebruik van digitale portalen (paragraaf 2.3). Als de gegevensverzameling gebeurt in het kader van het behandeltraject, dan vallen deze gegevens onder het beroepsgeheim. Geldt dat ook voor informatie over het gebruik van het portal? Zulke informatie geeft misschien prijs welke therapieën iemand volgt.⁴⁹ Ook zou een hulpverlener gebruiksgegevens kunnen inzetten voor het vaststellen van een diagnose, zoals informatie over hoe snel (of hoe langzaam) de patiënt een vragenlijst invult. Mag de patiënt verwachten dat die data worden beschermd als onderdeel van het medisch dossier? Als de antwoorden hierop “ja” zijn, dan is het logisch de data te behandelen als gegevens beschermd onder het medisch beroepsgeheim.

Zijn de gegevens over de patiënt *niet* verzameld in het kader van de behandelrelatie en is er geen beroepsgeheim van toepassing, dan kunnen de AVG en de UAVG van toepassing zijn op de handelingen met de gegevens, als deze te kwalificeren zijn als *persoonsgegevens*. Hetzelfde geldt als de hulpverlener de gegevens in herleidbare vorm heeft verstrekt aan de onderzoekers. Zij moeten dan

⁴⁹ Zie ook: Autoriteit Persoonsgegevens, ‘ziekenhuiswebsites volgen in strijd met wet bezoekers via cookies’, 23 juni 2016, <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-ziekenhuiswebsites-volgen-strijd-met-wet-bezoekers-cookies>.

rekening houden met de AVG en Uitvoeringswet AVG, maar de (kopieën van de verstrekte) gegevens zijn dan niet (meer) beschermd door een medisch beroepsgeheim. Zijn de gegevens niet beschermd door het beroepsgeheim of zijn ze reeds – conform de WGBO zoals uiteengezet in deze paragraaf – verstrekt, ga dan naar paragraaf 3.2.

3.1.1 Hoofregel: toestemming vragen

Is eenmaal vastgesteld dat de gegevens voor het medische data-onderzoek beschermd worden door het beroepsgeheim, dan geldt de WGBO. De WGBO kent de volgende hoofregel: de hulpverlener moet ervoor zorgen dat er aan anderen (dan de patiënt) geen inlichtingen over de patiënt worden verstrekt – c.q. inzage in het medisch dossier of een kopie van de gegevens daaruit – **behalve mét toestemming van de patiënt**. De term ‘anderen’ gaat *niet* over hulpverleners uit hetzelfde behandelteam (als dit nodig is voor hun werkzaamheden) en de wettelijk vertegenwoordigers van de patiënt, zoals de ouders en/of voogd van (minderjarige) patiënten of andere wettelijk vertegenwoordigers, zoals de curator van de patiënt. Deze personen mogen zonder toestemming informatie over de patiënt ontvangen. De groep is niet breder.

Collega’s van de hulpverlener, bijvoorbeeld van andere afdelingen binnen hetzelfde ziekenhuis, die *niet* betrokken zijn bij de behandeling, zijn ‘anderen’. Zij mogen dus niet zomaar gegevens ontvangen. Onderzoekers, onderzoeksinstellingen of andere partijen die data uit medische dossiers willen analyseren, vallen ook onder de noemer ‘anderen’. Als zij – net als alle andere ‘anderen’ – inzage willen of een kopie van de gegevens uit het medisch dossier, **dan moet hiervoor in principe de toestemming van de patiënt worden gevraagd. In principe, omdat dit soms niet hoeft voor statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid**. Zie hierover paragraaf 3.1.2.

Overigens hoeft voor *eigen onderzoek* van de hulpverlener geen toestemming te worden gevraagd.⁵⁰ Dit gegevensgebruik wordt niet als een schending van beroepsgeheim opgevat (Ploem 2004). Hetzelfde geldt als de hulpverlener eigen statistieken opstelt (WP131, 2007). Hiermee is overigens niet gezegd dat eigen onderzoek altijd is toegestaan, omdat het eigen onderzoek niet mag conflicteren met de zorg die een goed hulpverlener betaamt.⁵¹ Bovendien moet het gaan om de

50 Tweede Kamer, vergaderjaar 1989-1990, 21 561, nr. 3, *Memorie van Toelichting WGBO*, p. 16. Tweede Kamer, vergaderjaar 1991-1992, 21 561, nr. 11, *Nadere Memorie van Antwoord WGBO*, p. 24. Zie ook Raad van Europa Aanbeveling Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics (vervangen door Aanbeveling No. R(97)18 concerning the protection of personal data collected and processed for statistical purposes).

51 *Nadere Memorie van Antwoord WGBO*, p. 25. Tweede Kamer, vergaderjaar 1990-1991, 21 561, nr. 6, *Memorie van Antwoord WGBO*, pp. 43 – 44.

behandeld hulpverlener(s) en niet om 'anderen', zoals collega's van een huisartsenpraktijk. In haar proefschrift stelt Ploem dat een nadere wettelijke regeling over 'eigen onderzoek' gewenst is, onder meer omdat de privacybelangen van de patiënt in het geding kunnen zijn. Van een nadere wettelijke regeling is het nooit gekomen (2004).

Volgens de WGBO-wetgever moet de toestemming in ieder geval **expliciet en voldoende specifiek** zijn. Daarbij is het niet verplicht om schriftelijke toestemming te verlangen of om toestemming te vragen in de vorm van een handtekening. Bij zorgevaluatieonderzoek en bij onderzoek in de sociale- en gedragswetenschappen is dit volgens onderzoekers zelfs niet de best passende manier. Zo kan bij gevoelig psychologisch onderzoek toestemming leiden tot selectiebias (Ministerie VWS 2020a). Daarnaast behoort de patiënt minimaal te worden geïnformeerd over de aard, de inhoud en het doel van het onderzoek, het belang ervan en de te verwachten duur van het onderzoek (Ploem 2006). Deze informatie kan worden uitgebreid met bijzondere aspecten van het onderzoek, zoals het karakter ervan (bijvoorbeeld erfelijkheidsonderzoek), of de schaal waarop het plaatsvindt (landelijk of internationaal). Met betrekking tot internationaal onderzoek: zie ook paragraaf 3.3. Het gaat er telkens om wat de patiënt in redelijkheid mag verwachten als hij toestemming geeft voor wetenschappelijk onderzoek.⁵² De patiënt moet daarbij met een redelijke mate van nauwkeurigheid kunnen overzien waartoe zijn toestemming strekt.

Als niet vooraf een alomvattende toestemmingsvraag geformuleerd kan worden, dan verwacht het Europees Comité voor gegevensbescherming (*European Data Protection Board* - EDPB) dat er **per onderzoeksfase** om toestemming wordt gevraagd. De EDPB benadrukt allereerst dat wetenschappelijke onderzoeksprojecten alleen persoonsgegevens mogen gebruiken op basis van een specifieke doelomschrijving. Alleen als de doelen niet van meet af aan gespecificeerd kunnen worden, mag een meer algemene doelomschrijving gebruikt worden, aldus de EDPB in haar *Guidelines* over toestemming onder de AVG (EDPB Guidelines 05/2020). Dit impliceert dat een brede toestemming zou zijn toegestaan. Echter, zo vervolgt de EDPB, als de onderzoeksdoeleinden niet volledig gespecificeerd kunnen worden, dan moet de verwerkingsverantwoordelijke (lees: meestal de onderzoeker of onderzoeksinstelling) zoeken naar manieren om te voldoen aan de essentie van de AVG-toestemmingseisen (zie Bijlage 3). Bijvoorbeeld door van de betrokkene (patiënt) toestemming te vragen voor het onderzoek in algemene termen én specifiek voor projectfases die reeds bekend zijn bij de onderzoeker.

52 Tweede Kamer, vergaderjaar 1992-1993, 21 561, nr. 15, *Nota n.a.v. het Eindverslag WGBO*, p. 9 en pp. 33 – 34.

Naarmate het onderzoek vordert, kan de onderzoeker vragen om toestemming voor opvolgende fases. De EDPB erkent dat hierbij de eventueel toepasselijke ethische standaarden voor onderzoek opgevolgd dienen te worden. In Nederland is er de Gedragscode Gezondheidsonderzoek, die momenteel wordt herzien.⁵³ Andere waarborgen om het gebruik aan een specifieke toestemming te ondervangen zijn denkbaar, zoals verdergaande transparantie. Bijvoorbeeld door een onderzoeksplan gereed te hebben dat de patiënt kan inzien. In Finland is dit zelfs wettelijk verplicht. Ook vindt de EDPB het belangrijk dat principes als dataminimalisatie, anonimisering (zodra de persoonsgegevens niet meer nodig zijn voor het onderzoek) en informatiebeveiliging goed worden nageleefd. In knelpunt 9 van paragraaf 4.2.1 zetten wij nader uiteen, dat de lezing van de EDPB over toestemming niet door iedereen wordt omarmd.

Er zijn nog twee andere wetten op basis waarvan toestemming soms ook vereist is: de **Telecommunicatiewet** en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (**Wabvpz**). Onderstaand kader licht deze verder toe.

Naast gegevensverstrekking voor statistiek of wetenschappelijk onderzoek (zie de paragraaf hierna), zijn **er andere situaties waarin toestemming vragen niet hoeft**. Namelijk:

- op grond van een wettelijke bepaling;
- als de hulpverlener verkeert in een 'conflict van plichten' als hij zich aan zijn beroepsgeheim houdt;
- in verband met zwaarwegende belangen; en
- in het geval van 'veronderstelde toestemming'.

Hoewel deze omstandigheden voor de zorgpraktijk belangrijk zijn, spelen ze doorgaans geen rol bij de uitvoering van onderzoek met gegevens uit medische dossiers. Voor de volledigheid zijn deze begrippen in Tabel 6 van Bijlage 1 nader toegelicht, waarbij we ook de bepalingen uit de AVG toelichten op basis waarvan hulpverleners zonder toestemming gezondheidsgegevens mogen gebruiken.

53 Federa, Gedragscode Gezondheidsonderzoek ("code Goed Gedrag"), 2004, <https://www.federa.org/code-goed-gedrag>.

Kader **Andere toestemmingen: Cookies en WABVPZ**

*Naast de WGBO kent de wet andere voorschriften die ‘toestemming’ voor gegevensgebruik regelen. Bijvoorbeeld wettelijke voorschriften over ‘cookies’. Als gegevens tot stand zijn gekomen met bijvoorbeeld cookies, of als met cookies (of vergelijkbare technieken) gegevens zijn afgelezen van het device van een patiënt, zoals een Fitbit-horloge, mobieltje of computer, dan kan de **Telecommunicatiewet** een rol spelen. Bijvoorbeeld bij *quantified self* (paragraaf 2.2) of digitale portalen (paragraaf 2.3). Voordat het plaatsen van de cookies of het aflezen van de device mag plaatsvinden, moet de patiënt hierover geïnformeerd worden en om toestemming worden gevraagd (al kent de wet uitzonderingen hierop, bijvoorbeeld als de cookies of vergelijkbare technieken louter voor analytische doeleinden worden gebruikt of de betreffende situatie valt niet onder het bereik van de Telecommunicatiewet). De toestemming moet aan dezelfde eisen voldoen als de AVG-toestemming (zie Bijlage 3). Deze ‘cookieregels’ gelden ongeacht de vraag of er sprake is van een behandelrelatie en ongeacht of het gaat om persoonsgegevens.*

*Verder moeten zogeheten ‘**cookiewalls**’ worden vermeden, zoals bij het gebruik van digitale portalen. Dit zijn digitale muren die bijvoorbeeld als pop-up in beeld verschijnen. De websitegebruiker moet akkoord gaan met de in de pop-up vermelde voorwaarden over het cookiegebruik, anders is toegang niet mogelijk. De AP hekelt deze praktijk, omdat het neerkomt op een ‘take it or leave it’-aanbod. Dat is geen ‘echte’ of ‘vrije’ keuze, aangezien het weigeren van de toestemming leidt tot nadelige gevolgen, omdat dan de zorgportal niet gebruikt kan worden. Hoewel deze opvatting van de AP redelijk klinkt in de context van portals, die zouden immers breed toegankelijk moeten zijn, volgt die opvatting niet expliciet uit de Telecommunicatiewet. Die wet kent namelijk enkel een cookiewall-verbod voor overheidswebsites. Tegelijkertijd krijgt de AP bijval van de Europese privacytoezichthouders (EDPB Guidelines 05/2020). Het door de AP geopperde verbod op cookiewalls mag dus niet zomaar genegeerd worden.*

*Toestemming wordt ook genoemd in **Wabvpz**. Op basis hiervan mag de zorgaanbieder (lees: een instelling c.q. een solistisch werkende zorgverlener) slechts gegevens van de cliënt (lees: patiënt) **beschikbaar stellen via een***

elektronisch uitwisselingssysteem, voor zover hij heeft vastgesteld dat de cliënt daartoe uitdrukkelijk toestemming heeft gegeven. Een 'elektronisch uitwisselingssysteem' is een systeem waarmee zorgaanbieders op elektronische wijze dossiers (en gedeelten van dossiers of gegevens uit dossiers) voor andere zorgaanbieders raadpleegbaar kunnen maken, voor het bijhouden van een elektronisch dossier. Bijvoorbeeld via de zorginfrastructuur Landelijk Schakelpunt (LSP). Bij medisch data-onderzoek kan de Wabvpz een rol spelen als hiervoor gegevens elektronisch worden uitgewisseld tussen zorgaanbieders. Echter, lang niet ieder IT-systeem waarmee dit kan, voldoet aan de definitie 'elektronisch uitwisselingssysteem'. Interne ziekenhuissystemen vallen er niet onder. Het hangt van de inrichting van een digitaal gegevensuitwisselingssysteem af, of de Wabvpz van toepassing is.⁵⁴ Dit zou voorafgaand aan het onderzoek geverifieerd moeten worden, om te voorkomen dat een toestemmingsverplichting onder de Wabvpz niet wordt nageleefd. Zo'n verificatie is nodig, omdat de Wabvpz het niet mogelijk maakt dat voor onderzoek zonder toestemming gegevens uit een elektronisch uitwisselingssysteem gehaald mogen worden.⁵⁵

3.1.2 Uitzondering: geen toestemming nodig voor gebruik van gegevens, mits voldaan aan de voorwaarden

Soms is de verstrekking van gegevens over patiënten of inzage in patiëntdossiers aan 'anderen', zoals onderzoekers, **toegestaan zónder toestemming van de patiënt**. De WGBO stelt hieraan drie eisen, die hieronder worden toegelicht. Overigens is het zo dat hulpverleners alleen *desgevraagd* patiëntgegevens aan onderzoekers mogen verstrekken of hen inzage in dossiers mogen verschaffen, waarbij het **initiatief tot verzoek om gegevensverstrekking behoort uit te gaan van de onderzoeker** (Ploem 2006).

54 Programma GTS, 'Juridisch kennisdocument. Toestemming bij elektronische gegevensuitwisseling van medische gegevens', 9 augustus 2019, <https://www.rijksoverheid.nl/documenten/rapporten/2019/08/09/programma-gts>, pp. 8 – 9. Kamerbrief van Minister Bruins van Volksgezondheid, Welzijn & Sport, 12 juli 2019, Derde brief elektronische gegevensuitwisseling in de zorg, <https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/12/kamerbrief-over-derde-brief-elektronische-gegevensuitwisseling-in-de-zorg>.

55 Eerste Kamer, vergaderjaar 2015–2016, 33 509, N, *Nota naar aanleiding van het Verslag Cliëntenrechten bij elektronische verwerking van gegevens*, pp. 8 – 9.

A. Statistiek of wetenschappelijk onderzoek

In de eerste plaats moet het onderzoek onder de noemer vallen van **statistiek of wetenschappelijk onderzoek**. Hoewel er onduidelijkheid bestaat over de exacte afgrenzing van deze begrippen,⁵⁶ komen we op basis van de AVG en de opinies van de EDPB tot de omschrijvingen in Tabel 2.

B. Op het gebied van de volksgezondheid

Daarnaast moet het gaan om onderzoek op het gebied van de **volksgezondheid**. Voor de invulling van de term 'volksgezondheid' legt de AVG een link met een EU-verordening.⁵⁷ Hierin wordt 'volksgezondheid' uitgelegd als: *“alle elementen in verband met de gezondheid, namelijk gezondheidstoestand, inclusief morbiditeit en beperkingen, de determinanten die een effect hebben op die gezondheidstoestand, de behoeften aan gezondheidszorg, middelen ten behoeve van de gezondheidszorg, de verstrekking van en de universele toegang tot gezondheidszorg, alsmede de uitgaven voor en de financiering van de gezondheidszorg, en de doodsoorzaken.”*

Denk aan onderzoeken naar de oorzaak van de ziekten, de kwaliteit van het medisch handelen of de effectiviteit van programma's ter voorkoming van chronische ziekten.⁵⁸ Bevolkingsonderzoeken kunnen in een grijs gebied vallen. Niet-risicovolle onderzoeken vallen onder de WGBO.⁵⁹ Dit kan een bevolkingstoets naar darmkanker zijn (RIVM 2011; RIVM 2017).

C. Ten behoeve van een algemeen belang

Bovendien moet het onderzoek volgens de WGBO een **algemeen belang** dienen. Onderzoeken waarvan de resultaten naar verwachting niet kunnen bijdragen aan nieuwe wetenschappelijke inzichten, zullen niet aan het 'algemeen belang'-criterium voldoen.⁶⁰ Dit geldt evenmin voor onderzoeken die zijn ingegeven door 'persoonlijk hobbyisme'. **Hetzelfde geldt voor onderzoeken die louter een industrieel of commercieel belang dienen.**⁶¹ Dit laatste betekent overigens niet dat *for profit* onderzoek geen algemeen belang zou kunnen dienen⁶², of dat wetenschappelijk onderzoek altijd volledig uit publieke middelen gefinancierd moet zijn.⁶³

56 Tweede Kamer, vergaderjaar 2017–2018, 34 851, nr. 3, *Memorie van Toelichting UAVG*. Zie ook EDPS 2020.

57 Overweging 54 AVG, onder verwijzing naar Verordening (EG) nr. 1338/2008 van het Europees Parlement en de Raad.

58 *Memorie van Toelichting WGBO*, p. 15.

59 *Nadere Memorie van Antwoord WGBO*, p. 41.

60 *Nadere Memorie van Antwoord WGBO*, p. 47.

61 *Nadere Memorie van Antwoord WGBO*, p. 47.

62 Tweede Kamer, vergaderjaar 1998–1999, 25 892, nr. 6, *Nota n.a.v. het Verslag Wet bescherming persoonsgegevens (Wbp)*, p. 17 – 18.

63 *Memorie van Toelichting UAVG*, p. 51.

Tabel 2 Omschrijvingen van statistiek en wetenschappelijk onderzoek

Type onderzoek	Omschrijving	Voorbeelden
Wetenschappelijk onderzoek	Een onderzoeksproject dat wordt opgezet in overeenstemming met de relevante methodologische en ethische normen van de wetenschappelijke sector waarin de onderzoeker zich bevindt, en conform goede praktijken (Engels: <i>good practice</i>) (WP259, 2018). Het hoeft niet per se om publiek gefinancierd onderzoek te gaan. ⁶⁴	technologische ontwikkeling en demonstratie; fundamenteel onderzoek; toegepast onderzoek; en uit particuliere middelen gefinancierd onderzoek.
Statistiek	Het verzamelen en verwerken van persoonsgegevens die nodig zijn voor statistische onderzoeken en voor het produceren van statistische resultaten. De statistische resultaten mogen ook voor andere doeleinden worden gebruikt, zoals voor wetenschappelijke onderzoeksdoeleinden. Het statistische oogmerk betekent dat <i>het resultaat van de verwerking</i> voor statistische doeleinden niet uit persoonsgegevens bestaat, maar uit geaggregeerde gegevens. ⁶⁵ Het geaggregeerde resultaat en de onderliggende persoonsgegevens mogen niet worden gebruikt als ondersteunend materiaal voor maatregelen of beslissingen die een patiënt raken, aldus de EU-privacytoezichthouders.	Door ziekenhuizen verzamelde informatie over de aantallen van verkeersslachtoffers.

Moeten de resultaten van het onderzoek **publiekelijk beschikbaar** zijn? Dit lijkt voort te vloeien uit de eis van algemeen belang (CBP 2002) maar dit is niet zeker. **Niet alle onderzoeken leiden immers tot publicaties⁶⁶ en de AVG verplicht het**

⁶⁴ *Memorie van Toelichting UAVG*, p. 51.

⁶⁵ Overweging 162 AVG.

⁶⁶ Vgl. Eerste Kamer, vergaderjaar 2017–2018, 34 851, D, *Memorie van Antwoord UAVG*, antwoord op vraag 6 (in de context van artikel 43 UAVG over o.a. academische uitdrukkingsvormen).

niet.⁶⁷ Daarentegen verwachtte voormalig minister Bruins wel publicatie over het onderzoek en de resultaten, ook als de resultaten negatief zijn. Hij verwachtte ook dat er wordt voldaan aan de FAIR-principes.⁶⁸ De FAIR-principes staan niet in de wet, maar worden erkend in de (inter)nationale onderzoekswereld als richtlijnen voor datamanagement⁶⁹ en eisen voor de integriteit voor het onderzoek. Deze uitspraak deed de voormalige minister in de context van de UAVG, maar het betreffende artikel over het ‘algemeen belang’ uit die wet is dezelfde norm als die uit de WGBO.⁷⁰ Hieruit kan in ieder geval geconcludeerd worden, dat publicatie volgens de minister wenselijk is, maar verheldering is op dit punt nog nodig.

Het ‘algemeen belang’-criterium betekent dat de bevordering of bescherming van de volksgezondheid wordt nagestreefd. Volgens de wetgever betekent dit, dat er een redelijke mate van waarschijnlijkheid moet zijn dat een groep van enige omvang daarbij een aanzienlijk voordeel kan hebben. Een voorbeeld van zo’n groep zijn de DES-dochters (Berkvens & Prins 2007). Andere voorbeelden van onderzoeken die een algemeen belang kunnen dienen, zijn:⁷¹

- Retrospectief onderzoek, bijvoorbeeld met behulp van algoritmes of *data mining* op medisch dossiers;
- Onderzoek gericht op medische diagnostiek en behandeling (curatieve en preventieve gezondheidszorg);
- Onderzoek over mortaliteitsgegevens in relatie tot causale factoren in de individuele historie;
- Vervolgonderzoek naar causaliteit en clustering van ziekten of sterfte in relatie tot familiale factoren of omgevingsfactoren.

Het algemeen belang moet van meet af aan aanwezig zijn. Dit belang mag dus niet later door de onderzoekers ‘erbij’ worden bedacht om zo de gegevensverstrekking te rechtvaardigen (CBP 2005).

67 Overweging 159 AVG: “Om als verwerking van persoonsgegevens met het oog op wetenschappelijk onderzoek te worden aangemerkt, moet de verwerking aan specifieke voorwaarden voldoen, met name wat betreft het publiceren of anderszins openbaar maken van persoonsgegevens voor wetenschappelijke onderzoeksdoeleinden.”

68 Reactie Minister Bruins voor Medische Zorg & Sport, ‘Kamerbrief met reactie op artikel over secundair gebruik data’, 4 oktober 2019, <https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/04/kamerbrief-over-reactie-artikel-fd-over-secundair-gebruik-data>.

69 ELSI Servicedesk, <https://elsi.health-ri.nl/wat-fair>.

70 Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr. 3, *Memorie van Toelichting Wbp*, bij artikel 23 lid 2 Wbp.

71 *Nadere Memorie van Antwoord WGBO*, p. 47.

3.1.3 Situatie gelegen bij de patiënt: toestemming vragen is in redelijkheid niet mogelijk

Als een onderzoeker gegevens wenst te verkrijgen zonder toestemming, dan dient in alle gevallen het onderzoek te voldoen aan de eisen genoemd bij A t/m C in de voorgaande paragraaf. Daarna dient te worden onderzocht of het **mogelijk is om af te wijken van de hoofdregel** (paragraaf 3.1.1) dat er toestemming moet worden gevraagd van de patiënt. De wet omschrijft **twee situaties waarin toestemming niet aan de orde hoeft te zijn**. De toestemming is in redelijkheid niet mogelijk (deze paragraaf 3.1.3) en/of de toestemming kan in redelijkheid niet worden verlangd (paragraaf 3.1.4). Eén van deze situaties moeten aan de orde zijn, anders mag er geen verstrekking zonder toestemming plaatsvinden.

Als toestemming in redelijkheid niet mogelijk is voor de gegevensverstrekking, dan mag deze achterwege worden gelaten. Het gaat dan om bepaalde omstandigheden gelegen bij de patiënt.⁷² Bijvoorbeeld als de contactgegevens niet meer te achterhalen zijn, of omdat de betreffende patiënten zijn overleden. Toestemming mag ook achterwege blijven als dit te belastend is voor de patiënt, of in onderzoeken waarin uit een grote patiëntenpopulatie een steekproef moet worden getrokken. In paragraaf 2.1 zagen we dat dit één van de genoemde redenen is van de ziekenhuizen die een database creëerden met gegevens van coronapatiënten. Het is overigens niet vereist dat toestemming vragen feitelijk *onmogelijk* moet zijn.⁷³ Zie het overzicht in Tabel 3 met een uitwerking van voorbeelden waarin toestemming achterwege zou kunnen blijven.

Sommige redenen volstaan niet om toestemming achterwege te laten.

Bijvoorbeeld de reden dat het vragen van toestemming een onderzoek te duur zou maken of het onderzoek teveel zou vertragen, zo lichtte de wetgever toe.⁷⁴ Dit is dus anders dan wat het RIVM vermeldt in een handreiking, waarin 'hoge kosten' als een praktisch bezwaar wordt genoemd waardoor toestemming redelijkerwijs niet mogelijk zou zijn (RIVM 2019). Die opvatting dient dus genuanceerd te worden.

Als het vragen van toestemming in redelijkheid niet mogelijk is, mag de hulpverlener direct naar de patiënt herleidbare gegevens verstrekken, mits de uitvoering van het onderzoek is voorzien in zodanige waarborgen, dat de persoonlijke levenssfeer van de patiënt niet onevenredig wordt geschaad (Ploem 2006). Hiermee wordt bedoeld op de 'inbreuk' die door de verstrekking van de gegevens wordt toegebracht aan de persoonlijke levenssfeer. De inbreuk wordt in hoge mate bepaald door de aard van de gegevens. Bij delicate gegevens zal

72 Tweede Kamer, vergaderjaar 1993-1994, 21 561, nr. 20, *Vierde Nota van Wijziging WGB0*, p.3.

73 *Memorie van Antwoord WGB0*, p. 67. *Nota n.a.v. het Eindverslag WGB0*, p. 35.

74 *Memorie van Toelichting WGB0*, pp. 40 – 41.

eerder duidelijk zijn, dat het belang dat met de verstrekking is gemoeid, niet opweegt tegen de schade die daaruit voortvloeit voor de persoonlijke levenssfeer van de patiënt, dan bij gegevens die door de patiënt niet als (erg) gevoelig worden ervaren.⁷⁵

Daarnaast zijn de omstandigheden waaronder de gegevensverstrekking plaatsvindt van belang voor de beslissing tot verstrekking. Bijvoorbeeld de kwaliteit of de integriteit van de onderzoeker, of de afspraken die de onderzoeker bereid is te maken met de hulpverlener over de gegevensbescherming tijdens het onderzoek.⁷⁶ Afspraken kunnen gaan over een begrenzing van het aantal personen dat in het kader van het onderzoek de gegevens onder ogen krijgt. **De hulpverlener moet dus nagaan wat voor vlees hij in de kuip heeft.**

Of het vragen van toestemming in redelijkheid niet mogelijk is, hangt af van de omstandigheden van het geval. De wetgever vertrouwt op de wettelijke zorgplicht die de hulpverlener heeft om hierin een goede afweging te maken.⁷⁷ Hieruit vloeit voort dat de hulpverlener – gelet op de omstandigheden en op de gevoeligheid van de gegevens die nodig zijn voor het onderzoek – **passende waarborgen** verbindt aan het gegevens gebruik door de onderzoeker. De wetgever verwacht bijvoorbeeld dat persoonsgegevens over erfelijke ziekten aan andere voorwaarden worden gebonden dan gegevens over een griepepidemie.⁷⁸ **De hulpverlener dient ook het belang van het onderzoek af te wegen tegen mogelijk belastende effecten bij de patiënt als er om toestemming wordt gevraagd.**⁷⁹ Hierbij mag niet te snel worden aangenomen dat de patiënt niet in staat is om zijn belangen te behartigen, aldus de wetgever.⁸⁰ Of die aanname terecht is, is onderwerp van verdere discussie.

75 *Memorie van Toelichting WGBO*, p. 41.

76 *Memorie van Toelichting WGBO*, p. 41.

77 Artikel 7:453 BW.

78 *Nota n.a.v. het Eindverslag WGBO*, p. 8 en p. 33.

79 *Nadere Memorie van Antwoord WGBO*, p. 47.

80 *Nota n.a.v. het Eindverslag WGBO*, p. 35.

Tabel 3 Situaties waarin toestemming vragen achterwege kan blijven

Voorbeeld	Toelichting
<p>De contactgegevens van de patiënten zijn niet meer te achterhalen, bijvoorbeeld omdat het een historisch onderzoek naar jaren geleden betreft, of omdat de patiënt vanwege een verhuizing niet meer bereikbaar is.</p>	<p>Dit gebeurt bijvoorbeeld bij retrospectieve onderzoeken waar de te onderzoeken gegevens vaak ver in het verleden zijn vastgelegd.</p> <p>Of denk aan historisch-wetenschappelijk onderzoek ter uitvoering van Arbeidsomstandighedenbesluit dat een bewaartermijn van 40 jaar voorschrijft voor de resultaten van arbeidsgezondheidskundig onderzoek over gevaarlijke stoffen en biologische agentia (Berkvens & Prins 2007). De voor het wetenschappelijke onderzoek benodigde gegevens betreffen een aanzienlijke groep ex-werknemers van wie het adres niet meer te achterhalen is. Het vragen van hun toestemming zal niet of nauwelijks mogelijk zijn.</p>
<p>Overleden patiënten</p>	<p>Overleden patiënten kunnen logischerwijs geen toestemming meer geven. N.B. zelfs als de patiënt overleden is, worden de gegevens uit zijn of haar medisch dossier tot op bepaalde hoogte beschermd door de WGBO. Inzage in het dossier door anderen is alleen toegestaan als het gaat om: een persoon die van de patiënt (bij leven) hiervoor toestemming heeft gekregen, een nabestaande als die een melding heeft ontvangen van een 'medische misser'⁸¹ of aan iedereen die een zwaarwegend belang heeft en aannemelijk maakt dat dit belang mogelijk wordt geschaad en dat inzage in of afschrift van gegevens uit het dossier noodzakelijk is voor de behartiging van dit belang. In al deze gevallen worden alleen de gegevens verstrekt voor zover deze betrekking hebben op de grond waarvoor inzage wordt verleend.</p>
<p>Het vragen van de toestemming zou te zeer belastend zijn voor de patiënt, bijvoorbeeld als hierdoor ernstige psychische belasting van de (ex-)patiënt of ex-patiënt wordt veroorzaakt.</p>	<p>Belastende effecten kunnen ook aan de orde zijn als door de gevraagde toestemming de ex-patiënt op belastende wijze geconfronteerd met een onderzoek naar zijn gegevens. De patiënt krijgt dan mogelijk een herhaalde onwenselijke herinnering aan de ziekteperiode, of er ontstaat bij hem valse hoop. Het benaderen van dergelijke patiënten met een verzoek om toestemming zou onkies kunnen zijn. Vermijding van het veroorzaken van ernstige psychische belasting van de (ex-)patiënt kan zich bijvoorbeeld voordoen in een onderzoek naar achtergronden van poging tot zelfdoding.</p>
<p>Onderzoeken waaruit in een grote patiëntenpopulatie een steekproef moet worden getrokken.</p>	<p>Om patiënten hiervoor te kunnen selecteren is inzage nodig in niet-geanonimiseerde gegevens. In de eerste fase van het onderzoek is het lastig alle betreffende patiënten aan te schrijven, terwijl de voorselectie voor de steekproef ook moeilijk door de hulpverlener zelf gedaan kan worden.</p>

81 Artikel 7:458a lid 1 en 7:458b BW.

3.1.4 Situatie gelegen in de aard van het onderzoek: toestemming in redelijkheid niet te verlangen

Een andere omstandigheid waarin toestemming niet gevraagd hoeft te worden, is **als de toestemming in redelijkheid niet kan worden verlangd**.⁸² Deze uitzondering is van toepassing vanwege omstandigheden die zijn gelegen in de aard van het onderzoek.⁸³ Het gaat bijvoorbeeld om:

- onderzoeken waarbij zulke grote aantallen patiënten betrokken zijn, dat redelijkerwijs niet kan worden gevergd dat er inspanningen worden gedaan om alle patiënten te bereiken. Het is goed denkbaar dat onderzoekers met *big data* analyses, al dan niet met behulp van AI of *data mining* deze situatie zullen aantreffen;
- de situatie waarin het vragen van toestemming zou leiden tot een selectieve respons, waarmee er een reëel risico bestaat op vertekening van het onderzoeksresultaat.⁸⁴ Volgens de Gezondheidsraad moet het gaan om “een aantoonbaar risico van vertekening van de onderzoeksresultaten door een op goede gronden te verwachten selectieve respons.” (Gezondheidsraad 2000)

Deze uitzondering op het beginsel dat toestemming nodig is, kent als eis dat de hulpverlener ervoor zorgt dat de te verstrekken gegevens in **zodanige vorm worden verstrekt dat herleiding tot patiënten redelijkerwijs wordt voorkomen**. Om dit te bewerkstelligen kan ervoor worden gekozen om gecodeerde of geanonimiseerde gegevens te verstrekken (zie actiepunt #1 hierna). Ook een toezichtscommissie en het gebruik van een intermediaire organisatie kunnen eraan bijdragen dat risico's op herleidbaarheid worden verkleind (zie actiepunt #2 hierna). Sowieso mogen de resultaten van het onderzoek niet in tot de persoon herleidbare vorm gepresenteerd worden. Dit staat niet letterlijk in de wet en dat was ook niet nodig, omdat de wetgever constateerde dat dit principe in de wetenschappelijk wereld onderzoek aanvaard is.⁸⁵

Actiepunt #1: Gegevens moeten zo worden verstrekt, dat herleiding redelijkerwijs wordt voorkomen

'Gecodeerd' betekent dat onderzoekers beschikking krijgen over medische gegevens van patiënten, maar niet over hun direct identificerende kenmerken, zoals NAW-gegevens of geboortedata. Het idee is dat de onderzoeker of het

82 Dit is dezelfde norm die in de Uitvoeringswet AVG wordt beschreven als “het vragen van uitdrukkelijke toestemming een onevenredige inspanning kost”. Zie CBP 2005, p. 25, voetnoot 9. Artikel 23 lid 2 Wbp is overgenomen in artikel 24 sub c Uitvoeringswet AVG.

83 *Vierde Nota van Wijziging WGBO*, p.3.

84 *Vierde Nota van Wijziging WGBO*, p.3.

85 *Memorie van Antwoord WGBO*, p. 41.

onderzoeksinstituut niet beschikt over informatie waarmee de onderzoeksgegevens herleid kunnen worden naar de patiënt.

Als er wordt gekozen voor codering, dan is het de bedoeling om de aan te leveren, gecodeerde, onderzoeksgegevens te koppelen aan willekeurige nummers. Daardoor blijft het mogelijk om terug te gaan naar de persoon van wie de gegevens afkomstig zijn, voor het geval men de onderzoeksgegevens op een later moment aan nieuwe gegevens van diezelfde patiënt willen koppelen (Ploem 2013). In zulke gevallen vindt de herleiding naar de patiënt plaats via een sleutel, die wordt bewaard door een hulpverlener of een **trusted third party** (zie verderop in deze paragraaf).

Gecodeerde gegevens zijn geen geanonimiseerde gegevens en dienen doorgaans als gepseudonimiseerde persoonsgegevens te worden beschouwd. Immers, via de route van decodering blijft herleiding naar individuen mogelijk. Dat terwijl anonimisering onomkeerbaarheid veronderstelt. In plaats daarvan is er veelal sprake van pseudonimisering. **Pseudonimisering** wordt in de AVG omschreven als 'het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene – zoals een patiënt – kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en (...) maatregelen worden genomen om ervoor te zorgen dat de gegevens niet worden gekoppeld aan [de patiënt].' Hulpverleners en onderzoekers moeten dus beseffen dat **gecodeerde, gepseudonimiseerde, gegevens meestal persoonsgegevens zijn**. Dat is in ieder geval bij 'tweewegscodering' zo (ook wel tweewegspseudonimisering genoemd), waarin er een sleutel 'terug' is van de codering (of het pseudoniem) naar direct identificerende gegevens waarop de codering is gebaseerd. Er bestaat ook 'eenwegscodering', waarin gegevens worden 'gehashed' en er geen sleutel is die de gehashte gegevens kan doen verkleuren naar direct identificerende gegevens, maar zelfs daarvan is niet uit te sluiten dat dit 'persoonsgegevens' zijn in de zin van de AVG (Stüssgen et al. 2019). **De AVG blijft dus van toepassing op gecodeerde gegevens** (Ploem 2000).

In de onderzoekspraktijk is **anonimiseren**, voor zover dat mogelijk is en het onderzoeksdoel niet frustreert, **een nuttige beveiligingsmaatregel**, net als pseudonimiseren. Zowel bij anonimiseren als bij pseudonimiseren wordt het risico verkleind dat een kwaadwillende met de gegevens aan de haal kan gaan, bijvoorbeeld als gevolg van een datalek.

De wetgever houdt de deur open voor de mogelijkheid dat de onderzoeker, na verstrekking, **nadere gegevens** kan verkrijgen over patiënt. Soms moet de onderzoeker namelijk 'terug' naar de dossiers die de hulpverlener onder zich houdt.

Als dat noodzakelijk is, dan verkrijgt de onderzoeker de nadere gegevens alsnog via de daarvoor afgesproken procedures langs de weg van daadwerkelijke herleiding. Hier is dus geen sprake van anonimisering. Voor de herleiding is doorgaans de medewerking van de hulpverlener vereist. Als voor het onderzoek de dossiers van de patiënten op naam moet worden ingezien, dan moet de hulpverlener alsnog om toestemming van de patiënt vragen, tenzij de toestemming daarvoor in redelijkheid niet mogelijk is (zie paragraaf 3.1.3).

Actiepunt #2: Toezichtcommissie en een intermediaire organisatie ('trusted third party')

Het is niet de bedoeling dat de onderzoekers de ontvangen gegevens zelfstandig gaan herleiden naar individuele patiënten, bijvoorbeeld met behulp van bestandsvergelijking. Is een dergelijke vergelijking voor het onderzoek toch nodig, dan dienen hiervoor **besluitvormingsprocedures** te zijn ingericht, bijvoorbeeld in de vorm van een toezichtcommissie van het onderzoeksinstituut, alvorens tot herleiding naar patiënt overgaan mag worden.⁸⁶

Volgens de wetgever is het denkbaar dat de hulpverlener een intermediaire organisatie ('**trusted third party**') inschakelt die de sleutel van de gecodeerde gegevens beheert, en zodoende technisch beschikt over de mogelijkheid gegevens tot de patiënt te herleiden.⁸⁷ De feitelijke **herleiding** gebeurt dan via de hulpverlener en niet de onderzoeker. Zo behoudt de hulpverlener de zeggenschap over de herleidbaarheid. Het gebruik van een intermediaire organisatie als '**trusted third party**' is echter niet verplicht. Als er gebruik van wordt gemaakt, dan moet deze derde-partij op afstand optreden van de onderzoekers en onderzoeksinstituten. Ook dienen er waarborgen te zijn dat de gegevensverstrekking aan de intermediair past binnen de onderzoeksdoelstellingen. Zo dient er met de intermediair een overeenkomst te worden gesloten. In de overeenkomst kunnen afspraken worden gemaakt over codering en verstrekking van gecodeerde gegevens aan een onderzoeker of een onderzoeksinstituut.⁸⁸

86 Vierde Nota van Wijziging WGBO, p. 4.

87 Vierde Nota van Wijziging WGBO, p. 4.

88 Vierde Nota van Wijziging WGBO, p. 4.

Nadat is vastgesteld dat:

- er sprake is van een onderzoek met wetenschappelijke of statistische doeleinden (paragraaf 3.1.2, A);
- op het gebied van volksgezondheid (*idem*, B);
- ten behoeve van het algemeen belang (*idem*, C); en dat
- minimaal één van de twee situaties (paragrafen 3.1.3 en 3.1.4) van toepassing zijn,

dan resteren er twee voorwaarden. Ten eerste moet worden vastgesteld dat het onderzoek niet kan worden uitgevoerd zonder de gevraagde gegevens (paragraaf 3.1.5) en dat de patiënt geen bezwaar heeft (gehad) tegen de gegevensverstrekking (paragraaf 3.1.6.).

3.1.5 Eerste voorwaarde: het onderzoek kan niet zonder desbetreffende gegevens worden uitgevoerd

Een eerste vereiste om de gegevens uit het medische dossier te mogen gebruiken is dat **het onderzoek niet zonder de desbetreffende gegevens uitgevoerd kan worden**. Dit betekent dat bij iedere gegevensverzameling en het gebruik daarvan nagegaan moet worden of het onderzoek niet op een andere manier uitgevoerd kan worden, die minder ingrijpend is ten aanzien van de rechten en belangen van de patiënt. Bijvoorbeeld door in plaats van direct herleidbare gegevens geanonimiseerde of gecodeerde gegevens te gebruiken. Of het beoogde resultaat op een andere wijze kan worden bereikt, die voor de privacy van de patiënt minder belastend is, is een vraag die zowel de hulpverlener als onderzoeker zich moeten stellen (Berkvens & Prins 2007).⁸⁹

3.1.6 Tweede voorwaarde: de patiënt heeft geen uitdrukkelijk bezwaar gemaakt tegen de verstrekking

Patiënten kunnen via hun **bezwaarmogelijkheid** de gegevensverstrekking blokkeren. Hulpverleners moeten daarom nagaan of de patiënten wier gegevens gebruikt worden voor het onderzoek, hiertegen uitdrukkelijk bezwaar hebben gemaakt, voordat zij tot verstrekking overgaan.

Als een patiënt niet wil dat zijn persoonsgegevens voor wetenschappelijk onderzoek en statistiek worden gebruikt en hiertegen bezwaar maakt, dan hoeft hij

89 Anders: Ploem 2006.

dit niet verder onderbouwen.⁹⁰ Het bezwaar moet worden gerespecteerd, al kan hij in tweede instantie alsnog de gegevensverstrekking toestaan op basis van toestemming.⁹¹

De bezwaarmogelijkheid moet zijn geboden voorafgaand aan het onderzoek. Voor onderzoek met anoniem lichaamsmateriaal geldt een vergelijkbaar 'geen-bezwaarsysteem'. In die context heeft de wetgever verduidelijkt dat ziekenhuizen voorzieningen moeten treffen om de zorgvuldige uitvoering van dit systeem te verzekeren. Bijvoorbeeld met behulp van algemene voorlichting van het publiek door voorlichtingsbureaus en folders.⁹²

Het ligt voor de hand dat ook in de context van onderzoek vergelijkbare voorzieningen gelden.⁹³ Diverse auteurs beamen dit en noemen bijvoorbeeld eveneens informatiefolders in het ziekenhuis als informatievoorziening over het geen-bezwaarsysteem (Ploem et al. 2020, Scholte et al. 2019, Stüssgen et al. 2019). Soms gaat dit mis, zoals toen het RIVM volgens (de voorganger van) de AP geen maatregelen had getroffen, die ertoe strekten de patiënt naar behoren in kennis te stellen van de mogelijkheid een dergelijk bezwaar aan te tekenen.⁹⁴

Hulpverleners zijn vrij om naar eigen inzicht een **geen-bewaarsysteem** in te richten. Vooralsnog worden de systemen per hulpverlener, zoals per ziekenhuis, ingericht. Er zijn meer praktische oplossingen denkbaar. Zo doet onderzoeksinstituut Nivel een voorstel voor een centraal bezwaarregister, dat te vergelijken is met het landelijke donorregister (Stüssgen et al. 2019). PGO's kunnen hierin een rol spelen, maar er blijven vragen over de praktische uitvoering. Zie kader hieronder.

Als patiënten niet op de hoogte zijn gesteld van het feit dat de gegevens uit hun dossier voor statistiek of wetenschappelijk onderzoek gebruikt konden worden, of als er geen bezwaarmogelijkheid is geweest, dan mogen die gegevens niet worden verstrekt voor onderzoek. De **informatieplicht over het geenbezwaar-systeem** richting de patiënt rust op de hulpverlener die de gegevens aanlevert, maar het ligt voor de hand dat de onderzoekers daarbij een ondersteunende rol spelen (Ploem 2006).

90 *Vierde Nota van Wijziging WGBO*, p. 4.

91 *Nadere Memorie van Antwoord WGBO*, p. 25.

92 *Memorie van Antwoord WGBO*, p. 74.

93 *Vierde Nota van Wijziging WGBO*, p. 4.

94 Autoriteit Persoonsgegevens, 'Triple-test: registratie van post-partumgegevens door het RIVM', 12 maart 2002, <https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/triple-test-registratie-van-post-partumgegevens-door-het-rivm-%C2%A0>.

Kader **PGO's, de WABVPZ en onderzoek**

De gegevens in persoonlijke gezondheidsomgevingen (PGO's) kunnen met de hulpverlener worden gedeeld als dit nodig is voor de behandeling, maar de PGO's fungeren niet als medisch dossier in de zin van de WGBO. Ook zijn PGO's niet in de wet geregeld, maar deze digitale toepassingen kunnen wel een rol spelen binnen de wettelijke kaders. Zo regelt de Wabvpz de randvoorwaarden voor elektronische gegevensuitwisseling in de zorg en de beschikbaarheid van gegevens via elektronisch uitwisselingssystemen. Sinds 1 juli 2020 bepaalt de Wabvpz dat patiënten (in de Wabvpz 'cliënten' genoemd) recht hebben op elektronische inzage of elektronisch afschrift van zijn dossier, of van diens gegevens die de zorgaanbieder via een elektronisch uitwisselingssysteem beschikbaar stelt.

De Wabvpz schrijft de vorm niet voor waarop elektronische inzage of een elektronisch afschrift moet worden ontsloten.⁹⁵ De digitale ontsluiting van zorggegevens kan dus plaatsvinden via een PGO. Het gaat hier in de regel om PGO's met een MedMij-label. Het MedMij-label vertegenwoordigt een veilige en betrouwbare koppeling van medische gegevens uit het medisch dossier van de zorgverlener. Voor onderzoekers kunnen PGO's relevant zijn. Zo signaleert Nivel dat PGO's geschikt kunnen zijn om bij te houden of de patiënt wel of geen bezwaar heeft tegen onderzoek met gegevens. PGO's faciliteren op die manier geen-bezwaarsystemen die hulpverleners verplicht moeten hanteren (paragraaf. 3.1.6). Dit zou een alternatief kunnen zijn, zowel voor de huidige situaties, waarin ziekenhuizen zelf de bezwaren registeren als voor een centraal bezwaarregister (Stüssgen et al. 2019). De gegevens die zijn verzameld in de PGO kunnen zo, onder regie van de patiënt, ter beschikking worden gesteld aan onderzoekspartijen.

De vraag is of het voorstel van Nivel direct in de praktijk kan worden gebracht, los van de technische en organisatorische uitdagingen. Zo vallen de gegevens in een PGO doorgaans niet onder het beroepsgeheim van de hulpverlener, aldus Patiëntenfederatie Nederland (2019a). De patiënt beheert immers de PGO en dus ontbreekt de hulpverlener als tussenstap bij een informatievraag door derden. Dit betekent, dat informatie over de keuze 'wel of geen bezwaar voor onderzoek', of informatie over de vraag of een patiënt toestemming heeft gegeven, niet beschermd wordt door de

WGBO. Dat kan echter wel wenselijk zijn (Dove & Chen 2020). Om gezondheidsgegevens die buiten het medisch beroepsgeheim vallen te beschermen, raadt onder meer Patiëntenfederatie Nederland een wettelijk 'patiëntgeheim' aan (2019a). Dit geheim beoogt burgers te beschermen tegen de druk om hun gezondheidsgegevens, die bijvoorbeeld zijn opgeslagen in PGO's, te delen met derden.⁹⁶ De minister gaat vooralsnog niet mee in dit voorstel en stelt dat de huidige regels van het gegevensbeschermingsrecht (paragraaf 1.3.1) voldoen.⁹⁷

Los van de vraag of de gegevens in PGO's beschermd kunnen – of zullen – worden door het beroepsgeheim of een patiëntgeheim, kunnen onderzoekers nu al gegevens gebruiken in PGO's, op basis van toestemming van degene op wie de gegevens betrekking hebben. Zij dienen dan rekening te houden met de (U)AVG. Zie hierover paragraaf 3.2.

Tot slot mogen patiënten bezwaar maken, ook *nadat* de (niet-anonieme) gegevens zijn verwerkt (Scholte et al. 2019). Volgens het Amsterdam UMC is het gevolg hiervan dat alleen de ruwe gegevens vernietigd hoeven te worden. Dus niet de gegevens uit de voor analyse bedoelde gegevensbestanden en onderzoeksresultaten. Als de gegevens worden verstrekt voor onderzoek, of als er voor onderzoek inzake is verleend in het medisch dossier, dan dient de hulpverlener hiervan een aantekening te maken in het dossier.⁹⁸

95 Brief van de Minister voor Medische Zorg d.d. 13 december 2019, <https://zoek.officielebekendmakingen.nl/kst-27529-209.html/>.

96 Rathenau Instituut, Gezondheid centraal – Bericht aan Parlement, 23 januari 2019, <https://www.rathenau.nl/sites/default/files/2019-01/20190123%20BAP%20Gezondheid%20centraal.pdf>.

97 Minister voor de Medische Zorg en Sport, Commissiebrief Tweede Kamer inzake Verzoek om stand van zaken over de zienswijze op het voorstel van de Patiëntenfederatie Nederland over het creëren van een patiëntgeheim, 1 oktober 2019, <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2019/10/01/commissiebrief-inzake-verzoek-om-stand-van-zaken-over-de-zienswijze-op-het-voorstel-van-de-patintfederatie-nederland-over-het-creeren-van-een-patintgeheim/commissiebrief-inzake-verzoek-om-stand-van-zaken-over-de-zienswijze-op-het-voorstel-van-de-patintfederatie-nederland-over-het-creeren-van-een-patintgeheim.pdf>.

98 7:458 lid 3 BW.

3.2 Gegevensgebruik door de onderzoekers

Als een onderzoeker aan de slag wil met gegevens afkomstig uit medische dossiers, dan dient hij eerst vast te stellen of de hulpverlener de gegevens had mogen verstrekken. Met andere woorden, kan de eerste stroomdiagram (zie Bijlage 4) succesvol worden doorlopen? Als dat niet het geval is, dan mogen de gegevens niet worden gebruikt.

Daarnaast dient de onderzoeker zich ervan te vergewissen of de hulpverlener de gegevens verstrekt op basis van toestemming van de patiënt (paragraaf 3.1.1) of op basis van de mogelijkheid die de WGBO biedt voor statistiek of wetenschappelijk onderzoek (paragraaf 3.1.2). Als de verstrekking plaatsvindt op basis van toestemming, dan is van belang dat de onderzoeker de gegevens **niet gebruikt buiten de reikwijdte van de gegeven toestemming**. Overigens geeft de wetgever van de (U)AVG, net als de WGBO-wetgever, de voorkeur aan het vragen van toestemming.⁹⁹

3.2.1 Onderzoeker ontheven van verbod om bijzondere persoonsgegevens te gebruiken

Bevatten de te onderzoeken gegevens *bijzondere persoonsgegevens*, zoals gezondheidsgegevens of genetisch gegevens, dan mogen deze gegevens volgens de UAVG gebruikt worden als aan bepaalde eisen is voldaan. Dit zal doorgaans geen probleem opleveren, als de eerste stroomdiagram (zie Bijlage 4) succesvol is doorlopen. De eisen luiden als volgt:

A. Wetenschappelijk onderzoek of statistische doeleinden

Ten eerste moet het gegevensgebruik noodzakelijk zijn met het oog op wetenschappelijk onderzoek of statistische doeleinden. Deze voorwaarden kwamen al aan de orde in paragraaf 3.1.2, punt A (statistiek of wetenschappelijk onderzoek) en paragraaf 3.1.5 (het onderzoek kan niet zonder de betreffende gegevens).

B. Algemeen belang

Ten tweede moet het onderzoek een algemeen belang dienen. Dit kwam al aan de orde in paragraaf 3.1.2, punt C. Naar aanleiding van het artikel in *Het Financieele Dagblad* over de klacht dat strenge privacyregels onderzoek zou hinderen, gaf voormalig minister Bruins aan, dat er sprake is van '*wetenschappelijk onderzoek in*

99 Memorie van Toelichting UAVG bij artikel 24 UAVG. Evenzo Memorie van Toelichting Wbp bij artikel 23 lid Wbp.

het algemeen belang' als het onderzoek als wezenlijk doel heeft het bevorderen en beschermen van de volksgezondheid door het op systematische wijze vergaren en bestuderen van gegevens. Onderzoek in uitsluitend commerciële of industriële context past daar niet in.¹⁰⁰ De minister vervolgt dat het verder redelijkerwijs aannemelijk moet zijn dat de onderzoeksresultaten nieuwe wetenschappelijke inzichten genereren die geldend zijn voor een populatie groter dan de directe onderzoekspopulatie.

De onderzoekers zullen zich moeten inspannen om hun resultaten inzichtelijk te maken voor een breder publiek dan alleen de kring van betrokken onderzoekers en betrokken patiënten, aldus de minister. Op basis van FAIR-principes dienen de onderliggende onderzoeksgegevens bewaard te worden voor validatie en onder voorwaarden beschikbaar te zijn voor andere onderzoekers.¹⁰¹ Zoals we hebben gezien in paragraaf 3.1.2, is dit een nieuwe opvatting die vooralsnog geen bijval heeft van de wetgever, een rechter of de AP.

C. Uitdrukkelijke toestemming blijkt onmogelijk of kost onevenredige inspanning

Ten derde vereist de UAVG dat het vragen van uitdrukkelijke toestemming alleen achterwege mag blijven als het onmogelijk blijkt, of een onevenredige inspanning kost. Ook deze eisen zijn vergelijkbaar met de WGBO-regeling (zie paragraaf 3.1.3 en 3.1.4).¹⁰²

D. Waarborgen

Tot slot verlangt de UAVG, dat bij de uitvoering van het onderzoek is voorzien in zodanige waarborgen, dat de persoonlijke levenssfeer van de patiënt niet onevenredig wordt geschaad. Het coderen van gegevens is zo'n waarborg, maar er zijn meer maatregelen denkbaar.

De UAVG verwijst naar de AVG, op basis waarvan wetenschappelijk onderzoek of statistische doeleinden onderworpen moeten zijn aan 'passende waarborgen'.¹⁰³ Dit

100 Brief van de Minister voor Medische zorg, d.d. 4 oktober 2019, nr. 191, <http://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2019/10/04/kamerbrief-over-reactie-artikel-fd-over-secundair-gebruik-data/kamerbrief-over-reactie-artikel-fd-over-secundair-gebruik-data.pdf>.

101 Zie bijvoorbeeld hierover de reactie van COREON op het wetsvoorstel van UAVG, te raadplegen via: <https://www.internetconsultatie.nl/uitvoeringswetavg/reactie/68998/bestand>.

102 De Minister merkt hierover op: "In sommige gevallen kan het ook voor deze wetenschappelijke onderzoeken onmogelijk zijn of een onevenredige inspanning vergen om toestemming te vragen, bijvoorbeeld indien men voor het onderzoek gebruik moet maken van een grote hoeveelheid data. Daarbij merk ik op dat het enkele feit dat er kosten gemoeid zijn met het vragen van toestemming niet kwalificeert als onevenredige inspanning.", Brief van de Minister voor Medische Zorg, d.d. 4 oktober 2019, nr. 191.

103 Artikel 24 sub a j.o. artikel 89 lid 1 AVG.

zijn waarborgen die er bijvoorbeeld voor zorgen dat de onderzoekers technische en organisatorische maatregelen treffen om het principe van dataminimalisatie te garanderen. Zoals door middel van pseudonimisering of anonimisering, voor zover dit nog niet bij de hulpverlener is gebeurd en voor zover dit mogelijk is.

Ook moeten de onderzoekers ervoor zorgen dat zoveel mogelijk voorkomen wordt dat de gegevens worden gebruikt voor het nemen van maatregelen of besluiten die tegen een patiënt gericht zijn.¹⁰⁴ Onderzoeken met een dergelijke impact zijn niet de bedoeling, volgens de EU-privacytoezichthouders (WP203, 2013). Andere waarborgen, zoals verdergaande transparantie en verhoogde informatiebeveiliging, waaronder begrepen een adequaat autorisatiesysteem, zodat alleen de onderzoekers kennis kunnen nemen van de gegevens, kwamen reeds in paragraaf 3.1.2 aan de orde.

E. Rechtsgrond voor gegevensgebruik blijft nodig

Als aan de voorwaarden genoemd bij A t/m D is voldaan, heft de UAVG het verbod op om de gegevens, zoals gezondheidsgegevens en genetische gegevens, te gebruiken. De onderzoekers dienen erop bedacht te zijn, dat zij nog steeds een rechtsgrond voor het gegevensgebruik moeten hebben op basis van de AVG. De AVG vereist immers dat persoonsgegevens – of dit nu gezondheidsgegevens zijn of niet – worden gebruikt voor een gerechtvaardigd doel en dat dit rechtmatig gebeurt.

Het gebruik van persoonsgegevens is volgens de AVG rechtmatig, als de betrokkene, zoals een patiënt, **(a) toestemming** heeft gegeven voor het gebruik van zijn persoonsgegevens (voor één of meer specifieke doeleinden) **óf** als **een andere rechtsgrond** aan de orde is, zoals hieronder in Tabel 4 weergegeven.

Afhankelijk van de situatie, zullen onderzoekers een beroep kunnen doen op:

- **(a) toestemming;**
- **(c) wettelijke verplichting;**
- **(e) vervulling van een publieke taak; of**
- **(f) de behartiging van de gerechtvaardigde belangen van de onderzoeksinstelling of een derde.**¹⁰⁵

104 Article 29 Working Party, WP203, Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013.

105 De aanduidingen (a), (c), (e) en (f) corresponderen met de aanduidingen van de rechtsgronden in artikel 6 lid 1 van de AVG.

Tabel 4 Rechtsgronden voor gebruik persoonsgegevens, naast toestemming

Rechtsgrond	Het gegevensgebruik is rechtmatig, als dit noodzakelijk is...
(b) uitvoering van een overeenkomst	... voor de <i>uitvoering van een overeenkomst</i> waarbij de betrokkene partij is (zoals een behandelingsovereenkomst); ¹⁰⁶
(c) wettelijke verplichting	... om te voldoen aan een <i>wettelijke verplichting</i> die op de verwerkingsverantwoordelijke (zoals een ziekenhuis of onderzoeksinstelling) rust; ¹⁰⁷
(d) vitale belangen	... om de <i>vitale belangen</i> van de betrokkene of van een andere natuurlijke persoon te beschermen (lees: acute leven-of-dood situaties); ¹⁰⁸
(e) vervulling van een publieke taak	... voor de <i>vervulling van een taak van algemeen belang</i> of van een <i>taak in het kader van de uitoefening van het openbaar gezag</i> dat aan de verwerkingsverantwoordelijke is opgedragen; ¹⁰⁹
(f) behartiging van de gerechtvaardigde belangen	... voor de <i>behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde</i> , behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene, zwaarder wegen dan die belangen (de hiervoor benodigde balansstoets moet zijn gedocumenteerd in een <i>legitimate impact assessment – LIA</i>). ¹¹⁰

3.2.2 Onderzoeker moet altijd rekening houden met overige AVG-verplichtingen

Daarnaast dienen de onderzoekers vanzelfsprekend aan alle overige toepasselijke AVG-verplichtingen te voldoen. Zo moeten de te gebruiken persoonsgegevens:

- tot een minimum worden beperkt (*'dataminimalisatie'*);
- juist zijn en indien nodig worden gecorrigeerd (*'juistheid'*);
- niet langer worden bewaard in identificerende vorm, gelet op de doelen waarvoor de gegevens zijn opgeslagen (*'opslagbeperking'*); en
- passend beveiligd zijn (*'integriteit en vertrouwelijkheid'*).¹¹¹

106 "of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen", aldus artikel 6 lid 1 sub b AVG.

107 Artikel 6 lid 1 sub c AVG.

108 Artikel 6 lid 1 sub d AVG.

109 Artikel 6 lid 1 sub e AVG.

110 Deze rechtsgrond geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken. Zie artikel 6 lid 1 sub f en laatste zin AVG.

111 Artikel 5 lid 1 sub c t/m f AVG.

Bovendien moet voor de betrokkene, zoals de patiënt, onder meer transparant zijn wat er met de gegevens gebeurt.¹¹² De verwerkingsverantwoordelijke – de persoon of entiteit die verantwoordelijk is voor de naleving van de AVG, hier: meestal de onderzoeker – moet kunnen aantonen dat hij voldoet aan de AVG-principes ('*verantwoordingsplicht*').¹¹³

Daarnaast maakt de AVG duidelijk dat het voldoen aan de regels over persoonsgegevens geen 'vinkje' achteraf is, maar van meet af aan moet worden meegenomen bij de opzet van het onderzoek vanwege het *data protection by design by default*-principe. **De AVG-principes dwingen onderzoekers ertoe om zowel voorafgaand als tijdens het onderzoek na te gaan hoe er gehandeld kan worden in lijn met de AVG.**

Tot slot zijn er ook andere verplichtingen, zoals:

- het naleven van toepasselijke gedragscodes;
- het sluiten van een overeenkomst met de hulpverleners, met daarin bijvoorbeeld afspraken over een veilige gegevensoverdracht en de mate van pseudonimisering; en
- een plicht om iedere onderzoeker contractueel aan geheimhouding te binden.

3.3 Internationaal onderzoek: datadoorgifte buiten EU

De AVG staat het toe dat gegevens voor onderzoek binnen de EU (en EER) de grenzen passeren. Zo kunnen bijvoorbeeld Nederlandse en Duitse onderzoekers samenwerken. Maar de regels voor medisch data-onderzoek kunnen per EU-land verschillen. Onder omstandigheden moeten onderzoekers rekening houden met die nationale regels van een ander EU-land, zoals dat in paragraaf 4.2.1 wordt uitgelegd. In deze paragraaf staan we stil bij onderzoeken waarvoor persoonsgegevens vanuit een EU-land, zoals Nederland, naar een land buiten de EU/EER worden 'geëxporteerd', zoals naar het Verenigd Koninkrijk (VK) of de Verenigde Staten van Amerika (V.S.).

Als het onderzoek inhoudt dat er persoonsgegevens vanuit de EU (inclusief de EER) worden geëxporteerd naar niet-EU/EER-landen, dan mag dit niet zomaar. De AVG hanteert namelijk het uitgangspunt dat landen buiten de EU/EER niet vanzelfsprekend hetzelfde beschermingsniveau bieden ten aanzien van gegevens. Het exporteren van persoonsgegevens buiten de EU/EER is dan ook verboden, bijvoorbeeld voor gegevensanalyse in dat land, tenzij de AVG voorziet in

112 Artikel 5 lid 1 sub c t/m f AVG.

113 Artikel 5 lid 2 AVG.

een mogelijkheid om dat verbod op te heffen. De volgende juridische mogelijkheden zijn denkbaar.

Het verbod op internationale gegevensexport kan worden opgeheven als het niet-EU-land een ‘adequaate beschermingsniveau’ biedt, zoals vastgesteld door de Europese Commissie. Landen als Argentinië, Israël en Zwitserland zijn zulke ‘adequate landen’.¹¹⁴ De AVG verhindert dus niet dat met deze landen onderzoeken worden verricht waarvoor persoonsgegevens uit de EU/EER worden gebruikt. Of het Verenigd Koninkrijk na 1 januari 2021 bestempeld zal worden als ‘adequaate’, is niet zeker.¹¹⁵ De V.S. zijn in ieder geval geen ‘adequaate land’, zodat gegevensexport naar dat land op een andere juridische mogelijkheid moet worden gebaseerd.

Tot voor kort mochten er gegevensverstrekkingen vanuit de EU/EER naar de V.S. plaatsvinden, zolang de ontvangende partij zich committeerde aan het zogeheten *Privacy Shield Framework*. Het gaat om in Amerika gevestigde bedrijven, waarvan mocht worden aangenomen dat ze zich aan de Europese privacystandaarden hielden. Op 16 juli 2020 heeft het Hof van Justitie in de *Schrems II*-zaak deze constructie ongeldig verklaard.¹¹⁶ Volgens het Hof biedt de Amerikaanse wet te weinig waarborgen voor EU-burgers wiens gegevens in de V.S. worden opgeslagen. Amerikaanse opsporingsdiensten bijvoorbeeld, zouden te gemakkelijk bij die data kunnen.

Met het wegvallen van *Privacy Shield* resteert er voor gegevensexport naar de V.S., en andere derde-landen zoals het VK, een andere mogelijkheid: de *Standard Contract Clauses* (SCC's). De SCC's betreffen een overeenkomst tussen de exporterende en de importerende partij, waarbij de gegevensimporteur contractueel verbonden is te handelen naar de Europese privacystandaarden. Als er SCC's zijn gesloten, is het verbod om persoonsgegevens buiten de EU/EER te exporteren, niet van toepassing.

Echter, de vraag is hoe praktisch SCC's zullen zijn voor onderzoekers. Ten eerste twijfelen juristen hardop of SCC's praktisch gebruikt kunnen worden voor gegevensexport naar de V.S. (Kuner 2020; Solove 2020). Volgens de SCC's moet de Amerikaanse importeur de Europese exporteur waarschuwen als hij meent dat de persoonsgegevens volgens de Europese standaarden niet beschermd kunnen worden. Dan mag de gegevensexport niet (meer) doorgaan.

114 European Commission, 'Adequacy decisions', https://ec.europa.eu/info/law/law-topic/dataprotection/international-dimension-data-protection/adequacy-decisions_en.

115 EURActiv, 'Commission uncertain on future UK data adequacy agreement', 24 juni 2020, <https://www.euractiv.com/section/data-protection/news/commission-uncertain-on-future-uk-data-adequacyagreement/>.

116 Hof van Justitie EU 16 juli 2020, C-311/18 (*Facebook Ireland en Schrems*).

Ook Duitse privacytoezichthouders menen dat het niet zomaar mogelijk is om SCC's te gebruiken voor gegevensexport naar de V.S. (DSK 2020; BlnBDI 2020). De EDPB heeft aangegeven hoe dit probleem opgelost kan worden, maar deze aanwijzingen zijn vooralsnog onderwerp van discussie (EDPB 2020).

Ten tweede speelt er een praktisch probleem. Ook al zouden SCC's gebruikt kunnen worden, dan zullen Amerikaanse publieke instellingen, zoals overheden en bepaalde universiteiten, deze niet altijd ondertekenen. De SCC's bepalen namelijk dat zij hun gegevenssystemen beschikbaar moeten houden voor audits door de Europese exporteurs. Daartoe zullen niet alle Amerikaanse publieke instellingen bereid zijn (Peloquin et al. 2020, Rabesandratana 2019).

Als SCC's niet kunnen of mogen worden afgesproken, of dat nu gaat om de V.S., het VK of een ander derde-land, dan biedt de AVG specifieke mogelijkheden die de internationale data-doorgifte mogelijk kunnen maken. Bijvoorbeeld als de doorgifte noodzakelijk is wegens gewichtige redenen van algemeen belang, of als de patiënt met de gegevensexport uitdrukkelijk heeft ingestemd.¹¹⁷ **Dit zijn specifieke situaties waarvan eerst goed onderzocht moet worden of deze de vereiste juridische houvast bieden.** Zulke situaties kunnen bijvoorbeeld een rol spelen bij internationale-dataverstrekking ter bestrijding van de wereldwijde COVID-19 crisis, maar liggen minder voor de hand bij regulier grensoverschrijdend onderzoek (EDPB Guidelines 3/2020). Het gaat hier telkens om noodzakelijke incidentele gegevensverstrekkingen naar een land buiten de EU/EER. **Voor algemeen medisch data-onderzoek dat pas op enig moment in de toekomst resultaten zal opleveren, zullen deze mogelijkheden waarschijnlijk niet geschikt zijn** (MinVWS 2020b).

Mocht internationaal onderzoek juridisch mogelijk zijn, dan wordt zowel vanuit de WGBO (paragraaf 3.1.1), als vanuit de AVG verwacht, dat de patiënt hierover geïnformeerd is. Volgens de AVG moet dan ook worden uitgelegd welke juridische basis hiervoor wordt gebruikt: een adequaatheidsbesluit van de Commissie, SCC's of een andere basis zoals uitdrukkelijke instemming van de patiënt.

3.4 Tot slot

De wetgeving voor gebruik van gegevens uit medische dossiers voor nWMO-onderzoek is zo opgesteld, dat belangrijke rechten worden beschermd. De wetgeving is aardig complex. Voor de hulpverlener – als poortwachter van de medische dossiergegevens – is steeds de belangrijkste vraag: “Mag ik de data

verstrekken aan de onderzoeker die nWMO-onderzoek wil doen en moet daarvoor nog toestemming worden gevraagd aan de patiënt?” En de onderzoeker moet zichzelf steeds afvragen: “Mag de hulpverlener de gegevens verstrekken en welke extra stappen moet ik nog ondernemen om de gegevens te mogen gebruiken voor het onderzoek?” Onderzoeker en hulpverlener hebben beiden de plicht om secuur na te gaan of ze volgens de wet handelen. Ze kunnen daarbij samen optrekken. De (U)AVG vraagt daarnaast aan onderzoekers extra waarborgen bij het uitvoeren van het onderzoek.

Zoals we in hoofdstuk 4 zullen schetsen, bestaan er flink wat knelpunten voor zowel de hulpverlener als de onderzoeker:

- bij interpretatie van de wetgeving;
- bij internationaal onderzoek;
- bij anonimiseren en pseudonimiseren;
- bij toestemming vragen (of niet); en
- bij betrokkenheid van commerciële partijen.

4 Knelpunten die datasolidariteit in de weg staan

Digitale gegevens uit medische dossiers kunnen van nut zijn voor het verbeteren van de zorg en volksgezondheid. Daarover zijn partijen het wel eens. Onder de noemer 'nWMO-onderzoek' kan door onderzoekers – binnen en buiten de muren van de instituten van de hulpverleners – allerlei nuttig onderzoek worden gedaan. Bijvoorbeeld medische statistieken beschrijven per regio (denk aan COVID-19-besmettingen), effecten van screeningsbeleid onderzoeken (denk aan de impact van bevolkingsscreening naar darmkanker op de sterftcijfers voor die ziekte), verbanden onderzoeken tussen bepaalde verklarende variabelen en uitkomsten (denk aan kenmerken of medicatie van de patiënt en duur van de ziekenhuisopname bij specifieke ziekten) of innovaties in de zorg ontwikkelen (denk aan beslissystemen die ondersteunen bij het stellen van diagnoses op basis van beeldmateriaal van weefsel van de patiënt).

Informatie over hun gezondheid krijgen burgers inmiddels al lang niet meer alleen van hun arts of andere hulpverlener. Via zogenoemde *wearables* kunnen ze bijvoorbeeld hun eigen hartslag, lichaamstemperatuur, slaap- en voedingspatronen meten. Ook laten burgers zelf hun DNA-materiaal analyseren bij commerciële bedrijven. Zij kunnen de door hen zelf vergaarde gezondheidsinformatie inbrengen bij de behandeling. Ook extra communicatiegegevens tussen hulpverlener en patiënt, bijvoorbeeld bij *blended care* in de GGZ, worden in zekere zin toegevoegd aan het medische dossier. Gezondheidsinformatie vertelt veel over een persoon en kan anderen macht geven over een individu. Huidige of toekomstige werkgevers, verzekeraars en overheden kunnen burgers ermee profileren en mogelijk stigmatiseren of uitsluiten. Daarom is het zo belangrijk dat de wetgever strikte regels heeft opgesteld voor het beschermen van medische gegevens, zeker nu technologie nieuwe bronnen van gezondheidsinformatie aanboort en commerciële spelers binnen het zorgdomein treden.

Sterke basis voor datasolidariteit

De wetgeving is zo opgesteld, dat belangrijke fundamentele rechten in principe worden beschermd. Voor onderzoek met medische gegevens uit behandeldossiers spelen met name de volgende rechten een rol:

- de **bescherming van persoonsgegevens**;
- de **eerbiediging van het privéleven**; en
- de **wetenschapsvrijheid**.

Het 'medisch beroepsgeheim' is op zichzelf geen fundamenteel recht, maar Nederland moet hier als verdragsstaat wel voor zorgen en het hangt samen met het fundamentele **recht op toegang tot gezondheidszorg**.

Uit hoofdstuk 3, waar we de hulpverlener en de onderzoeker stap voor stap langs de wetgeving leidden (zie ook de stroomdiagrammen in Bijlagen 4 en 5), bleek dat de wetgeving die het gebruik van gegevens uit medische dossiers voor nWMO-onderzoek regelt, specifieke voorwaarden stelt aan de verstrekking van gegevens voor onderzoek. Voor de hulpverlener was daarbij de belangrijkste vraag: "Mag ik de data verstrekken aan de onderzoeker die nWMO-onderzoek wil doen en moet daarvoor nog toestemming worden gevraagd aan de patiënt?" En voor de onderzoeker was de belangrijkste vraag "Mag de hulpverlener de gegevens verstrekken en welke extra stappen moet ik nog ondernemen om de gegevens te mogen gebruiken voor het onderzoek?"

In hoofdstuk 4 zullen we eerst de belangrijkste stappen en overwegingen van hulpverlener en onderzoeker nog kort samenvatten. Vervolgens beschrijven we de knelpunten per deelvraag. Daarna volgt een paragraaf met 'goede voorbeelden' uit andere landen, in aanloop naar hoofdstuk 5 (conclusies en oplossingsrichtingen).

De lijst met knelpunten is geenszins een limitatieve lijst. In de loop der jaren hebben juristen meermaals gepubliceerd over de regels en mogelijke vraagstukken. Onderstaande selectie is vooral gebaseerd op terugkerende knelpunten, genoemd in recente bronnen zoals nieuwsberichten en literatuur. Maar ook onze eigen observaties zijn opgenomen.

4.1 Wetgeving voor nWMO-onderzoek in een notendop

De wet- en regelgeving voor gebruik van gegevens uit medische dossiers voor nWMO-onderzoek zijn uitgebreid toegelicht in hoofdstuk 3. We vatten ze hier nog kort samen, zodat de knelpunten en oorzaken daarvan vervolgens duidelijker kunnen worden geschetst.

De belangrijkste overwegingen voor de **hulpverlener**, ingegeven door de WGBO, zijn:

- Het **initiatief** tot verzoek om gegevensverstrekking behoort uit te gaan van de onderzoeker.
- **Aan de patiënt toestemming vragen is het uitgangspunt:** als nWMO-onderzoekers inzage willen of een kopie van de gegevens uit het medisch dossier, dan moet hiervoor in principe de toestemming van de patiënt

worden gevraagd. Voor eigen onderzoek door de hulpverlener hoeft dat niet.

- Toestemming moet in ieder geval **expliciet en voldoende specifiek** zijn. De patiënt moet daarbij met een redelijke mate van nauwkeurigheid kunnen overzien waartoe zijn toestemming strekt.
- Verstrekking van gegevens over patiënten of inzage in patiëntdossiers aan nWMO-onderzoekers is in bepaalde situaties **toegestaan zónder toestemming van de patiënt** als het onderzoek valt onder de noemer van **statistiek of wetenschappelijk onderzoek** op het gebied van de **volksgezondheid** én daarbij een **algemeen belang** dient.
- In bovenstaand geval moet te allen tijde onderzocht worden of het inderdaad **mogelijk is om af te wijken van de hoofdregel** 'toestemming vragen van de patiënt'. De wet omschrijft **twee situaties waarin toestemming vragen niet hoeft**. Eén van deze situaties moeten aan de orde zijn, anders mag er geen verstrekking van de gegevens zonder toestemming plaatsvinden:
 - toestemming vragen is in redelijkheid niet mogelijk en/of
 - toestemming vragen kan in redelijkheid niet worden verlangd.
- **Deze uitzonderingen op het beginsel dat toestemming nodig is, kennen als eis** dat de te verstrekken extra gegevens beschermd worden, bijvoorbeeld door codering. Hiervan kan worden afgeweken als direct herleidbare persoonsgegevens voor het onderzoek noodzakelijk zijn, en als toestemming in redelijkheid niet mogelijk is en er wordt voorzien in zodanige waarborgen, dat de persoonlijke levenssfeer niet onevenredig wordt geschaad.
- Tot slot zijn er nog twee belangrijke voorwaarden waaraan moet worden voldaan om de gegevens voor nWMO-onderzoek te mogen gebruiken:
 - **Het onderzoek kan niet zonder de desbetreffende gegevens uitgevoerd worden**, bijvoorbeeld op een andere manier die minder ingrijpend is ten aanzien van de rechten en belangen van de patiënt;
 - De patiënt heeft **geen uitdrukkelijk bezwaar** gemaakt tegen de verstrekking. Hulpverleners moeten een **geen-bewaarsysteem** inrichten. Als patiënten niet op de hoogte zijn gesteld van het feit dat de gegevens uit hun dossier voor statistiek of wetenschappelijk onderzoek gebruikt konden worden, of als er geen bezwaarmogelijkheid is geweest, dan mogen die gegevens niet worden verstrekt voor onderzoek. De **informatieplicht over het geenbezwaar-systeem** richting de patiënt rust op de hulpverlener die de gegevens aanlevert, maar het ligt voor de hand dat de onderzoekers daarbij een ondersteunende rol spelen.
- Als de gegevens worden verstrekt voor onderzoek, of inzage wordt verleend in het dossier voor onderzoek, dan **maakt de hulpverlener hiervan aantekening in het medisch dossier**.

De belangrijkste overwegingen voor de **onderzoeker**, vooral ingegeven door de AVG en UAVG zijn:

- Kan met zekerheid worden vastgesteld of **de hulpverlener de gegevens had mogen verstrekken**? Als dat niet het geval is, dan mogen de gegevens niet worden gebruikt.
- Verstrekkt de hulpverlener de gegevens op basis van toestemming van de patiënt of op basis van de mogelijkheid die de WGBO biedt voor statistiek of wetenschappelijk onderzoek? Als de verstrekking plaatsvindt op basis van toestemming, dan is van belang dat de onderzoeker de gegevens **niet gebruikt buiten de reikwijdte van de gegeven toestemming**. Overigens geeft de wetgever van de (U)AVG, net als de WGBO-wetgever, de voorkeur aan het vragen van toestemming.
- De UAVG **heft voor de onderzoeker het verbod op** om bijzondere persoonsgegevens, zoals gezondheidsgegevens of genetische gegevens, te gebruiken, als aan bepaalde **eisen** is voldaan:
 - het gegevensgebruik moet **noodzakelijk** zijn met het oog op **wetenschappelijk onderzoek of statistische doeleinden**;
 - het onderzoek moet een **algemeen belang** dienen;
 - het vragen van uitdrukkelijke **toestemming mag alleen achterwege** blijven als het onmogelijk blijkt of een onevenredige inspanning kost;
 - bij de uitvoering van het onderzoek is voorzien in zodanige waarborgen, dat de **persoonlijke levenssfeer** van de patiënt niet onevenredig wordt geschaad. Het coderen van gegevens is zo'n waarborg, maar er zijn meer maatregelen denkbaar. Ook moeten de onderzoekers ervoor zorgen dat zoveel mogelijk voorkomen wordt, dat de gegevens worden gebruikt voor het nemen van maatregelen of besluiten die *tegen* een patiënt gericht zijn.
- De onderzoekers dienen erop bedacht te zijn, dat zij nog steeds een rechtsgrond voor het gegevensgebruik nodig hebben op basis van de AVG: zij moeten worden gebruikt voor een **gerechtvaardigd (onderzoeks)doel** en zorgen dat dit **rechtmatig** gebeurt. Zij moeten daarom een **rechtsgrond** hebben.
- **Daarnaast dienen de onderzoekers vanzelfsprekend aan alle overige toepasselijke AVG-verplichtingen te voldoen.** Zo moeten de te gebruiken persoonsgegevens:
 - tot een minimum worden beperkt (*'dataminimalisatie'*);
 - juist zijn en waar nodig worden gecorrigeerd (*'juistheid'*);
 - niet langer worden bewaard in identificerende vorm, gelet op de doelen waarvoor de gegevens zijn opgeslagen (*'opslagbeperking'*);
 - en
 - passend beveiligd zijn (*'integriteit en vertrouwelijkheid'*).

Bovendien moet voor de betrokkene, zoals de patiënt, onder meer **transparant** zijn wat er met de gegevens gebeurt. De verwerkingsverantwoordelijke – de persoon of entiteit die verantwoordelijk is

voor de naleving van de AVG (lees: meestal de onderzoeker) – moet kunnen aantonen dat hij voldoet aan de AVG-principes ('*verantwoordingsplicht*').

- Daarnaast maakt de AVG duidelijk, dat bij de opzet van het onderzoek het ***data protection by design by default-principe*** geldt: onderzoekers moeten zowel voorafgaand als tijdens het onderzoek nagaan hoe er gehandeld kan worden in lijn met de AVG. maakt de AVG duidelijk, dat bij de opzet van het onderzoek het ***data protection by design by default-principe*** geldt: onderzoekers moeten zowel voorafgaand als tijdens het onderzoek nagaan hoe er gehandeld kan worden in lijn met de AVG.

4.2 Knelpunten en hun oorzaken

De stappen die de hulpverlener en de onderzoeker moeten langslopen zijn in principe helder, maar toch zijn er vaak klachten over onduidelijkheid van de wetgeving. De **centrale vraag** in ons onderzoek luidt: **“Wat zijn mogelijke oplossingen voor de knelpunten rond wet- en regelgeving, zoals die nu worden ervaren bij het doen van nWMO-onderzoek?”** Hieronder zullen we de knelpunten en hun oorzaken schetsen.

In deze paragraaf rangschikken we de **knelpunten over drie thema's, direct gerelateerd aan de deelvragen**:

1. Is de kritiek op de huidige wetgeving bij nWMO-onderzoek terecht, of is er sprake van veronderstelde belemmeringen in plaats van werkelijke belemmeringen? Zijn er extra belemmeringen voor internationaal nWMO-onderzoek? Welke dan?
2. Welke extra kwesties doen zich voor bij nieuwe technologische ontwikkelingen – vaak gefaciliteerd door commerciële partijen – zoals kunstmatige intelligentie, zelfmetingen door patiënten met wearables en digitale communicatie tussen patiënt en hulpverlener? Mogen technologische bedrijven toegang hebben tot de gegevens uit medische dossiers, zelfs voor *for profit* onderzoek?
3. Zijn de regels rond het krijgen van toestemming van de patiënt helder genoeg of kan dat beter?

4.2.1 Knelpunten die hun oorzaak in de (internationale) wetgeving vinden

Een klacht die onderzoekers soms uiten is dat de **AVG de ruimte voor doen van onderzoek inperkt**. Ook zouden de AVG en WGBO niet altijd op één lijn liggen. Een punt waarop de wetgeving eigenlijk niet meer van deze tijd lijkt, is de eis dat onderzoekers, en niet de hulpverlener, het **initiatief voor onderzoek** moeten nemen. Verder is uit recent onderzoek naar voren gekomen dat onderzoekers knelpunten ervaren met betrekking tot de **voorwaarden waaronder gegevens geanonimiseerd gebruikt mogen worden en waaronder gegevens gepseudonimiseerd mogen worden** (Ministerie VWS 2020a). Ook bestaat er **onduidelijkheid over de betekenis van die begrippen**.

Het is begrijpelijk dat er onduidelijkheid bestaat over juridische begrippen onder doorgaans niet-juridisch geschoolden, zoals hulpverleners en onderzoekers. De stroomdiagrammen (Bijlagen 4 en 5) in samenhang met hoofdstuk 3 trachten hen door de juridische regels heen te leiden, maar knelpunten blijven onvermijdelijk. Tot slot blijkt het lastig om te voldoen aan de regels voor **internationaal onderzoek**. We bespreken de knelpunten één voor één.

Knelpunt 1. Wetgeving vraagt flinke inspanningen bij doen van nWMO-onderzoek

Nieuwe uitdagingen

Veel gehoord onder onderzoekers is de stelling, dat de AVG onderzoek, waaronder nWMO-onderzoek, (te) vergaand aan banden legt. Toch is het niet zo dat de AVG inhoudelijk méér eisen stelt aan onderzoek met persoonsgegevens dan voorheen. In Nederland is ervoor gekozen om de AVG 'beleidsneutraal' in te voeren. Dat wil zeggen, dat de normen die ook onder de Wet bescherming persoonsgegevens (Wbp) golden, zijn overgenomen in nationale wetgeving. De **AVG legt onderzoek niet verder aan banden ten opzichte van de regels die golden vóór de invoering van deze verordening** (Ploem et al. 2020, Dove 2018, Mostert 2017).

Wel is het zo dat de AVG **nieuwe uitdagingen** met zich meebrengt die voorheen niet of slechts als '*best practice*' golden. Denk aan de verplichte aanstelling van een Functionaris Gegevensbescherming (FG), het uitvoeren van een Data Protection Impact Assessment (DPIA), het bijhouden van een verwerkingenregister, of het documenteren van de maatregelen die de organisatie heeft genomen en de overwegingen daarbij om zo te voldoen aan de verantwoordingsplicht (paragraaf 3.2.2). Organisaties die hier niet op voorbereid zijn (geweest), zullen de AVG vooral als een organisatorische last ervaren.

De Uitvoeringswet AVG (UAVG) ten slotte, legt onderzoek evenmin verder aan banden. De UAVG introduceert een nieuw wetsartikel over genetische gegevens, maar de bepalingen daarover haken aan bij het bestaande systeem voor onderzoek met bijzondere gegevens (paragraaf 3.2).

Extra lastig voor kleine spelers

De WGBO en de UAVG vragen van hulpverleners en onderzoekers de nodige inspanningen om na te gaan of het beoogde onderzoek aan de wettelijke vereisten voldoet. Zoals we hebben gezien in hoofdstuk 3, is deze taak niet ondoenlijk, maar zeker niet eenvoudig. **Sommige categorieën van hulpverleners en onderzoekers worden ondersteund worden door experts die hen helpen bij het maken van de juiste afwegingen.** Bijvoorbeeld een toetsingscommissie van een ziekenhuis waar de hulpverlener werkt, of een onderzoeksprotocol waarop de onderzoeker kan bouwen.

Er is sprake van een ‘**dubbele zorgplicht**’.¹¹⁸ Enerzijds dient de hulpverlener die de gegevens verstrekt aan de onderzoeker daaraan passende voorwaarden te verbinden omtrent het verdere gebruik, waaronder verstrekking aan andere onderzoekers (paragraaf 3.1). Anderzijds rusten op de onderzoeker verplichtingen met betrekking tot een zorgvuldige omgang met de aan hem ter beschikking gestelde persoonsgegevens (paragraaf 3.2). In dat laatste geval speelt de (U)AVG een belangrijke rol. De onderzoeker moet nagaan of hij voldoet aan de (U)AVG, maar hij moet er ook op kunnen vertrouwen, dat de hulpverlener de gegevens had mogen verstrekken of inzage had mogen verlenen in de gegevens.

De door de hulpverlener te maken beoordeling is niet eenvoudig. De WGBO-voorwaarden laten een zekere ruimte voor interpretatie, omdat er een afweging moet worden gemaakt tussen de persoonlijke levenssfeer en het belang van het wetenschappelijk onderzoek.¹¹⁹ **De vraag is, of van een hulpverlener die niet de ‘luxe’ heeft van expert-ondersteuning, bijvoorbeeld een zelfstandige huisarts, diëtist of optometrist, verlangd mag worden dat hij/zij een gedegen beoordeling maakt of aan de criteria voor gegevensverstrekking wordt voldaan.**¹²⁰ Een verkeerde beoordeling kan grote gevolgen hebben. De hulpverlener kan bijvoorbeeld civiel- of tuchtrechtelijk worden aangesproken, omdat het medisch beroepsgeheim in het geding kan zijn. Ook hebben toezichthouders als de IGJ en de Autoriteit Persoonsgegevens handhavende bevoegdheden (paragraaf 1.1.3).

118 *Nadere Memorie van Antwoord WGBO*, p. 45.

119 *Memorie van Antwoord WGBO*, p. 67.

120 *Memorie van Antwoord WGBO*, p. 41 en 66.

Het is denkbaar dat een hulpverlener zonder inhoudelijke ondersteuning een verzoek om gegevens daarom veiligheidshalve afwijst. Kansen met gezondheidsgegevens blijven hierdoor liggen. Een knelpunt is dus, dat gegevens die verstrekt hadden mogen worden, achter een gesloten (digitale) dossierkast blijven. Het spiegelbeeld is ook een knelpunt: de situatie waarin gegevens verstrekt worden, terwijl dit achteraf gezien niet mocht.

Knelpunt 2: Spanningsveld tussen WGBO en (U)AVG

De verhouding tussen de UAVG en de WGBO leidt tot discussie. Er rijzen namelijk diverse vragen naar aanleiding van opmerkingen die zijn gedaan onder de oude Wbp-regeling in het licht van de huidige UAVG-regels. Het Rathenau Instituut kaartte dit spanningsveld al aan in een brief aan minister Dekker als reactie op de Verzamelwet gegevensbescherming op 14 juli 2020 (Rathenau Instituut 2020a). We zetten de vragen hieronder nogmaals op een rij.

Hoe rekbaar is het begrip ‘onmogelijk’?

Onder de Wbp was duidelijk dat met de eis met betrekking tot de onmogelijkheid voor het vragen van *toestemming* (paragraaf 3.2.1, C), hetzelfde werd bedoeld als met de feitelijke onmogelijkheid van het *informer* van de patiënt over het onderzoek. De EDPB vindt, dat die laatstgenoemde verplichting, over de informatievoorziening, een alles-of-niets-situatie betreft: **er zijn geen gradaties van onmogelijkheid** (EDPB Guidelines 03/2020). De Wbp-normen zijn overgenomen in de UAVG, waardoor de opvatting van de EDPB ook voor de huidige situatie relevant is.

Hoe moeten we de EDPB-opvatting, die geldt in de context van de UAVG, zien ten opzichte van de WGBO? In paragraaf 3.3. is uiteengezet dat uit de WGBO volgt, dat toestemming *niet* feitelijk onmogelijk hoeft te zijn.¹²¹ Omwille van de praktische uitvoerbaarheid moet voorkomen worden, dat er situaties ontstaan waarin er onder de WGBO *geen* en onder de UAVG *wel* toestemming gevraagd moet worden voor onderzoek.

Wel of niet publiceren?

Een vergelijkbare vraag doemt op met betrekking tot de wel of niet bestaande verplichting tot publiceren. Een verplichte publicatie kan lastig zijn, omdat niet altijd op voorhand vast te stellen is of onderzoek tot een publicatie leidt (paragraaf 3.1.2, punt C). Toch vermeldt een Handreiking van het RIVM onomwonden dat “*de resultaten publiek beschikbaar [dienen] te komen*” (RIVM 2019). Voormalig minister Bruins verwachtte eveneens publicatie over het onderzoek en de

121 *Memorie van Antwoord WGBO*, p. 67. *Nota n.a.v. het Eindverslag WGBO*, p. 35.

resultaten (paragraaf 3.1.2). Deze uitspraak deed hij in de context van de UAVG, maar de norm uit het betreffende UAVG-artikel over het ‘algemeen belang’ – op basis waarvan publicatie verplicht zou zijn – is dezelfde norm als uit de WGBO.¹²² Betekent dit dat publicatie volgens de WGBO en UAVG altijd verplicht is? De AVG lijkt publicatie niet te verplichten, maar geeft aan dat wetenschappelijk onderzoek aan bepaalde voorwaarden dient te voldoen, zoals voorwaarden over publicatie.¹²³

Is de WGBO ‘AVG-proof’?

Tot slot blijft een grote vraag vooralsnog onbeantwoord: **hoever mag de nationale wetgever gaan bij het opstellen van regels voor onderzoek met patiëntgegevens (binnen de kaders van de AVG)?** De AVG erkent expliciet dat gezondheidsgegevens en genetische gegevens mogen worden verwerkt op basis van nationaal recht, als dit noodzakelijk is voor wetenschappelijke of statistische doeleinden. Volgens Ploem et al. 2020 betekent dit dat Nederland een eigen invulling mag geven aan ‘toestemming’ in de WGBO. Volgens hen is de WGBO-toestemming iets anders dan de toestemming volgens de AVG.¹²⁴ Is dit juist? De AVG vermeldt expliciet dat nationale regelingen zoals de WGBO de wezenlijke inhoud van het recht op de bescherming van persoonsgegevens moeten eerbiedigen (zie paragraaf 1.2.1).¹²⁵ **Dit impliceert dat er geen plaats is voor een WGBO die voorwaarden van toestemming bevat, die afwijken van de AVG-voorwaarden.**

Als het juist is wat Ploem et al. 2020 stellen, namelijk dat de WGBO een eigen invulling mag geven (en geeft) aan ‘toestemming’, dan rijst de vraag of dat wel is toegestaan volgens de AVG. Met andere woorden: is de WGBO ‘AVG-proof’? In het licht van deze vraag zet **knelpunt 9** uiteen, of het mogen vragen van een ‘brede’ toestemming wel of niet de bedoeling is.

Knelpunt 3: Initiatief tot onderzoek alleen bij de onderzoeker is achterhaald

Volgens de WGBO dient het initiatief tot gegevensverstrekking uit te gaan van de onderzoeker. Hoe strikt geldt deze eis? Hulpverleners kunnen immers ook onderzoeksinitiatieven ontplooien die breder gaan dan ‘eigen onderzoek’. Zij

122 *Memorie van Toelichting Wbp* bij artikel 23 lid 2 Wbp (=24 UAVG, zie par. 3.2.1 A t/m D): “Onderdeel a vergt dat het onderzoek een algemeen belang moet dienen. Deze eis komt overeen met artikel 7:458 BW. Waar de bepaling in het BW als *lex specialis* zijn gelding behoudt voor de daar bedoelde gegevens, is dit onderdeel van de regeling van de BW in dit wetsvoorstel overgenomen voor bijzondere gegevens in het algemeen.

123 Overweging 159 AVG: “Om als verwerking van persoonsgegevens met het oog op wetenschappelijk onderzoek te worden aangemerkt, moet de verwerking aan specifieke voorwaarden voldoen, met name wat betreft het publiceren of anderszins openbaar maken van persoonsgegevens voor wetenschappelijke onderzoeksdoeleinden.”

124 Artikel 7 en artikel 9 (“uitdrukkelijke toestemming”) AVG.

125 Artikel 9 lid 1 sub j, slot AVG. De UAVG-wetgever schrijft in de wetstoelichting: “De materiële normen voor gegevensverwerking zullen rechtstreeks volgen uit de AVG en mogen niet langer in nationale wetgeving worden vastgelegd. De bestaande nationale normen zijn hiermee betekenisloos geworden en moeten worden geschrapt.” *Memorie van Toelichting UAVG*, p. 14.

kunnen hiervoor derden-onderzoekers inschakelen. Zijn zulke initiatieven niet zomaar toegestaan? Het lijkt niet meer van deze tijd om dit zo te houden.

Knelpunt 4: Onduidelijkheden en onwettige handelingen bij anonimisering en pseudonimisering

Misverstand dat anonimiseren altijd moet

De WGBO en de (U)AVG verlangen geen anonimisering van gegevens als daardoor het onderzoek niet kan plaatsvinden, zolang het eindresultaat van het onderzoek geen herleidbare gegevens bevat. Anonimiseren zou vanuit dat perspectief geen knelpunt mogen zijn voor nWMO-onderzoek.¹²⁶ Toch zijn er veel onderzoekers, of zelfs experts als FG's (Ministerie VWS 2020a), die denken dat anonimiseren altijd moet.

Anonimiseren van gegevens wordt gezien als een methode om het onderzoek volledig te onttrekken aan de regels van de (U)AVG

De Handreiking van het RIVM vermeldt bijvoorbeeld: *“Is er geen toestemming én is er geen systeem van ‘geen bezwaar’? Dan is anonimiseren een mogelijkheid om de gegevens toch te gebruiken. Anonieme gegevens vallen namelijk niet onder de AVG.”* (RIVM 2019). Een vergelijkbare uitspraak is te vinden op een website van het Ministerie van Volksgezondheid, Welzijn en Sport. Als antwoord op de vraag *“Gelden er minder strenge regels als ik kan anonimiseren?”* meldt de website: *“ja, de AVG is niet van toepassing als gegevens uit bijvoorbeeld een patiëntendatabase zijn geanonimiseerd.”*¹²⁷

Het is risicovol om blind te varen op deze uitspraken. Het **anonimiseren** van persoonsgegevens is, net als bijvoorbeeld het vernietigen van gegevens, een **verwerkingshandeling waarop de AVG van toepassing is**. Dit betekent dat hiervoor een rechtsgrond nodig is én – als het gaat om het anonimiseren van bijzondere persoonsgegevens – een opheffingsmogelijkheid (Bijlage 1). Niet is vereist, dat de verwerkingsverantwoordelijke – meestal de onderzoeker – zelf de persoonsgegevens verwerkt, bijvoorbeeld door deze in herleidbare vorm te ontvangen of te analyseren. Daarom oordeelde het Europees Hof van Justitie, dat de beheerder van een Facebook Fanpage-site *verantwoordelijk* was voor het door Facebook laten anonimiseren van statistieken over het websitebezoek, ook al ontving de beheerder zelf geen herleidbare gegevens.¹²⁸ Dit betekent dat als een onderzoeker (of een andere derde partij, zoals de aanbieder van een AI-tool) een hulpverlener verzoekt om gegevens te anonimiseren, de verzoeker hiervoor een

126 Nota n.a.v. het Eindverslag WGBO, p. 9 en pp. 33 – 34. “Wij onderkennen (...) het feit dat geanonimiseerde gegevens zich lang niet altijd lenen voor wetenschappelijk onderzoek.”

127 Ministerie van VWS, ‘Gelden er minder strenge regels als ik kan anonimiseren?’, <https://www.datavoorgezondheid.nl/wegwijzer-ai-en-corona/vraag-en-antwoord/gelden-er-minder-strenge-regels-als-ik-kan-anonimiseren>.

128 Hof van Justitie EU 5 juni 2018, C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*).

wettelijke grondslag moet hebben. Dit hoeft geen probleem te zijn, zolang aan de WGBO en (U)AVG-vereisten worden voldaan (paragrafen 3.1 en 3.2). **Maar als deze vereisten *niet* zijn ingevuld en er ook geen toestemming is gevraagd om de gegevens (geanonimiseerd) te mogen verstrekken, dan ontstaat er een juridisch knelpunt.** Immers, op basis van welke rechtsgrond en opheffingsmogelijkheid zouden de patiëntgegevens (geanonimiseerd) verstrekt mogen worden? Hierop blijft de RIVM-handreiking het antwoord schuldig. De website van het ministerie zou het meer precies kunnen uitdrukken: “Ja, de AVG is niet *meer* van toepassing als gegevens uit bijvoorbeeld een patiëntendatabase zijn geanonimiseerd.”

De WGBO beschermt gegevens onvoldoende in het anonimiseringsproces

De WGBO-wetgever stelde begin jaren '90 dat de WGBO-regeling voor onderzoek (paragraaf 3.1) *niet* geldt, als de te verstrekken gegevens geen persoonsgegevens bevatten.¹²⁹ De wetgever deed deze uitspraak onder de voorloper van de Wbp (en de UAVG), de Wet persoonsregistraties (Wpr) uit 1989. Kennelijk was de wetgever in de veronderstelling, dat in zo'n geval er geen reden was om de gegevens te beschermen, omdat de Wpr die bescherming ook niet bood. Het idee was, dat de WGBO-regels pas golden als de betreffende gegevens persoonsgegevens waren onder de Wpr. **De vraag is, of de wetgever 30 jaar geleden zich gerealiseerd heeft, dat onder de AVG gegevens ook beschermd worden voor en tijdens het anonimiseringsproces**, zoals beschreven bij knelpunt 6. Met andere woorden, de WGBO zou – net als de (U)AVG – van toepassing moeten zijn op de gegevens totdat ze anoniem zijn.

In de praktijk wordt niet altijd aan de voorwaarde van pseudonimisering voldaan

Duidelijk is dat als gegevens aan personen gekoppeld kunnen worden, deze onder de AVG en WGBO vallen (paragraaf 1.2.1). **Gecodeerde gegevens**, die aan de orde zijn als het vragen van toestemming in redelijkheid niet kan worden verlangd (paragraaf 3.1.3), dienen als (**gepseudonimiseerde**) persoonsgegevens te worden beschouwd. Hoewel deze gegevens zijn ontdaan van persoonsidentificerende kenmerken zoals geboortedatum, naam en patiëntnummer, blijft re-identificatie mogelijk, omdat een derde-partij zoals de *trusted third party* het sleutelbestand beheert. Op basis van dat bestand kunnen de gecodeerde, gepseudonimiseerde, gegevens herleid worden naar personen. De voorwaarden voor pseudonimiseren

129 ‘[De WGBO-bepaling over gegevensverstrekking of inzage voor onderzoek] is alleen van belang in de gevallen waarin niet kan worden volstaan met het verstrekken van gegevens die redelijkerwijs niet – d.w.z. in het geheel niet of slechts met onevenredige moeite of kosten – herleidbaar zijn tot de persoon van de patiënt.’, aldus de wetgever. Zie: Tweede Kamer, vergaderjaar 1989-1990, 21 561, nr. 3, *Memorie van Toelichting WGBO*, p. 40. In gevallen waarin niet-herleidbare gegevens worden verstrekt, is geen privacybescherming meer nodig zo blijkt uit antwoorden van de wetgever op vragen van Tweede Kamerleden. Het gaat immers om informatie die niet aan welke persoon dan ook kan worden gekoppeld, zo luidde de opvatting. Zie: Tweede Kamer, vergaderjaar 1990-1991, 21 561, nr. 6, *Memorie van Antwoord WGBO*, pp. 65 – 66. De wetgever lijkt hier voorbij te gaan aan de risico's op re-identificatie, zoals beschreven in paragraaf 1.3.1 van ons rapport.

staan in de AVG. Uit een onderzoek uit 2016, uitgevoerd in opdracht van het Ministerie van VWS, blijkt dat **in de praktijk niet altijd aan de voorwaarden van pseudonimisering worden voldaan** (PBLQ 2016). De onderzoekers constateren bijvoorbeeld dat niet alle organisaties de sleutels voor het pseudonimiseren goed hebben beschermd.

Knelpunt 5: Voldoen aan de regels voor internationaal onderzoek is complex

Onderzoekers klagen erover, dat de AVG onderzoek hindert bij samenwerking tussen EU-landen en daarbuiten. Dat is niet verwonderlijk. Voor onderzoeken **binnen de EU** geldt, dat ieder EU-land eigen wet- en regelgeving mag opstellen voor onderzoeken met medische data.¹³⁰ De Nederlandse regeling staat in de WGBO tezamen met artikel 24 van UAVG.¹³¹

De regels binnen de EU voor onderzoek met medische gegevens kunnen per land verschillen. En dus genieten betrokkenen, zoals patiënten, niet in iedere lidstaat dezelfde rechten. Zo mag in Nederland het recht van bezwaar niet beperkt worden, terwijl dat in 16 andere EU-landen dat wel mag, bijvoorbeeld in België en Duitsland (Piechaud-Boura & Dumortier 2018). Ook bestaan er uiteenlopende eisen binnen de EU met betrekking tot de te nemen maatregelen, zoals pseudonimisering. Daarnaast verplichten sommige landen goedkeuring van een ethische commissie, alvorens het onderzoek gestart mag worden. Een door de Europese Commissie gesponsord project heeft de nationale verschillen onderzocht en concludeert: “*Rules applying to processing of health data for scientific research purposes remain complex and differentiated across the EU.*” (Piechaud-Boura & Dumortier 2018). **In een EU-breed onderzoek moet per land worden nagegaan wat de nationale regels zijn en hoe daaraan kan worden voldaan.** Dat is tijdrovend en kostbaar.

De AVG staat onder voorwaarden gegevensverstrekking toe aan ontvangers in landen **buiten de EU/EER**, maar ook dit is niet eenvoudig. Publieke (onderzoeks)instellingen in de VS bijvoorbeeld, zullen doorgaans geen SCC's ondertekenen. Ook is het de vraag of SCC's gebruikt kunnen worden, naar aanleiding van de uitspraak van het Europees Hof in de *Schrems II*-zaak. **Dit betekent dat EU-onderzoekers op dit moment effectief geen juridisch middel hebben om op structurele basis persoonsgegevens naar Amerikaanse partijen te sturen.** Wellicht zou per geval een patiënt om ad hoc toestemming gevraagd kunnen worden, als de gegevens worden doorgegeven buiten de EU. Maar dit vergt kostbare organisatie en is niet in alle gevallen juridisch mogelijk (zie voor onmogelijke omstandigheden paragrafen 3.1.2 en 3.1.3, alsook paragraaf 3.3). **Als achteraf bezien ad hoc toestemming had moeten worden gevraagd voor**

130 Artikel 9 lid 2 sub j en artikel 89 lid 2 AVG alsook artikel 9 lid 4 AVG.

131 Zie ook artikel 28 UAVG over genetische gegevens.

de internationale gegevensdoorgifte, en dat is niet meer mogelijk, dan kan dat onderzoek waarschijnlijk geen doorgang meer vinden.

Naast de AVG, is ook de **WGBO relevant in het geval van internationaal onderzoek**. De WGBO-wetgever heeft aangegeven, dat het betreffende internationaal onderzoek bij de toestemmingsvraag aangekondigd moet zijn (paragraaf 3.1.1). Wat als dat niet is gebeurd? Mogen de gegevens over de Nederlandse patiënten niet worden gebruikt in het internationale onderzoek?

4.2.2 Knelpunten die samenhangen met nieuwe technologie en de toetreding van commerciële spelers in het zorgdomein

In hoofdstuk 2 gaven we drie voorbeelden van nieuwe (digitale) ontwikkelingen die extra uitdagingen opleveren voor bij het gebruik van gegevens uit medische dossiers ten behoeve van nWMO-onderzoek. De patiënt zelf levert bijvoorbeeld gezondheidsgegevens aan met behulp van *wearables* en *health apps*. Niet alleen hulpverleners zelf en onderzoekers bij onderzoeksinstituten, maar ook technologiebedrijven hebben buiten de behandelrelatie om interesse in de gegevens. Deze bedrijven ontwikkelen bijvoorbeeld de patiëntportalen, kunstmatige intelligentie of *apps* die bij de behandeling of zorg worden ingezet. De grootste van deze bedrijven bevinden zich buiten de EU, bijvoorbeeld in de Verenigde Staten. Data uit medische dossiers helpen hen om hun product of service te verbeteren of zelfs nieuwe services aan te bieden. Maar ze raken daarmee ook gemakkelijk buiten het medische domein. De WGBO-wetgever ging uit van nWMO-onderzoek, waarbij het gangbare medisch-wetenschappelijk onderzoek steeds minder wordt uitgevoerd door hulpverleners en steeds meer door gespecialiseerde onderzoekers.¹³²

Wat de WGBO-wetgever destijds niet voorzag, is dat data – met name gezondheidsinformatie – grote commerciële waarde bezitten (EY 2019). Het is dan ook niet verwonderlijk dat partijen als Google en Microsoft samenwerkingen aangaan met ziekenhuizen of medische onderzoeksinstituten. De data die worden verwerkt in het kader van onderzoek, kunnen dan ook worden gebruikt voor eigen dienstverlening. Zo heeft Google-bedrijf Verily onlangs een verzekeringstak opgericht.¹³³

132 Nota n.a.v. het Eindverslag WGBO, p. 33.

133 <https://www.theverge.com/2020/8/25/21401124/alphabet-verily-insurance-coefficient-stop-loss>.

Als de commerciële partijen de medische gegevens voor eigen doeleinden (onderzoek of iets anders) willen gebruiken, of een vergaande zeggenschap hebben over de te verwerken gegevens uit medisch dossiers, dan zijn ze te kwalificeren als ‘verwerkingsverantwoordelijken’, al dan niet gezamenlijk met andere samenwerkende partijen.¹³⁴ De bediening van louter eigen, private, belangen vallen logischerwijs niet onder de ‘algemeen belang’-eis (paragraaf 3.1.2). Dat betekent, dat de WGBO hen geen ruimte biedt om zonder toestemming gegevens uit medische dossiers te gebruiken. Het trainen van AI, of de toepassing van *machine learning* behoeven immers, net als anonimiseren, een rechtsgrond en – in het geval van bijzondere persoonsgegevens – een opheffingsmogelijkheid (Bijlage 1) (Hacker 2020, AEPD 2020). Amsterdam UMC lost dit op door het beleid te hanteren dat commerciële onderzoeken alleen mogen plaatsvinden op basis van toestemming van de patiënt (Scholte et al. 2019).

De intrede van technologie in de behandelpraktijk (zoals apps, patiëntportalen en *machine learning*) levert dus de nodige vragen op. Bijvoorbeeld of de wetgeving van toepassing is op met de technologie verzamelde en verwerkte gegevens, al dan niet ingebracht in de behandelrelatie door de patiënt zelf. Ook het gebruik van deze gegevens door bedrijven voor eigen product- of serviceontwikkeling roept vragen op. We zetten de door ons geïdentificeerde knelpunten op een rij.

Knelpunt 6: Data verzameld met nieuwe technologie beschermd door het beroepsgeheim of niet?

In het voorgaande hoofdstuk hebben we geleerd dat, zodra een hulpverlener bij de uitoefening van zijn/haar beroep kennisneemt van informatie over de patiënt, het beroepsgeheim die informatie beschermt. De WGBO-regels zijn dan van toepassing. Het is dus van belang dat geverifieerd wordt **of het onderzoek gebruik maakt van door het beroepsgeheim beschermde data**.

Het is niet altijd eenvoudig om na te gaan welke gegevens onder het beroepsgeheim vallen en wanneer dit het geval is. We beschreven dit al in paragraaf 3.1, in het kader ‘beschermd door het medisch beroepsgeheim’? Als een arts van de patiënt verlangt een **app** te installeren waarmee het slaapritme kan worden gemeten, worden deze *quantified self*-data dan beschermd door het medisch beroepsgeheim? Zo ja, hoe kunnen onderzoekers nagaan of aan de app-gegevens een ‘beroepsgeheim’ kleeft? Als dat het geval is, moet rekening worden gehouden met de WGBO. Als dat ten onrechte niet is gebeurd, dan vindt het onderzoek plaats in strijd met de wet. Vergelijkbare vragen doen zich voor met betrekking tot gegevens gegenereerd door **digitale portalen** (paragraaf 3.3) of

134 Vgl. Ploem et al. 2020: “Wanneer verschillende onderzoeksinstellingen samenwerken (het kan echter ook gaan om samenwerking met een commerciële partij, zoals een bedrijf) zijn ze te beschouwen als ‘gezamenlijke verwerkingsverantwoordelijken’, als ze althans tezamen doel en middelen van de gegevenswerkingen vaststellen.”

gegevens opgenomen in **PGO's** (paragraaf 3.1.6, kader 'PGO's, Wabvpz en onderzoek') of gegevens direct ontvangen van burgers via de **Personal Health Train** (zie kader).

Daarnaast is het om een andere reden van belang om na te gaan of gegevens beschermd zijn door het medisch beroepsgeheim. Namelijk als voorgestelde wetgeving of beleidsmaatregelen het beroepsgeheim raken. In zo'n geval dienen de individuele en algemene belangen expliciet te worden benoemd en te worden gewogen (zie paragraaf 1.2). Dat gaat niet altijd goed. Het wetsvoorstel over de **CoronaMelder-app** illustreert dat. In die context wordt het beroepsgeheim slechts mondjesmaat genoemd. De toelichting bij de wet merkt op, dat bij constatering van een (mogelijke) infectie sprake is van een behandelrelatie tussen een geïnfecteerde burger en de GGD. Het beroepsgeheim is dan van toepassing.¹³⁵ Het voorstel noemt verder de mogelijkheid van een afgeleide geheimhoudingsplicht, maar verklaart verder niet hoe dat begrip van toepassing is ten aanzien van de app. Wanneer exact gegevensverwerkingen onder het beroepsgeheim vallen, en wat dit betekent in het licht van de rechten van burgers (paragrafen 1.2.1 en 1.2.3) of de mogelijkheden voor onderzoekers (paragrafen 1.2.3), werkt het wetsvoorstel niet uit. Zou het beroepsgeheim ook moeten gelden voor de data die nog niet aan de GGD zijn verstrekt, maar slechts lokaal op de mobiele telefoon, door de app-gebruiker zijn geregistreerd? Waarom wel? Waarom niet? Hoe zit dat met de gegevens over de afspraak met de teststraat? Op basis van de wet voor de CoronaMelder kunnen GGD-hulpverleners en onderzoekers moeilijk vaststellen wanneer welke data, zoals de app-data en de gegevens over de afspraak met de teststraat, beschermd worden door het beroepsgeheim - laat staan achterhalen welke belangenafwegingen hieraan ten grondslag liggen.

Hoogleraar Gezondheidsrecht Johan Legemaate constateert in zijn inaugurele rede dat het noemen van het beroepsgeheim en weging van individuele en algemene belangen vaker niet dan wel is gebeurd (Legemaate 2011). Hij signaleert dat wetgeving vooral wordt ingezet als instrument om politieke beleidsdoelen te realiseren, waardoor het losser komt te staan van de normatieve uitgangspunten en opvattingen die binnen het recht relevant zijn. Hij waarschuwt voor de zogeheten '**instrumentaliserende werking' van wettelijke regelingen**, zeker wanneer die regelingen voortkomen uit de wens om een actueel probleem op te lossen. De relatie tussen middel en doel wordt dan al snel uit het oog verloren. Hij geeft onder meer het voorbeeld van zorgverzekeraars die sinds de inwerkingtreding van de Zorgverzekeringswet in 2006 meer mogelijkheden hebben gekregen om ter controle van de juistheid van declaraties zo nodig gegevens uit patiëntendossiers te raadplegen.

135 Tweede Kamer, vergaderjaar 2019–2020, 35 538, nr. 3, *Memorie van Toelichting Tijdelijke wet notificatieapplicatie covid-19*.

Knelpunt 7: Hoe te toetsen aan wetgeving bij het trainen en ontwikkelen van AI?

Een belangrijke vraag die een hulpverlener moet beantwoorden is, of nWMO-onderzoek voldoet aan de WGBO-eis 'statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid, ten behoeve van het algemeen belang.' Zie paragraaf 3.2.1. Als aan die eis is voldaan, hoeft mogelijk geen toestemming te worden gevraagd aan de patiënten. En dat wordt als prettig ervaren. Onderzoekers willen het liefste zoveel mogelijk onbelemmerd aan de slag met data uit medische dossiers. Niet alleen omdat het vragen van toestemming enige organisatie vergt, maar ook omdat het verkrijgen van toestemming lastig blijkt (Ploem et al. 2020).

Het is echter niet altijd helder of zo'n onderzoek aan de orde is. Die vraag rijst vooral bij moderne onderzoeken met AI, zoals die met *machine learning* of *natural language processing* (paragraaf 2.1, paragraaf 3.1.2, kader 'Statistiek, wetenschappelijk onderzoek of iets anders?'). Waar ligt bijvoorbeeld het onderscheid tussen wetenschappelijk onderzoek met AI en het (verder) ontwikkelen en optimaliseren van een AI-toepassing in de zorg? Dit is een moeilijk te beantwoorden vraag, omdat de AI-modellen constant ontwikkeld en verbeterd worden naarmate ze meer (persoons)gegevens krijgen gevoed. Daardoor is het lastig vast te stellen waar 'onderzoek stopt en toepassing begint' (Mitrou 2018). De *Datenethikkommission*, die de Duitse regering adviseert over data en algoritmische systemen, zegt hierover: "*Uncertainty persists, however, in particular as regards the scope of the so-called research privilege for secondary use of data, and the scope of what counts as 'research' in the context of product development.*" (Data Ethics Commission 2020).

Als blijkt dat een AI-onderzoek meerdere doelen dient, bijvoorbeeld onderzoek en het ontwikkelen van een AI-toepassing in de zorg, dan zou toestemming alleen achterwege kunnen blijven als de WGBO voor beide doelen die mogelijkheid biedt. Voor het onderzoeksdoel betekent dit onder meer, dat toestemming in redelijkheid niet mogelijk of te verlangen is (paragraaf 3.1.3 en 3.1.4). Maar geldt dat ook voor het productontwikkelingsdoel dat met de AI-toepassing wordt nagestreefd? De AVG zal meestal van toepassing zijn (zie paragraaf 4.2.4). Welke rechtsgrond (paragraaf 3.2.1, tabel 4) en, als de AI getraind wordt met gezondheidsgegevens, welke opheffingsmogelijkheid (Bijlage 1) gelden dan? Het lijkt erop, dat voor het productontwikkelingsdoel slechts toestemming een mogelijkheid is, terwijl dit vanuit onderzoeksperspectief juist niet altijd wenselijk is.

Deze knelpunten zullen meer actueel worden als de *Personal Health Train* (PHT) gerealiseerd wordt. PHT is ontwikkeld om een veilige omgeving te creëren waarin belangrijke fundamentele rechten worden geborgd door professionals, bijvoorbeeld binnen de setting van een ziekenhuis. Het idee achter PHT is om, al dan niet zelflerende, algoritmes te 'brengen' naar de data van de bronhouder, zoals een

ziekenhuis. Dit in tegenstelling tot dataverzameling door (commerciële) onderzoekers, of plaatsen van data op een centrale plaats (PBLQ 2019). In onderstaand kader zetten we uiteen wat PHT in de praktijk kan gaan betekenen.

Knelpunt 8: Delen met commerciële partijen vraagt om extra waarborgen

Hulpverleners niet altijd scherp genoeg op belangen van commerciële partijen

De vraag is of iedere hulpverlener net als Amsterdam UMC scherp let op de situatie waarin commerciële partijen een rol kunnen spelen. Gegevens kunnen onbedoeld zonder toestemming worden vrijgegeven, terwijl voor bepaalde onderdelen van het (onderzoeks)project toestemming gevraagd had moeten worden. Als achteraf blijkt dat dit inderdaad zo is, dan zijn er onrechtmatig gegevens verstrekt. De hulpverlener had nooit mogen verstrekken. Dat is onder meer tuchtrechtelijk laakbaar, de onderzoekers handelen in strijd met hun gedragscode en het commerciële bedrijf gebruikt gegevens in strijd met de AVG.¹³⁶

Mogen commerciële partijen verdienen aan de gegevens?

Een ander knelpunt ontstaat, als partijen die betrokken zijn bij het onderzoek, data willen toe-eigenen. Dit bleek onlangs, toen commerciële partijen met zorgdata van Britse patiënten onder meer AI-toepassingen wilden ontwikkelen ter bestrijding van COVID-19. De bedoeling was om één dataverzameling te creëren, die zou fungeren als dé waarheidsbron over de epidemie. **De deelnemende partijen hadden aanvankelijk bedongen dat alle intellectuele eigendomsrechten, waaronder die met betrekking tot de data, aan hen zouden toekomen.**

Uiteindelijk is deze afspraak teruggedraaid.¹³⁷

De vraag rijst of zo'n toe-eigening van de vruchten van de gegevensverwerkingen past binnen de noemer 'algemeen belang'? Met andere woorden: mogen dit soort deals gesloten worden, zonder dat de patiënt daarvoor toestemming heeft gegeven? Dit is een openstaande vraag, die bij de totstandkoming van de WGBO niet aan de orde is gekomen. Hoe zouden we daar nu over denken?

Vergelijkbare vragen kunnen naar een maatschappelijk niveau getild worden.

Mogen 'de Googles van deze wereld'¹³⁸ geld verdienen aan data uit medische dossiers? Zo ja, onder welke voorwaarden? Zo nee, waarom niet?

136 Dit is geen onrealistisch scenario. In 2016 werd duidelijk dat Google data van meer dan 1.6 miljoen Britse patiënten had gebruikt voor het trainen van haar AI en het testen van een app. Dit gebeurde zonder toestemming. Er volgde publieke verontwaardiging en de Britse toezicht-houder concludeerde dat de gegevensbeschermingswetgeving was overtreden (Lomas 2019).

137 <https://techcrunch.com/2020/06/05/uks-covid-19-health-data-contracts-with-google-and-palantir-finallyemerge/>.

138 NOS Nieuws, 'Slimme algoritmes moeten levens van intensive care-patiënten redden', 17 november 2019, <https://nos.nl/artikel/2310884-slimme-algoritmes-moeten-levens-van-intensive-care-patienten-redden.html>.

Kader **Personal Health Train en registratie aan de bron**

Het Ministerie van VWS ondersteunt Personal Health Train (PHT), een op de FAIR-data principes gebaseerde metafoor voor het afsprakenstelsel, de architectuur en de implementatie voor het verantwoord gebruik van gezondheidsdata. Bijvoorbeeld in AI-toepassingen.¹³⁹

Op basis van PHT gaan algoritmen als ‘treinen’ de decentrale datasets bevragen, die als ‘stations’ fungeren. De bedoeling is dat burgers, patiënten, zorgprofessionals of onderzoekers zelf de treinen kunnen besturen. Daarbij dienen personen en instellingen zelf te bepalen welke data toegankelijk zijn en waarvoor ze gebruikt mogen worden. Een voorbeeld van een toepassing is het ophalen van informatie bij bronhouders voor wetenschappelijk onderzoek. De stations, lees de bronhouders, zetten de data op een gestandaardiseerde wijze gereed en geven aan welke gegevens voor welke toepassingen mogen worden gebruikt.

Met PHT worden de data niet naar het algoritme (ook wel ‘de analyse’) gebracht, maar het algoritme naar een kopie van de data. De data blijven daarmee (dicht) bij de bron, zo is de gedachte. Daarmee is het noodzakelijk dat de gegevens op gestandaardiseerde wijze zijn vastgelegd voor het algoritme. Kennisorganisatie Nictiz signaleert namelijk dat de kwantiteit en de kwaliteit van medische data tekort schieten, terwijl dit nodig is voor betrouwbaar gebruik van AI en dus voor betrouwbare zorg (Nictiz 2019). Volgens Nictiz is het nodig dat er méér en efficiënter gestandaardiseerde gegevens worden verzameld. Dit kan onder meer worden bereikt door ‘registratie aan de bron’. Dit is het eenmalig, eenduidig vastleggen van patiëntgegevens tijdens het zorgproces voor meervoudig gebruik. De verwachting is dat door hergebruik van de registraties wetenschappelijk onderzoek eenvoudiger wordt.

De verwezenlijking van PHT heeft de nodige voeten in de aarde. Randvoorwaarden zijn onder meer dat de treinen en stations gecertificeerd zijn, er een audit trail is en dat het gegevensgebruik volledig gecontroleerd kan worden (PBLQ 2019). Hoewel PHT voor gezondheidsonderzoek vooralsnog toekomstmuziek is (Nivel 2019), kan de techniek gunstig uitpakken voor de bescherming van

patiëntgegevens zoals de AVG dat vereist. De AVG is namelijk van toepassing als het algoritme persoonsgegevens verwerkt, bijvoorbeeld door deze te analyseren (STOA 2020). Zo kan PHT voor dataminimalisatie zorgen, door de op te halen informatie te beperken tot noodzakelijke relevante gegevens. Naast een proportionele dataverzameling, kan het algoritme specifiek geïnstrueerd worden om het AVG-principe over doelgebonden gebruik in acht te nemen. Bovendien geeft PHT invulling aan het data-protection-by-design principe, door het mogelijk maken in analyses zelf gedetailleerde gegevens (persoonlijke gegevens) te gebruiken, zonder dat deze persoonsgegevens terug te vinden zijn in de (uitkomsten van) de algoritme-analyses (Zorginstituut Nederland 2018; Rijksoverheid 2019).

Als het algoritme data gebruikt die tot stand zijn gekomen vanwege een behandelrelatie, dan is – naast de AVG – ook de WGBO van toepassing. De WGBO-regels over onderzoek worden niet alleen geactiveerd als het gaat om ‘inlichtingen over de patiënt’, maar ook als er sprake is van ‘inzage in de gegevens uit het dossier’. Dat is wat het algoritme doet: door inzage in dossiers, bijvoorbeeld verwerking van gegevens ‘aan de bron’, worden de analyses gemaakt. Maar als het algoritme de burger als bronhouder aandoet, en de Kamerbrief van de minister lijkt deze mogelijkheid te suggereren,¹⁴⁰ dan is niet evident dat de WGBO van toepassing is, omdat de gegevens niet afkomstig zijn uit een behandelrelatie. Er is dan geen hulpverlener die, vanwege zijn beroepsgeheim, als ‘poortwachter’ fungeert om de data wel of niet te verstrekken.

139 Rijksoverheid, ' Strategisch Actieplan voor Artificiële Intelligentie', 8 oktober 2019, <https://www.rijksoverheid.nl/documenten/beleidsnotas/2019/10/08/strategisch-actieplan-voor-artificieelintelligentie>.

140 “Burgers (...) blijven zo bronhouder van data die kunnen werken voor goede zorg.”, aldus de voormalig minister Bruins. Kamerbrief over data laten werken voor gezondheid d.d. 15 november 2018, <https://www.rijksoverheid.nl/documenten/brieven/2018/11/15/data-laten-werken-voor-gezondheid>.

4.2.3 Knelpunten die spelen rond het vragen van toestemming aan patiënten

Bij het gebruik van gegevens uit medische dossiers is toestemming van de patiënt het uitgangspunt. Maar daarop zijn uitzonderingen. Zowel de zorgverlener als de onderzoeker hebben bij het overwegen of toestemming vragen van de patiënt nodig is, belangrijke 'checklists' af te werken. Het belangrijkste knelpunt ligt hier in de onduidelijkheden bij 'geen bezwaar' en 'brede toestemming'.

Knelpunt 9: Onduidelijkheden bij 'geen bezwaar' en 'brede toestemming'

Geen bezwaar, geen probleem?

Pas als de WGBO hiervoor de mogelijkheid biedt, mag het vragen van toestemming achterwege blijven (paragraaf 3.1.2 t/m 3.1.5) mits de patiënt geen bezwaar heeft gemaakt. **Bezwaar komt dus pas aan de orde, als eerst is vastgesteld dat er geen toestemming gevraagd hoeft te worden. In de praktijk leunen echter veel ziekenhuizen op het geenbezwaar-systeem** (Ploem et al. 2020). Bij veel ziekenhuizen is namelijk de stelregel: als de patiënt geen **bezwaar** heeft geuit, dan mogen de gegevens worden gebruikt door onderzoekers. **De ziekenhuizen gaan daarmee voorbij aan het uitgangspunt van toestemming.** Hiermee lopen zij het risico niet te voldoen aan de WGBO-regels, waardoor het onderzoek in het ergste geval gestaakt moeten worden. Aldus ontstaat *onnodig* een knelpunt, omdat de ziekenhuizen niet alleen hadden moeten verifiëren of er bezwaar is geuit, maar stap-voor-stap alle vereisten hadden moeten nagaan (paragraaf 3.1 en stroomdiagram in Bijlage 4).

Vooraf kleine hulpverleners hebben behoefte aan een centraal 'geenbezwaar-systeem'

Met betrekking tot een geenbezwaar-systeem signaleren we daarnaast het volgende aandachtspunt. **Waardevolle data voor onderzoek treft men niet alleen aan in ziekenhuizen, maar ook bij andere hulpverleners zoals huisartsen.** Een ziekenhuis heeft doorgaans een geenbezwaarregeling ingericht. Maar geldt dat ook voor alle huisartsen in Nederland? Of wat te denken van tandartsen, apothekers of optometristen? Zij zijn allemaal hulpverleners, gebonden aan de voorschriften van de WGBO. Zouden zij omwille van wetenschappelijk onderzoek gegevens verstrekken zonder een geenbezwaar-systeem, dan mag dit alleen met toestemming van de patiënt. Dit geldt ook als de mogelijkheid om bezwaar aan te tekenen niet onder de aandacht is gebracht. Bijvoorbeeld als informatie in de patiëntfolder.

De vraag rijst in hoeverre patiënten op de hoogte zijn van hun bezwaarrechten. **In de jaren '90 meende de WGBO-wetgever dat van 'mondige burgers' kan worden verlangd, dat zij zich informeren over hun rechten om op te komen**

tegen onderzoek met patiëntgegevens, als zij daartegen bezwaar hebben. Hoe realistisch is deze veronderstelling? Niet voor niets geeft het Amsterdam UMC patiënten een extra mogelijkheid om bezwaar aan te tekenen – los van de algemene bezwaarprocedure – als het vragen van toestemming in redelijkheid niet kan worden verlangd (paragraaf 3.1.4) (Scholte et al. 2019). De patiënten ontvangen dan een brief met uitleg over het doel van het onderzoek, de te hergebruiken gegevens, de betrokken partijen en de bewaartermijn. Vervolgens krijgt de patiënt vier weken de gelegenheid om laagdrempelig bezwaar te kunnen maken, bijvoorbeeld per e-mail of met een antwoordkaart.

Voldoet een brede toestemming?

Een meermaals in de literatuur en de praktijk aangetroffen knelpunt betreft de vraag hoe ‘breed’ of ‘nauw’ de toestemming moet zijn die aan de patiënt wordt gevraagd voor dataverstrekking of inzage voor onderzoek. De wens bestaat om slechts een ‘globale toestemming’ voor wetenschappelijk onderzoek of statistiek te hoeven vragen. Deze wens is vooral aan de orde, als onderzoekers de omvang en reikwijdte van hun onderzoek niet volledig kunnen formuleren.

Noch de WGBO, noch de AVG bieden ‘zomaar’ de mogelijkheid voor een brede toestemming. Een te breed geformuleerde toestemmingsvraag zou kunnen neerkomen op een ‘blanco volmacht’ en de WGBO-wetgever heeft aangegeven dat dat niet de bedoeling is.¹⁴¹

Ten tweede heeft de EDPB zich uitgelaten over toestemming in een onderzoekscontext. De EDPB geeft de voorkeur aan het vragen van toestemming in fases (paragraaf 3.1.1) en volgens de EDPB is een ‘breed geformuleerde toestemming’ moeilijk verenigbaar met de AVG. Hierop bestaat kritiek. De auteurs Ploem et al. vinden dat het toestemmingsprincipe niet gelegd hoeft te worden langs de strenge meetlat van de EDPB (2020). Volgens hen is de AVG-toestemming waarop de EDPB doelt een andere toestemming, dan bedoeld in de WGBO (en artikel 24 UAVG). Vooralsnog hebben wij geen brede steun gevonden voor deze opvatting. Het Nederlands Instituut voor Onderzoek van de Gezondheidszorg (Nivel) houdt zich op de vlakte en geeft geen concreet antwoord op de vraag of de AVG-toestemming anders is dan de WGBO-toestemming met betrekking tot persoonsgegevens (Stüssgen et al. 2019, Bijlage C). Zelfs al zouden Ploem et al.

141 *Nota n.a.v. het Eindverslag WGBO*, p. 9 en pp. 33 – 34. Tegelijkertijd zegt de WGBO-wetgever: “(...) Medisch-wetenschappelijk onderzoek met op naam gestelde gegevens is mogelijk indien degene van wie de gegevens afkomstig zijn, daartoe toestemming heeft gegeven. Deze toestemming kan in een vroeg stadium van de behandeling worden gegeven en in het - het zij herhaald - dossier worden vastgelegd. Zij kan tot op zekere hoogte een algemeen karakter dragen, (...). Het lijkt ons niet juist dat bij voorbeeld een huisarts van de patiënt, al bij het begin van de behandelrelatie, toestemming zou vragen, ongeacht welke aandoening, in de toch duurzame relatie, vastgelegde persoonsgegevens aan derden voor wetenschappelijk onderzoek te mogen verstrekken.”, *Nota n.a.v. het Eindverslag WGBO*, p. 34.

gevolgd worden in hun opvatting, dan blijft alsnog de visie van de WGBO-wetgever overeind die geen ‘blanco volmacht’ wenst.

Linksom (via de EDPB) of rechtsom (via de WGBO) lijkt er dus geen ruimte te zijn voor een ‘brede toestemming’, maar deze opvatting dient bevestigd te worden.

4.3 Voorbeelden van datasolidariteit in Europa

In paragraaf 4.2.1 signaleerden we het probleem dat grensoverschrijdend onderzoek in Europa wordt bemoeilijkt door uiteenlopende nationale wetten over medisch data-onderzoek. Auteurs Becker et al. onderschrijven dit (2020). Daarbij hekelen ze dat EU-landen niet het voortouw lijken te nemen om, tezamen met onderzoekers, na te gaan hoe grensoverschrijdend onderzoek kan bijdragen aan publieke gezondheid. Dit is volgens hen een aanwijzing dat wetgevers en privacy-toezichthouders te weinig diepgaand begrip hebben over wat gezondheidsonderzoek nodig heeft.

De vraag is, of de opmerking van Becker et al. over wetgevers en toezichthouders in alle gevallen gerechtvaardigd is. Gedurende het onderzoek voor dit rapport zijn we namelijk diverse buitenlandse voorbeelden tegengekomen waaruit het tegendeel blijkt. Zo publiceerde het Britse *Centre for Data Ethics* dit jaar het rapport *Addressing trust in public sector data use*. Hierin onderzoeken ze de meest voorkomende barrières die gegevensuitwisselingen in de weg kunnen staan, zoals juridische, technische en culturele hindernissen. De NHS komt hierin ook aan bod. Deze Britse gezondheidsdienst hanteert onder meer drie speerpunten van beleid:

- bevorder kennis en begrip onder het bredere publiek door transparantie en *public engagement*;
- moedig datadelen aan voor individuele zorg;
- waarborg het medisch beroepsgeheim en het zorgsysteem, door de redelijke verwachtingen uit te spreken en aan te geven welke *use-cases* geen doorgang mogen vinden.

Uit het rapport blijkt ook dat sinds mei 2018 de NHS een **landelijk geen-bezwaarprogramma faciliteert**. Dit is een tool waarmee patiënten kunnen aangeven dat ze niet willen dat ‘hun’ persoonsgegevens buiten de NHS worden gedeeld (CDEI 2020).

Daarnaast troffen we de plannen aan voor een *Nordic Commons for health data* (NordForsk 2019). Hierin bundelen de Scandinavische landen hun krachten ten behoeve van de mogelijkheden die secundair gebruik van gezondheidsdata bieden, zoals medisch data-onderzoek. In de plannen wordt stilgestaan bij de noodzaak

van verbeterde datakwaliteit, interoperabiliteit en het data machine-leesbaar maken van gegevens, bijvoorbeeld voor algoritmes. Obstakels van juridische, technische of procedurele aard dienen te worden weggenomen. Het doel is om op Scandinavisch niveau het delen van gezondheidsdata te bevorderen, zodat er een concurrentievoordeel ontstaat. De *Nordic Commons* beoogt hiertoe een platform te bieden door 'open research' te bieden ten behoeve van de Scandinavische volksgezondheid en maatschappij. Ze doen een oproep aan alle partijen die in actie moeten komen voor het bereiken van de doelen: beleidsmakers, subsidiegevers bij onderzoek en innovatie, en de eigenaren van de gegevens.

Een ander voorbeeld betreft Finland. In paragraaf 3.1.1 stipten we aan dat het in Finland wettelijk verplicht is om voor patiënten een onderzoeksplan beschikbaar te hebben dat ze kunnen inzien. Auteurs Piai et al. hebben onderzoek verricht naar de Finse situatie (2020). Ze beschrijven dat in Finland de afgelopen jaren flink is geïnvesteerd in de gezondheidssector, waarbij publieke en private partijen samenwerken om secundair gebruik van gezondheidsdata te bevorderen. Hiervoor is met een publiek innovatiefonds het project *Isaacus* opgericht. Het project had onder meer als doel om een data-hub te creëren, nieuwe wetgeving op te stellen en een nieuwe overheidsinstantie te organiseren. Dit heeft geresulteerd in:

- de *Digital health HUB*, waarmee in lijn met de AVG gezondheidsgegevens kunnen worden gedeeld;
- een wet die op 1 mei 2019 in werking trad en onder meer een juridisch raamwerk biedt voor dataverstrekkingen voor medisch data-onderzoek; en
- een nieuwe overheidsinstantie, *FinData* genaamd. FinData is belast met het verzamelen van de data, de coördinatie van dit proces en het bieden van diensten voor pseudonimisering en anonimisering. De instantie zorgt ervoor dat de coördinatie van dit proces en het bieden van diensten pseudonimisering- en anonimiseringsdiensten. De instantie zorgt ervoor dat de doelstellingen van de wet feitelijk uitgevoerd kunnen worden. In het voornoemde rapport beschrijven de auteurs ook de inspanningen ten behoeve van het faciliteren van medisch data-onderzoek in Frankrijk, Portugal en Italië (Piai et al. 2020).

Het Finse model wordt aangehaald in *A European strategy for data* van de Europese Commissie (Europese Commissie 2020). Deze datastrategie beoogt een interne markt voor data te realiseren en oplossingen voor de geconstateerde problemen aan te dragen, in de vorm van beleidsmaatregelen en financiering. Hiervoor zijn vier pijlers geformuleerd, waarbij de eerste pijler een sectoroverschrijdend governancekader betreft voor datatoegang en -gebruik. Het is de bedoeling dat de Commissie in het vierde kwartaal van 2020 een ondersteunend wetgevingskader formuleert voor de governance van gemeenschappelijke Europese dataruimtes. Hiervoor bouwt de Commissie voort op initiatieven als FinData. Onder meer data-interoperabiliteit wordt toegejuicht, dat volgens de Commissie volgens de FAIR-principes zou kunnen gebeuren. Een andere beoogde

maatregel betreft het faciliteren van vlottere besluitvorming over welke data, hoe en door wie gebruikt mogen worden voor wetenschappelijk onderzoek. Ook bekijkt de Commissie de mogelijkheden voor particulieren om de data die zij zelf genereren, in te kunnen zetten voor het algemeen nut, als particulieren dat willen. Dit noemt de Europese Commissie **data-altruïsme** en weerspiegelt de gedachte van datasolidariteit. Uiteindelijk is het de bedoeling dat er een *European Health Data Space* wordt gecreëerd.¹⁴²

4.4 Tot slot

De lijst van knelpunten die we op basis van ons onderzoek per vraagstelling identificeerden is niet mals. Sommige knelpunten zijn gerelateerd, maar de oorzaken – en daarmee de oplossingsmogelijkheden – verschillen.

We zien dat de huidige wetgeving rond nWMO-onderzoek niet zozeer belemmerend is, maar wel op veel punten **verhelderd en beter op elkaar afgestemd moet worden**. Een aantal andere landen zijn net een stap verder dan Nederland met hun initiatieven rond 'datasolidariteit'. In het Verenigd Koninkrijk is er bijvoorbeeld een landelijk geen-bezwaarsysteem. In Scandinavië bouwt men een gezamenlijk platform om data uit medische dossiers te delen. En Finland heeft zelfs een speciale instantie om te zorgen dat de doelstellingen van de wet uitgevoerd worden. Nederland zou actief mee kunnen doen bij de ontwikkeling van de *European Health Data Space*.

We zien ook dat bij nWMO-onderzoek dat is gebaseerd op gegevens die worden gegenereerd, gedeeld of geanalyseerd met nieuwe vormen van technologie, druk ontstaat op fundamentele rechten zoals de **bescherming van persoonsgegevens** en **de eerbiediging van het privéleven**. Een cruciale vraag is, wanneer gegevens beschermd worden onder het beroepsgeheim (en dus de WGBO-regels gevolgd moeten worden) en wanneer dit niet het geval is. Die problemen worden zichtbaar bij *quantified self*, bij het gebruik van een interactief portaal tussen patiënt en hulpverlener, maar ook bij de *Personal Health Train*. Daarbij gaan algoritmes naar de 'bron': de veilige, professionele omgeving waarin belangrijke fundamentele rechten worden geborgd.

Op de vraag of commerciële partijen toegang mogen hebben tot de gegevens uit medische dossiers, zelfs voor *for profit* onderzoek, is nu nog geen antwoord te

142 Europese Commissie, 'Member States meet with the European Commission to discuss protection of personal data in the health sector', 30 januari 2020, <https://ec.europa.eu/digital-singlemarket/en/news/member-states-meet-european-commission-discuss-protection-personal-data-health-sector>.

geven. De ruimte voor commerciële partijen om te verdienen in het kader van nWMO-onderzoek waarvan het de bedoeling is dat het een algemeen belang moet dienen, moet **maatschappelijke worden verkend**.

Verder is evident, dat de praktijk van nWMO-onderzoekers en professionals vraagt om **extra uitleg over toestemming, de reikwijdte ervan en opties om 'geen bezwaar' te regelen**.

In het volgende hoofdstuk presenteren we conclusies en oplossingsrichtingen. De voorbeelden uit de andere Europese landen zijn daarvoor soms een inspiratie geweest. Daarbij aangetekend, dat de daar opgezette structuren voor 'datasolidariteit' vaak toch nog vrij globaal zijn – op niveau van systemen en afspraken – en niet van toepassing op Nederlandse wetgeving.

5 Conclusies en oplossingsrichtingen

Bestaande gegevens uit medische dossiers zijn gewild en waardevol voor onderzoek in het kader van de volksgezondheid, of voor het ontwikkelen van commerciële diensten binnen de zorgsector. Denk aan patiëntportalen, beslissystemen gebaseerd op AI of apps die bij de behandeling of zorg worden ingezet. De Nederlandse overheid vraagt burgers en bedrijven daarom om datasolidariteit te tonen. Het zorgveld verwacht veel van de nieuwe technologie, die met behulp van de data ontwikkeld kan worden.

De WGBO, AVG en UAVG geven duidelijke voorwaarden en uitgangspunten waarmee het mogelijk is voor derden om met digitale gegevens uit medische dossiers dit nWMO-onderzoek te doen. Beroepsgroepen kunnen de toepassing van de wet verhelderen, bijvoorbeeld door richtlijnen op te stellen. Van zorgprofessionals die de gegevens beschikbaar kunnen maken voor onderzoek én van de onderzoekers die de gegevens willen gebruiken, wordt verwacht dat zij zorgvuldig te werk gaan, vanuit de uitgangspunten van de wet. Maar daarmee is niet alles gezegd.

Onderzoekers, hulpverleners en andere medische professionals zullen allereerst doel en voorgestelde methode van ieder nWMO-onderzoek moeten beoordelen. In het rapport *Doelgericht digitaliseren* van het Rathenau Instituut (Rathenau Instituut 2018a) benadrukten we al, dat het gebruiken van *big data* voor bijvoorbeeld het ontwikkelen van AI vraagt om een aanpak waarbij onderzoekers en de betrokken commerciële partijen samen met zorgprofessionals de goede vragen formuleren en met de juiste data en methoden waardevolle inzichten en toepassingen ontwikkelen. Veel ontwikkelde technologie op basis van AI is niet aan de maat en doet niet wat wordt beloofd. Daarmee werkt deze niet voor professionals en is de technologie vaak ook niet in het belang van burgers en patiënten (Rathenau Instituut 2020a). De medische professionals kunnen de context geven die immers vaak niet besloten ligt in digitale medische gegevens. Op deze manier worden het *ecosystem of innovation* en het *ecosystem of trust* op elkaar betrokken. Een belangrijke voorwaarde voor succes, zoals het Rathenau Instituut betoogde in een reactie op het Europese Witboek met betrekking tot AI (Rathenau Instituut 2020c).

Het Rathenau Instituut wil met dit rapport bijdragen aan **een goed geïnformeerd politiek en maatschappelijk** gesprek over de ervaren en werkelijke belemmeringen bij het gebruik van digitale gegevens uit medische dossiers voor

nWMO-onderzoek, inclusief de data die door de patiënt zelf zijn verzameld en aangereikt binnen het dossier. We lieten zien, dat de uitdaging bij het opstellen en toepassen van wetgeving voor nWMO-onderzoek ligt in het zorgvuldig afwegen van de belangen, rechten en plichten van de **patiënt** (of cliënt), de **hulpverlener** (arts of andere hulpverlener in de behandelrelatie, bevoegd om de gegevens beschikbaar te maken) en de **onderzoeker** (of ontwikkelaar). Die afweging van belangen wordt gemaakt tegen een achtergrond van kansen op verbetering of bescherming van de volksgezondheid, mogelijk gemaakt door het gevraagde nWMO-onderzoek.

Voor het doen van nWMO-onderzoek zijn er nationale en Europese wettelijke kaders. Desondanks signaleren het Ministerie van VWS, de zorgsector, onderzoekers en behartigers van patiëntbelangen in de afgelopen jaren, zeker rond de invoering van de AVG, allerlei knelpunten bij het gebruik van gegevens uit medische dossiers voor nWMO-onderzoek.

De **centrale vraag** in dit onderzoek luidde dan ook: Wat zijn mogelijke oplossingen voor de knelpunten rond wet- en regelgeving, zoals die nu worden ervaren bij het doen van nWMO-onderzoek?

In dit rapport hebben we allereerst stapsgewijs uitgelegd hoe de wetgever rekening houdt met de belangen, rechten en plichten van de hulpverlener, patiënt en onderzoeker. Deze verheldering is belangrijk, omdat duidelijk is dat hierover veel verwarring bestaat. Door die verwarring is een goed politiek en maatschappelijk gesprek lastig. We hebben ook onderzocht welke complexiteit nieuwe technologische ontwikkelingen opleveren, zoals AI, *wearables* en health apps en digitale portalen tussen patiënt en hulpverlener. In eerdere onderzoeken van het Rathenau Instituut hebben we de kansen en beperkingen voor 'regie op eigen gezondheid voor de burgers' al aangegeven (Rathenau Instituut 2014, 2016, 2019a), maar in dit rapport ligt de nadruk op de knelpunten bij het doen van nWMO-onderzoek met de gegevens uit medische dossiers.

In hoofdstuk 4 hebben we in totaal negen knelpunten op een rij gezet rond gebruik van digitale gegevens uit medische dossiers voor nWMO-onderzoek. Daarbij gaven we aan waar het *precies* knelt. Hoofdstuk 5 geeft in drie paragrafen de belangrijkste conclusies over de knelpunten bij nWMO-onderzoek. Daarbij geven we vervolgens steeds een aantal oplossingsrichtingen aan voor de wetgevers, ministeries, toezichthouders, beroeps- en belangenverenigingen en hulpverleners.

5.1 Huidige wetgeving rond nWMO-onderzoek is niet zozeer belemmerend, maar moet wel helderder

De kritiek op de huidige wetgeving geuit door onderzoekers, hulpverleners en behartigers van patiëntbelangen is niet mals. Maar is die kritiek terecht?

Onze eerste deelvraag luidde daarom: Is de kritiek op de huidige wetgeving bij nWMO-onderzoek terecht, of is er sprake van veronderstelde belemmeringen in plaats van werkelijke belemmeringen? Zijn er extra belemmeringen voor internationaal nWMO-onderzoek? Welke dan?

Paragraaf 4.2.1 benoemde de **vijf knelpunten** die we bij de beantwoording van deze vraag identificeerden. In paragraaf 5.1 trekken we overkoepelende conclusies en schetsen vervolgens daaraan verbonden oplossingsrichtingen.

5.1.1 Verheldering nodig bij AVG, UAVG en WGBO

Deze conclusies zijn gebaseerd op de knelpunten 1 t/m 3 die we op een rij zetten in paragraaf 4.2.1.

Conclusies

- De **AVG** legt nWMO-onderzoek niet verder aan banden ten opzichte van de regels die golden vóór de invoering van deze verordening, maar brengt wel **nieuwe verplichtingen** met zich mee. Zoals de verplichte aanstelling van een Functionaris Gegevensbescherming (FG) en het uitvoeren van een *Data Protection Impact Assessment* (DPIA). De **UAVG** legt nWMO-onderzoek evenmin verder aan banden, vergeleken met eerdere wetgeving.
- De **WGBO-voorwaarden** laten aan een hulpverlener een zekere **ruimte voor interpretatie**, omdat er een afweging moet worden gemaakt tussen de persoonlijke levenssfeer en het belang van het wetenschappelijk onderzoek. Het risico bestaat, dat met name kleine hulpverleners die niet de 'luke' hebben van **expert-ondersteuning** (denk aan een zelfstandige huisarts, diëtist of optometrist), een verzoek om gegevens voor nWMO-onderzoek veiligheidshalve afwijzen, vanwege de zorg om civiel- of tuchtrechtelijk aangesproken te worden. Kansen met gezondheidsgegevens blijven hierdoor liggen.
- De **verhouding tussen de UAVG en de WGBO** geeft aanleiding voor diverse vragen op basis van opmerkingen die zijn gedaan onder de oude Wbp-regeling in het licht van de huidige UAVG-regels, namelijk over:

- a. de **(feitelijke) onmogelijkheid om toestemming te vragen** voor het onderzoek. Volgens de WGBO-wetgever hoeft het niet feitelijk onmogelijk te zijn om toestemming te vragen, maar door de afwijkende opinie van de EDPB is dit niet (meer) zeker;
 - b. de plicht om het onderzoek te **publiceren** (aldus voormalig minister Bruins in 2018);
 - c. **voorwaarden van toestemming** in de WGBO die anders zijn dan de AVG-voorwaarden.
- De voorwaarde gesteld in de WGBO dat het **initiatief tot gegevensverstrekking** uit dient te gaan van de onderzoeker (en niet een hulpverlener) lijkt 'niet meer van deze tijd'.

Oplossingsrichtingen

- Beroepsorganisaties van hulpverleners zouden kunnen bijdragen aan **expert-ondersteuning voor het maken van een gewogen beslissing om gegevens ter beschikking te stellen aan onderzoek**. Algemene voorlichting kan door het Ministerie van VWS worden verzorgd, alsook door toezichthouders als IGJ en de AP. De **gedragscode Goed Gedrag** die momenteel herzien wordt, is eveneens een geschikte plek om hulpverleners en onderzoekers te **informer** over hoe zij overwegingen kunnen maken in lijn met de (U)AVG en WGBO.
- De nationale wetgever dient te **verduidelijken hoe de UAVG-norm** over 'het vragen van uitdrukkelijke toestemming dat onmogelijk blijkt of een onevenredige inspanning kost' **zich verhoudt tot de WGBO-normen**.
- De minister van VWS dient te verduidelijken of **publicatie inderdaad een vereiste** is voor wetenschappelijk onderzoek en of de FAIR-principes verplicht zijn op te volgen. Het vereiste van publiceren past bij het belang van openbaar maken van belangrijke inzichten, zoals verwoord in de Unesco standaard¹⁴³ en het Nederlandse beleid ten aanzien van *Open Science*.
- Er dient nader onderzocht te worden of de WGBO inderdaad een ander **toestemmingsregime** heeft dan de AVG en zo ja, of dit leidt tot de conclusie dat de WGBO niet geheel AVG-proof is.
- De nationale wetgever dient te verduidelijken hoe **de eis uit de jaren '90** (initiatief tot gegevensverstrekking ligt bij onderzoeker) **anno 2020** uitgelegd dient te worden.

5.1.2 Verheldering nodig bij anonimiseren en pseudonimiseren

Deze conclusies zijn gebaseerd op knelpunt 4 van paragraaf 4.2.1.

Conclusies

- Onder nWMO-onderzoekers bestaat het **misverstand dat anonimiseren van gegevens altijd een verplichting is**. Dit belemmert soms het onderzoek. Echter, de WGBO en de (U)AVG verlangen geen anonimisering van gegevens als daardoor het onderzoek niet kan plaatsvinden, zolang het eindresultaat van het onderzoek geen herleidbare gegevens bevat.
- Het **anonimiseren** van gegevens zien sommigen onterecht als een **methode** om het onderzoek volledig te **onttrekken aan de regels van de (U)AVG**.
- Onder de AVG **worden persoonsgegevens beschermd voor en tijdens het anonimiseringsproces**. Bij de WGBO is het onduidelijk of dit ook het geval is.
- In de praktijk wordt niet altijd aan de voorwaarden van **pseudonimisering** voldaan.

Oplossingsrichtingen

- Het ministerie van **VWS zou een discussie kunnen faciliteren over wanneer de WGBO en de (U)AVG dienen te gelden in het licht van geanonimiseerde gegevens**. De discussie zou niet alleen hulpverleners en onderzoekers helderheid kunnen verschaffen over de (on)mogelijkheden van onderzoek met data uit medisch dossiers, maar ook hun FG's en eventuele toezichts- of toetsingscommissies.
- De nationale wetgever dient te **verduidelijken of ook de WGBO en de UAVG gelden tot en met het proces van anonimiseren**. Omdat het hier een vraag betreft die deels EU-recht betreft, ligt het voor de hand dat de EDPB betrokken wordt bij de beantwoording hiervan.
- Organisaties verbonden aan hulpverleners en onderzoeksinstituten zouden **procedures voor een goede pseudonimiseringspraktijk** kunnen opstellen, voor zover zulke procedures nog niet bestaan. De (aan te passen) gedragscode kan hieraan eveneens aandacht besteden.
- Aan de oproep van de onderzoekers aan de wetgever om in de UAVG een duidelijk antwoord te geven op de vraag of en in hoeverre, en onder welke voorwaarden, gepseudonimiseerde patiëntgegevens gebruikt mogen worden bij wetenschappelijk onderzoek, bestaat ons inziens **geen dringende noodzaak**. De voorwaarden voor gebruik zijn onder meer reeds beschreven in richtlijnen van de EDPB en de (toelichtingen bij) de wet- en regelgeving, als waarborgen die ervoor zorgen dat de persoonlijke levenssfeer van de patiënt niet onevenredig wordt geschaad.

5.1.3 Internationaal onderzoek is lastig binnen de EU

Deze conclusies zijn gebaseerd op knelpunt 5 van paragraaf 4.2.1.

Conclusies

- **Binnen de EU gelden afwijkende regels voor (nWMO-)onderzoek** met medische gegevens. De AVG staat het immers toe dat ieder EU-land eigen wet- en regelgeving opstelt voor onderzoeken met medische data. De WGBO en de UAVG bevatten de Nederlandse regeling. In EU-breed onderzoek moet dus per land worden nagegaan wat de nationale regels zijn en hoe daaraan kan worden voldaan. Dat is zeer lastig.
- Gegevensverstrekking aan landen buiten de EU wordt onder voorwaarden toegestaan door de AVG, maar er zijn **knelpunten ten aanzien van gegevensdoorgifte naar de V.S.** en mogelijk ook andere derde-landen, als met de betreffende ontvangers geen bestendige SCC's gesloten kunnen worden of andere constructies die de gegevensdoorgifte juridisch kunnen onderbouwen.

Oplossingsrichtingen

- De grensoverschrijdende knelpunten dienen grensoverschrijdend te worden aangepakt. Een **bespreking van de problematiek via de EU-privacytoezichthouders in de EDPB** ligt voor de hand, maar dit lost het probleem niet op. Uiteindelijk is de **EU-wetgever aan zet om een geharmoniseerd raamwerk te bewerkstelligen** voor onderzoek met gezondheidsdata. Nederland kan daarin haar stem laten doorklinken via het EU-beleid om tot een Europese onderzoeksruimte te komen, waarvan de beoogde *European Health Data Space* een onderdeel is. Omdat het probleem niet beperkt blijft tot de EU, zal ook contact gezocht moeten worden met de Raad van Europa, voor internationale afspraken over gezondheidsdata.
- Daarnaast dient gekeken te worden naar **EU-brede gedragscodes** die onder de AVG erkend worden.¹⁴⁴ Deze kunnen grensoverschrijdende werkwijzen opleggen aan de deelnemende partijen. Ook niet-EU partijen kunnen zich committeren aan zulke EU-brede gedragscodes. De Nederlandse overheid kan daarin, al dan niet via de daartoe bestemde EU-kanalen, een faciliterende rol spelen.
- Tot slot zouden onderzoekers ondersteund kunnen worden bij de beantwoording van vragen voor het opzetten van internationaal onderzoek. Als op internationaal niveau gegevens uit medische dossiers worden verzameld voor een onderzoek, dan kan een **clearing house** nagaan of iedere datastroom voldoet aan de toepasselijke wet- en regelgeving. Voor

144 Internationaal bestaan er ethische richtlijnen voor onderzoek zoals de *Council for International Organizations of Medical Sciences (CIOMS) Guidelines* en de *World Medical Association's (WMA) Declaration of Taipei*, maar dit zijn geen gedragscodes in de zin van artikel 40 AVG.

onderzoekers zelf is dit welhaast een ondoenlijke taak. Zo'n *clearing house* zou een **initiatief van de EU kunnen zijn, aangejaagd door lidstaat Nederland.**

5.2 Fundamentele rechten vaker in de knel bij gebruik van nieuwe technologie in nWMO-onderzoek

De technologie om gegevens over gezondheid te verzamelen of te gebruiken schrijdt voort. Dit leidt tot allerlei ideeën om meer met deze data te doen. Ook door commerciële partijen.

Onze tweede deelvraag luidde daarom: Welke extra kwesties doen zich voor bij nieuwe technologische ontwikkelingen – vaak gefaciliteerd door commerciële partijen – zoals kunstmatige intelligentie, zelfmetingen door patiënten met wearables en digitale communicatie tussen patiënt en hulpverlener? Mogen technologische bedrijven toegang hebben tot de gegevens uit medische dossiers, zelfs voor *for profit* onderzoek?

Paragraaf 4.2.2 besprak de **drie knelpunten** die we bij de beantwoording van deze vraag identificeerden. In paragraaf 5.2 trekken we overkoepelende conclusies en schetsen vervolgens daaraan verbonden oplossingsrichtingen.

Conclusies

- Het is niet altijd eenvoudig om na te gaan **welke gegevens door het medisch beroepsgeheim worden beschermd**, bijvoorbeeld als het gaat om *quantified self* data van de patiënt die op verzoek van de arts in de behandelrelatie worden ingebracht, of gegevens gegenereerd in een digitaal portaal, bewaard in een PGO of 'bezocht' door een *Personal Health Train*.
- Bij plannen voor bijzondere beleidsmaatregelen, zoals het introduceren van de CoronaMelder-app, moet helder zijn **welke gegevens door het beroepsgeheim worden beschermd, in welke fases van de gegevensverwerkingen en door wie**. Als dit niet helder is, heeft dat gevolgen voor de rechten van burgers of de mogelijkheden voor onderzoekers, en daarmee mogelijk voor het algemeen belang. Onderzoekers kunnen bijvoorbeeld niet met zekerheid vaststellen of de lokaal opgeslagen data van de CoronaMelder-app en de hieruit voortvloeiende gegevens over de afspraak met de teststraat, behandeld moeten worden volgens de WGBO of alleen de (U)AVG.
- Door wetgeving vooral in te zetten als **instrument** om politieke beleidsdoelen te realiseren, komt deze losser te staan van de **normatieve uitgangspunten** en opvattingen die binnen het recht relevant zijn. De relatie tussen middel en doel wordt dan al snel uit het oog verloren. Op basis van de wet voor de

CoronaMelder kunnen GGD-hulpverleners en onderzoekers bijvoorbeeld moeilijk vaststellen wanneer welke data, zoals de app-data en de gegevens over de afspraak met de teststraat, beschermd worden door het beroepsgeheim, laat staan achterhalen welke belangenafwegingen hieraan ten grondslag liggen.

- Het is bij **onderzoeken met AI**, zoals die met *machine learning* of *natural language processing*, niet altijd helder of nWMO-onderzoek dat voldoet aan de WGBO-eis 'statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid, ten behoeve van het algemeen belang' aan de orde is. Waar ligt bijvoorbeeld het **onderscheid tussen wetenschappelijk onderzoek met AI en het (verder) ontwikkelen en optimaliseren van een AI-toepassing in de zorg?**
- Commerciële partijen die gegevens uit medische dossiers voor eigen doeleinden willen gebruiken of een vergaande zeggenschap hebben over de te verwerken gegevens uit medisch dossiers, **kunnen belangen hebben die niet vallen onder de 'algemeen belang'-eis**. Dat betekent dat de WGBO hen geen ruimte biedt om zonder toestemming gegevens uit medische data te gebruiken. Als hulpverleners hier niet scherp op letten, kunnen gegevens onbedoeld zonder toestemming worden vrijgegeven.
- Bij de totstandkoming van de WGBO is niet aan de orde gekomen of commerciële partijen betrokken bij onderzoek dat een 'algemeen belang' dient, **de vruchten mogen plukken** van de verwerkingen van gegevens uit medische dossiers. De vraag is of hulpverleners het verdienen aan gegevens uit medische dossiers mogen toelaten, **zonder dat de patiënt daarvoor toestemming heeft gegeven**. Zo ja, onder welke voorwaarden? Zo nee, waarom niet?

Oplossingsrichtingen

- Het kan een keuze van de wetgever zijn, om nWMO-onderzoek te doen met gegevens die verzameld worden met de CoronaMelder app. Dergelijke keuzes dient de wetgever te **expliciteren en te plaatsen in de context van de relevante kernwaarden en rechtsbeginselen**, waarmee rechten van burgers worden gewaarborgd en hen bescherming wordt geboden. Die beginselen omvatten onder meer publieke gezondheid, individuele vrijheid als de bescherming van persoonsgegevens en eerbiediging van het privéleven, en wetenschapsvrijheid.
- De wetgever dient in het bijzonder uit te leggen **wanneer gegevens onder het beroepsgeheim vallen**, bijvoorbeeld in het kader van de CoronaMelder-app, en wat dat betekent in het licht van de verankerde beginselen.
- De Autoriteit Persoonsgegevens zou kunnen toelichten wat de **reikwijdte is van 'verwerkingen ten behoeve van wetenschappelijk onderzoek of met een statistisch oogmerk'**, en of de **ontwikkeling van AI-tools op basis van dossierdata mogelijk is zonder toestemming**. Het ligt voor hand om de EU-

privacytoezichthouders, verenigd in de EDPB, hierbij te betrekken. De begrippen 'wetenschappelijk onderzoek' en 'statistiek' moeten namelijk autonoom uitgelegd worden binnen de Europese rechtsorde.

- Dit onderwerp verdient een **brede maatschappelijke discussie**. Kamerleden kunnen daarin een voorzet doen, bijvoorbeeld door relevante partijen uit te nodigen voor rondetafelgesprekken. Die partijen zijn in ieder geval patiënten, beroepsbeoefenaren, onderzoekers, technologie-aanbieders en sponsors van onderzoeken.
- Naar aanleiding van deze brede maatschappelijke discussie, kan de wetgever overwegen om de WGBO-wetgeving aan te passen.

5.3 De praktijk vraagt om extra uitleg over toestemming, de reikwijdte ervan en 'geen bezwaar'

Toestemming vragen voor onderzoek, nagaan of toestemming vereist is, of het inrichten van een 'geen-bezwaar systeem'. Dit zijn tijdrovende, ogenschijnlijk soms onmogelijke taken, die nodig zijn om nWMO-onderzoek binnen de wettelijke kaders uit te kunnen voeren. 'Het veld' vraagt om verheldering en steun.

Onze derde deelvraag luidde daarom: Zijn de regels rond het krijgen van toestemming van de patiënt helder genoeg of kan dat beter?

Paragraaf 4.2.3 besprak een **knelpunt** bij de beantwoording van deze vraag. In paragraaf 5.3 trekken we overkoepelende conclusies en schetsen vervolgens daaraan verbonden oplossingsrichtingen.

Conclusies

- Het '**geen-bezwaarsysteem**' wordt in veel ziekenhuizen **gebruikt om nWMO-onderzoek te faciliteren, maar dat gebeurt soms op de verkeerde manier**. Veel ziekenhuizen gaan er namelijk vanuit, dat als de patiënt geen bezwaar heeft geuit, de gegevens dan gebruikt mogen worden door onderzoekers. De ziekenhuizen gaan voorbij aan het uitgangspunt dat 'geen bezwaar' pas aan de orde komt, als eerst is vastgesteld dat er geen toestemming gevraagd *hoeft* te worden.
- 'Kleine' hulpverleners, zoals tandartsen, apothekers of optometristen zouden gebaat kunnen zijn bij een **centraal geen-bezwaarsysteem**.
- De wens blijft bestaan om slechts een '**globale toestemming**' voor wetenschappelijk onderzoek of statistiek te hoeven vragen, bijvoorbeeld in gevallen waarbij onderzoekers de omvang en reikwijdte van hun onderzoek

niet volledig kunnen formuleren. De Europese privacytoezichthouders, verenigd in de EDPB, geven de voorkeur aan het vragen van **toestemming in fases**. Hierop bestaat **kritiek**.

Oplossingsrichtingen

- Er moet geïnvesteerd worden in **voorlichting, om de verwarring rond ‘geen bezwaar’ en ‘toestemming vragen’ weg te nemen** bij hulpverleners, aan wie wordt gevraagd gegevens ter beschikking te stellen aan nWMO-onderzoek. Hier ligt een voorlichtende taak voor beroepsorganisaties van de hulpverleners, het Ministerie van VWS en de Autoriteit Persoonsgegevens.
- Nader onderzoek zou moeten uitwijzen, of **in de praktijk de bezwaarmogelijkheid afdoende wordt gefaciliteerd en of patiënten voldoende op de hoogte zijn van hun rechten**. Als dat niet het geval is, dan kan overwogen worden om de *best practice* van Amsterdam UMC breed toe te passen in de zorg. Bijvoorbeeld door verankering van deze praktijk in de WGBO of in de gedragscode die momenteel wordt herzien. Die *best practice* betreft het bieden van een extra mogelijkheid aan patiënten om bezwaar aan te tekenen – los van de algemene bezwaarprocedure – als het vragen van toestemming in redelijkheid niet kan worden verlangd.
- Daarnaast kan **nader onderzoek uitwijzen of een centraal ‘geen-bezwaarsysteem’ een oplossing kan zijn voor eventueel geconstateerde uitvoeringsproblemen**. Een dergelijk systeem kan, vergelijkbaar met het donorregister, patiënten in de gelegenheid stellen om hun bezwaar kenbaar te maken. Onderzoekers en hulpverleners zouden die status eenvoudig kunnen opvragen, hetgeen hun administratieve lasten kan doen verminderen.
- De nationale wetgever of de AP (en/of de EDPB) zouden de onduidelijkheid kunnen wegnemen door **concreet de vraag te beantwoorden of de ‘uitdrukkelijke toestemming’ uit de AVG hetzelfde is als de “uitdrukkelijke toestemming” uit de UAVG of de “toestemming” uit de WGBO**. Als de begrippen hetzelfde zijn, dan ligt het voor de hand de ‘gefaseerde toestemming’ van de EDPB te volgen. Maar als de begrippen van elkaar verschillen, dan dient uitleg te worden gegeven wat hiervan de gevolgen zijn.

5.4 Tot slot

In hoofdzaak constateren we de volgende **aandachtspunten voor wetgever, beroeps- en belangenverenigingen en ministeries**, die om een oplossing vragen:

- De huidige wetgeving rond nWMO-onderzoek, waarbij vooral de WGBO, AVG en Uitvoeringswet AVG van toepassing zijn, is niet zozeer belemmerend, maar moet wel op veel punten **verhelderd en beter op elkaar afgestemd worden**;

- Bij nWMO-onderzoek dat is gebaseerd op gegevens die worden gegenereerd of gedeeld met nieuwe vormen van technologie, ontstaat druk op fundamentele rechten, zoals de **bescherming van persoonsgegevens en de eerbiediging van het privéleven**. Een cruciale vraag is, wanneer gegevens beschermd worden onder het beroepsgeheim (en dus de WGBO-regels gevolgd moeten worden) en wanneer dit niet het geval is. Die problemen worden zichtbaar bij *quantified self*, gebruik van een interactief portaal tussen patiënt en hulpverlener, maar ook bij de *Personal Health Train*;
- Op de vraag **of commerciële partijen toegang mogen hebben tot de gegevens uit medische dossiers**, zelfs voor *for profit* onderzoek, is nu nog geen antwoord te geven. De ruimte voor commerciële partijen om te verdienen in het kader van nWMO-onderzoek waarvan het de bedoeling is dat het een algemeen belang moet dienen, moet **maatschappelijke worden verkend**;
- De praktijk van nWMO-onderzoek vraagt om **extra uitleg over het vragen van toestemming van patiënten, de reikwijdte van de toestemming en het onderwerp ‘geen bezwaar’** tegen gebruik van medische gegevens. Een structuur om vragen van toestemming te faciliteren en/of een (centraal) geen-bezwaarsysteem worden gemist in het veld.

Dit hoofdstuk heeft een reeks oplossingsrichtingen geboden. Een deel daarvan kan relatief snel in gang worden gezet. Andere vereisen bijvoorbeeld uitgebreid overleg binnen Europa of een maatschappelijke discussie. Zo kan het pad worden geëffend om nWMO-onderzoek op termijn eenvoudiger én volledig volgens de wet te kunnen uitvoeren.

De eerste stappen die gemaakt moeten worden zijn:

- het verhelderen van de wet- en regelgeving binnen Nederland en binnen Europa;
- het ondersteunen van kleinere hulpverleners bij de nWMO-vraagstukken;
- het organiseren van een brede toestemmingsmogelijkheid en/of van een centraal bezwaarregistratiesysteem; en
- het voeren van een maatschappelijke discussie over verdienopties van bedrijven met nWMO-onderzoek.

Ons rapport draagt bij aan een geïnformeerd gesprek over **hoe** de huidige juridische kaders het nWMO-onderzoek mogelijk bemoeilijken en **wat** daarvoor de oplossingen zijn.

Goede afwegingen maken over het beschikbaar maken of het gebruiken van medische gegevens zijn belangrijke verantwoordelijkheden voor hulpverleners en onderzoekers. Zeker nu de hoeveelheid van digitale medische data en vraag naar nWMO-onderzoek, waaronder *big data* analyse, gestaag toeneemt. **Nut en doel**

van nWMO-onderzoek moeten steeds goed worden beoordeeld, alvorens de hulpverlener overgaat tot verstrekken van gegevens uit medische dossiers. *Big data* analyses leiden maar al te vaak tot triviale conclusies die geen handelingsperspectief bieden. Analyses met kleinere datasets, evenwel met data van goede kwaliteit, kunnen belangrijkere inzichten geven voor de volksgezondheid dan het hypothesevrij *crunchen*. Kleinschalige data-analyse geeft tevens veel meer garanties, dat data niet buiten de context waarbinnen ze zijn verzameld of tot schade van patiënten worden gebruikt.

Daarnaast is belangrijk dat onderzoekers, met name als bedrijven betrokken zijn, **transparant zijn over wat er met de data van individuen gebeurt**. Wie gebruikt de data en voor wat? Welke rol laten we commerciële partijen hierbij hebben?

Alle spelers bij nWMO-onderzoek moeten zich voortdurend bewust blijven van hun verantwoordelijkheden. Ook de overheid, die onder druk soms belangrijke maatschappelijke doelen wil bereiken met nWMO-onderzoek. Daarbij raken cruciale zaken als bescherming van het beroepsgeheim op de achtergrond, zeker als daar nieuwe digitale technologie bij wordt gebruikt, zoals apps. Gevoelige persoonlijke gegevens raken met de nieuwe technologie en nieuwe spelers maar al te gemakkelijk buiten het medische domein. En in wiens handen komen de conclusies van het onderzoek? Wat wordt ermee gedaan, en is dat in het belang van de patiënten? Is de institutionele context waarin de inzichten of ontwikkelde technologie terecht komen voldoende meegenomen? Alleen door zich voortdurend de bijzondere status van deze gegevens te realiseren, kan met respect voor mensen onderzoek en innovatie worden gedaan. Pas dan kan datasolidariteit realiteit worden.

Referenties

Agencia Española de Protección de Datos (AEPD) (2020). RGPD compliance of processings that embed Artificial Intelligence An introduction, 24 february 2020, https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia-en_0.pdf.

Autoriteit Persoonsgegevens (2019). Rapport naar aanleiding van onderzoek gegevensverwerking SBG, definitief rapport, 16 december 2019, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapport_bevindingen_sbg_en_akwa_ggz.pdf.

Autoriteit Persoonsgegevens (2020). Over de anonimiteit van geaggregeerde telecomlocatiedata, april 2020, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/anonimiteit_en_geaggreerde_telecomdata.pdf.

Becker, R., Thorogood, A., Ordish, J., Beauvais, M.J. (2020) COVID-19 Research: Navigating the European General Data Protection Regulation, *Journal of Medical Internet Research*, Vol. 22, No. 8, 27 augustus 2020, <https://doi.org/10.2196/19799>.

Berliner Beauftragte für Datenschutz und Informationsfreiheit (2020). 'Nach „Schrems II“: Europa braucht digitale Eigenständigkeit', 17 juli 2020, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf.

Buijsen, M., Olga, F., Hulst, E., Van Noord, T. (2020). *Medisch beroepsgeheim in dubio - de verhouding van het medisch beroepsgeheim tot zwaarwegende maatschappelijke belangen*, eindrapport iBMG en Erasmus Universiteit Rotterdam, 1 oktober 2012, <https://zoek.officielebekendmakingen.nl/blg-203150.pdf>.

College Bescherming Persoonsgegevens (CBP) (2002). Privacy bij wetenschappelijk onderzoek en statistiek – kader voor een gedragscode, mei 2002, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rapporten/rap_2002_privacy_statistiek.pdf.

College Bescherming Persoonsgegevens (CBP) (2005). Landelijke zorgregistraties, maart 2005, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rapporten/rap_2005_zorgregistraties.pdf.

Centre for Data Ethics and Innovation (CDEI) (2020). *Independent report - Addressing trust in public sector data use*, 20 juli 2020, <https://www.gov.uk/government/publications/cdei-publishes-its-first-report-on-public-sector-data-sharing/addressing-trust-in-public-sector-data-use>.

Datenethikkommission (2020). Opinion of the Data Ethics Commission, 22 januari 2020, https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.pdf.

Dove, E.S., Chen J. (2020). Should consent for data processing be privileged in health research? A comparative legal analysis, *International Data Privacy Law*, Vol. 10, No. 2, mei 2020, Pages 117–131, <https://doi.org/10.1093/idpl/ipz023>.

Dove, E. (2018). The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. *Journal of Law, Medicine & Ethics*, Vol. 46, No. 4, 29 augustus 2018; Edinburgh School of Law Research Paper No. 2018/28, <http://dx.doi.org/10.2139/ssrn.3240459>.

Datenschutzkonferenz (2020). 'Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II“) stärkt den Datenschutz für EU-Bürgerinnen und Bürger', https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf.

European Court of Human Rights (2015). Thematic report - Health-related issues in the case-law of the European Court of Human Rights, juni 2015, https://www.echr.coe.int/Documents/Research_report_health.pdf.

European Court of Human Rights (2019). *Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life, home and correspondence*, 31 augustus 2019.

European Data Protection Board (EDPB) (2020). *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*, 21 april 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en.

European Data Protection Board (EDPB) (2020). *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 mei 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

European Data Protection Board (EDPB) (2020). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of*

personal data, Adopted on 10 November 2020 – version for public consultations, http://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

European Data Protection Supervisory (2020). *A Preliminary Opinion on data protection and scientific research*, 6 januari 2020, https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en.

Europese Commissie (2020). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *A European strategy for data*, COM(2020) 66 final, Brussel, 19 februari 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>.

EY (2019). *Realising the value of healthcare data: a framework for the future*, 19 juli 2019, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/life-sciences/life-sciences-pdfs/ey-value-of-health-care-data-v20-final.pdf

Garcia-Vidal, C., Moreno-García, E., Hernández-Meneses, M., Puerta-Alcalde, P., Chumbita, M., Garcia-Pouton, N., Linares, L., Rico, V., Cardozo, C., Martínez, J.A., García, F., Mensa, J., Castro, P., Nicolás, J.M., Muñoz, J., Vidal, D. and Soriano, A. (2020). *Personalized therapy approach for hospitalized patients with COVID-19*. *Clinical Infectious Diseases*, <https://eithhealth.eu/news-article/artificial-intelligence-tool-aiding-personalised-covid-19-treatment-decisions-demonstrates-50-percent-reduction-in-mortality/>.

Gezondheidsraad (2000). *De bewaartermijn voor medische gegevens*, 27 juni 2000, <https://www.gezondheidsraad.nl/documenten/adviezen/2000/06/27/de-bewaartermijn-voor-medische-gegevens-signalement>.

Hacker, Philipp, *A Legal Framework for AI Training Data* (March 18, 2020). *Law, Innovation and Technology* (forthcoming). Available at SSRN: <https://ssrn.com/abstract=3556598> or <http://dx.doi.org/10.2139/ssrn.3556598>

Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (2020). *'Schwere Zeiten für den internationalen Datenaustausch'*, 16 juli 2020, <https://datenschutz-hamburg.de/pressemitteilungen/2020/07/2020-07-16-eugh-schrems>.

Information Commissioner's Office (ICO) (2018). *'Big data, artificial intelligence, machine learning and dataprotection'*, 2018, <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

Klopotowska, J.E. (2020). AI WILL SEE YOU NOW - Het perspectief van de arts en de patiënt op een verantwoorde toepassing van Artificiële Intelligentie (AI) ter ondersteuning van medische beslissingen, SIDN Fonds, 17 juli 2020. <https://www.amc.nl/web/research-75/departments/medical-informatics-1/medical-informatics-1/rapport-ai-will-see-you-now-het-perspectief-van-de-arts-en-de-patient-op-een-verantwoorde-toepassing-van-artificiele-intelligentie-ai-ter-ondersteuning-van-medische-beslissingen.-.htm>.

Kuner, C. (2020). 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation', 17 juli 2020, <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/>.

Lee, K-F (2020). Covid-19 Will Accelerate the AI Health Care Revolution, Wired, 22 mei 2020, <https://www.wired.com/story/covid-19-will-accelerate-ai-health-care-revolution/>.

Legemaate, J. Wikken en wegen. Gezondheidsrecht in beweging, Vossiuspers UvA, Amsterdam, 2011, <https://arils.uva.nl/nl/content/evenementen/oraties/2011/05/mei-2011-inaugurele-rede-johan-legemaate.html>.

Lomas, N. (2019) 'Google has used contract swaps to get bulk access terms to NHS patient data | TechCrunch', 22 oktober 2019, <https://techcrunch.com/2019/10/22/google-has-used-contract-swaps-to-get-bulk-access-terms-to-nhs-patient-data/>.

Marill, M.C. (2020). 'Doctors Are Pooling Data to Help Understand Covid-19', Wired, 25 maart 2020, <https://www.wired.com/story/doctors-are-pooling-data-to-help-understand-covid-19/>.

Ministerie van Volksgezondheid, Welzijn & Sport (2016). Bijlage bij Kamerbrief van de Minister van Volksgezondheid, Welzijn & Sport, 34300 XVI, nr. 161, 'Basisprincipes medisch beroepsgeheim', 15 juni 2016, <https://www.rijksoverheid.nl/documenten/rapporten/2016/06/15/basisprincipes-medisch-beroepsgeheim>.

Ministerie van Volksgezondheid, Welzijn & Sport (2020a). Niet-WMO-plichtig onderzoek en ethische toetsing, 14 februari 2020, <https://www.rijksoverheid.nl/documenten/rapporten/2020/02/14/niet-wmo-plichtig-onderzoek-en-ethische-toetsing>.

Ministerie van Volksgezondheid, Welzijn & Sport (2020b). *Beleidslijn inzake het verzamelen van onderzoeksdata en doorgifte buiten EU vanwege COVID-19*, 14 april 2020, <https://www.datavoorgezondheid.nl/documenten/publicaties/2020/04/15/beleidslijn-inzake-het-verzamelen-van-onderzoeksdata-en-doorgifte-buiten-eu-vanwege-covid-19>.

Mitrou, L. (2018). Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'? (December 31, 2018). Available at SSRN: <https://ssrn.com/abstract=3386914> or <http://dx.doi.org/10.2139/ssrn.3386914>.

Mostert, M. (2018). 'Big data, medisch-wetenschappelijk onderzoek en gegevensbescherming', in: Vereniging voor Gezondheidsrecht, *Big data in de zorg*, Den Haag: SDU 2017.

Nictiz (2019). 'Artificial intelligence in de zorg'. Auteurs: Wouda, F., Hutink, H., 15 januari 2019, <https://www.nictiz.nl/rapporten/artificial-intelligence-in-de-zorg/>.

NordForsk, N. (2019). A vision of a Nordic secure digital infrastructure for health data: The Nordic Commons, <http://urn.kb.se/resolve?urn=urn:nbn:se:norden:org:diva-5826>.

Patiëntenfederatie Nederland (2019a). *Het Patiëntengeheim – position paper Patiëntenfederatie Nederland*, Utrecht 17 januari 2019, <https://www.patiëntenfederatie.nl/downloads/organisatie/220-patientengeheim/file>.

Patiëntenfederatie Nederland (2019b). *Rapport: Delen van uw data - Hergebruik van gezondheidsgegevens en lichaamsmateriaal voor wetenschappelijk onderzoek*, november 2019, <https://www.patiëntenfederatie.nl/downloads/rapporten/154-rapport-delen-van-je-data/file>.

PBLQ (2016). Onderzoek naar de beveiliging van patiëntgegevens, 1 december 2016, <https://zoek.officielebekendmakingen.nl/blg-793485.pdf>.

PBLQ (2019). 'Duurzame aanlevering OECD-indicatoren gezondheidszorg', oktober 2019, https://www.volksgezondheidenzorg.info/sites/default/files/eindrapport_oecd-indicatoren_gezondheidszorg_v1.0.pdf.

Peloquin, D., DiMaio, M., Bierer, B. et al. (2020). *Disruptive and avoidable: GDPR challenges to secondary research uses of data*. Eur J Hum Genet 28, 697–705 (2020). <https://doi.org/10.1038/s41431-020-0596-x>.

Piai, S., Allocato, A., Besana, G. (2020). *Update of the European Data Market SMART 2016/0063: Story 6 – The Secondary Use of Health Data and Data-driven Innovation in the European Healthcare Industry*, <http://datalandscape.eu/data-driven-stories/story-6-secondary-use-health-data-and-data-driven-innovation-european-healthcare>.

Piechaud-Boura, M., Dumortier, J. (eds.) (2018). *D7.1 - Legal Assessment: 'Big data' analytics and the processing of health data for scientific research purposes*, AEGLE, 29

augustus 2018, https://www.timelex.eu/sites/default/files/2018-12/01.%20AEGLE_D7.1_LEGAL_ASSESSMENT_FINAL.pdf.

Ploem, M.C. (2000). 'Medisch-wetenschappelijk onderzoek met gecodeerde gegevens. De toepasselijkheid van privacywetgeving', *Computerrecht* 2000, p. 69-75.

Ploem, M.C. (2004). *Tussen privacy en wetenschapsvrijheid. Regulering van gegevensverwerking voormedisch-wetenschappelijk onderzoek (diss.)*, reeks *gezondheidsrecht*, Den Haag: Sdu Uitgevers 2004, <https://hdl.handle.net/11245/1.240075>.

Ploem, M.C. (2006). De regeling inzake het gebruik van patiëntengegevens voor wetenschappelijk onderzoek in de WGBO. *TGVR* 6-2006, 30, 348 (2006). <https://doi.org/10.1007/BF03056270>.

Ploem, M.C. (2013). 'EU-verordening gegevensbescherming en medisch-wetenschappelijk onderzoek: een moeizaam evenwicht', *Tijdschrift voor Gezondheidsrecht* 2013, afl. 6, pp. 521-527.

Ploem, M.C., Rigter, T. & Gevers, J.K.M. (2020). *Medisch data-onderzoek in het AVG-tijdperk: een zoektocht naar de juiste regels*. *TvGR* 2020, afl. 2.

Prins, J. E. J., & Berkvens, J. M. A. (Eds.) (2007). *Privacyregulering in theorie en praktijk*. (Recht en Praktijk; No. 75). Deventer: Kluwer.

Rabesandratana T. (2019). *Researchers sound alarm on European data law*. *Science*. 2019;366(6468):936. <https://doi:10.1126/science.366.6468.936>.

Rathenau Instituut (2014). *Eerlijk advies - De opkomst van de e-coach*. Den Haag (auteurs: Kool L., J. Timmer en R. van Est (red.)) <https://www.rathenau.nl/nl/digitale-samenleving/eerlijk-advies>.

Rathenau Instituut (2016). *De Meetbare Mens. Het digitaal meten van het zieke en gezonde lichaam*. Den Haag (auteurs: Geesink, I., M. Heerings & S. van Egmond) <https://www.rathenau.nl/nl/digitale-samenleving/de-meetbare-mens>.

Rathenau Instituut (2017). *Opwaarderen - Borgen van publieke waarden in de digitale samenleving*. Den Haag (auteurs: Kool L., J. Timmer en R. van Est (red.)) <https://www.rathenau.nl/nl/digitale-samenleving/opwaarderen>.

Rathenau Instituut (2018a). *Doelgericht digitaliseren – Hoe Nederland werkt aan een digitale transitie waarin mensen en waarden centraal staan*. Den Haag (auteurs: Kool, L., E.

Dujso, en R. van Est) <https://www.rathenau.nl/nl/digitale-samenleving/doelgericht-digitaliseren>.

Rathenau Instituut (2018b). Digitale gezondheidsregie – Meer gegevens, meer grip? Den Haag (auteurs: M.G.H. Niezen & P. Verhoef) <https://www.rathenau.nl/nl/maakbare-levens/digitale-gezondheidsregie>.

Rathenau Instituut (2019a). Gezondheid centraal – Zorgvuldig data delen in de digitale samenleving. Den Haag (auteurs: Niezen, M.G.H., R. Edelenbosch, L. van Bodegom & P. Verhoef). <https://www.rathenau.nl/nl/maakbare-levens/gezondheid-centraal>

Rathenau Instituut (2019b), 'Bericht aan parlement - Gegevensuitwisseling in de zorg', 3 oktober 2019, <https://www.rathenau.nl/nl/maakbare-levens/gegevensuitwisseling-de-zorg>.

Rathenau Instituut (2020a), 'Bericht aan parlement – Zeven acties voor verantwoord innoveren met AI, 3 maart 2020, <https://www.rathenau.nl/nl/digitale-samenleving/zeven-acties-voor-verantwoord-innoveren-met-ai>.

Rathenau Instituut (2020b), 'Artikel in blogserie Gezonde Bytes: Innoveren met AI in de zorg: 'Eerst de data op orde brengen', 7 mei 2020, <https://www.rathenau.nl/nl/maakbare-levens/innoveren-met-ai-de-zorg-eerst-de-data-op-orde-brengen>.

Rathenau Instituut (2020c), 'Response of the Rathenau Instituut on the European Commission's White Paper on Artificial Intelligence, 15 mei 2020, <https://www.rathenau.nl/en/digitale-samenleving/eu-ensure-ai-makes-us-more-sustainable-healthier-freer-and-safer>.

Rathenau Instituut (2020d), 'Reactie op de Verzamelwet gegevensbescherming', 14 juli 2020, <https://www.rathenau.nl/nl/maakbare-levens/wetgever-moet-persoonlijke-gegevens-van-burgers-beter-beschermen>.

Rathenau Instituut (2020e), 'Bericht aan parlement - Overwegingen naar aanleiding van de Kamerbrief introductie "CoronaMelder", 5 augustus 2020, <https://www.rathenau.nl/nl/digitale-samenleving/plannen-voor-coronamelder-vragen-om-verduidelijking>.

Rijksoverheid (2019). *Strategisch Actieplan voor Artificiële Intelligentie*, 8 oktober 2019, <https://www.rijksoverheid.nl/documenten/beleidsnotas/2019/10/08/strategisch-actieplan-voor-artificiele-intelligentie>.

RIVM (2011). Uitvoeringstoets bevolkingsonderzoek naar darmkanker - Opsporing van darmkanker in praktijk gebracht. <https://zoek.officielebekendmakingen.nl/blg-117056.pdf>.

RIVM (2017). Juridisch kader gegevensuitwisseling bevolkingsonderzoeken naar kanker, v.1.0, december 2017, <https://www.rivm.nl/documenten/juridisch-kader-gegevensuitwisseling-bevolkingsonderzoeken-naar-kanker>.

RIVM (2019). *Handreiking ontsluiting patiëntgegevens voor wetenschappelijk onderzoek*, juli 2019, <https://www.rivm.nl/documenten/handreiking-ontsluiting-patientgegevens-voor-wetenschappelijk-onderzoek>.

Scholte, R., Kranendonk, E., Paardekooper, M. et al. (2019). Hergebruik van patiëntgegevens voor wetenschappelijk onderzoek: op weg naar eenduidige spelregels. *Tijdschrift voor gezondheidswetenschappen*, vol. 97, 55–58 (2019). <https://doi.org/10.1007/s12508-019-0213-y>.

Solove, D. (2020). 'Schrems II: Reflections on the Decision and Next Steps', 23 juli 2020, <https://teachprivacy.com/schrems-ii-reflections-on-the-decision-and-next-steps/>.

Spoelstra S. (2020). Van face to face naar zorg op afstand: De ggz na de coronacrisis. *Zorgvisie : vakopinieblad voor de zorgsector*, 50(4), 20–23. <https://doi.org/10.1007/s41187-020-0367-x>.

European Parliamentary Research Service, Scientific Foresight Unit (STOA) (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, juni 2020, [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf).

Struijs, A. (2017). *Omgaan met beroepsgeheim en bescherming persoonsgegevens*, oktober 2017, <https://www.raadrvs.nl/documenten/publicaties/2017/10/10/achtergrondstudie-omgaan-met-beroepsgeheim-en-bescherming-persoonsgegevens>.

Stüssgen, R., Coppen, R., Veen, E-B van, Urbanus, T., Verheij, R. (2019). *Zorggegevens voor onderzoek: bezwaar of toestemming? De wet en de praktijk*. Utrecht: Nivel, 2019, <https://www.nivel.nl/nl/publicatie/zorggegevens-voor-onderzoek-bezwaar-toestemming-de-wet-en-de-praktijk>.

Van Veen, E-B (2004). 'Het beroepsgeheim in de individuele gezondheidszorg', in: Vereniging voor Gezondheidsrecht, *Het beroepsgeheim, continuïteit en verandering*, Sdu Uitgevers 2004.

Veale, M., Binns, R. and Edwards, L. (2018). Algorithms that remember: model inversion attacks and data protection law, *Phil. Trans. R. Soc. A*.37620180083.
<http://doi.org/10.1098/rsta.2018.0083>.

Pekmez, C. (2020). Solidarity Call to Action-01 June 2020 EN, World Health Organization, 2 juni 2020, <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/global-research-on-novel-coronavirus-2019-ncov/covid-19-technology-access-pool/solidarity-call-to-action/docs/default-source/coronaviruse/solidarity-call-to-action/solidarity-call-to-action-01-june-2020>.

WP131: Article 29 Data Protection Working Party (WP29) (2007). *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, WP131, 15 februari 2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf.

WP203: Article 29 Working Party (WP29) (2013). *Opinion 03/2013 on purpose limitation*, WP203, adopted on 2 April 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

WP259: Groep Gegevensbescherming Artikel 29 (WP29) (2018) Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679, laatstelijk herzien en vastgesteld op 10 april 2018, WP259 versie 01,
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf.

Zorginstituut Nederland (2018). *Eindrapportage praktijktoets Personal Health Train*, 23 oktober 2018,
<https://www.zorginstituutnederland.nl/publicaties/rapport/2018/10/23/eindrapportage-praktijktoets-personal-health-train>.

Lijst met gebruikte afkortingen

(U)AVG	AVG en UAVG
AI	Artificial Intelligence ('kunstmatige intelligentie')
AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
CBP	College Bescherming Persoonsgegevens (voorganger van de AP)
C-TAP	COVID-19 Technology Access Pool
DNA	Desoxyribonucleïnezuur, chemische drager van erfelijke informatie
DPIA	Data protection impact assessment ('gegevensbeschermingseffectbeoordeling')
ECG	ElektroCardioGram
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EER	Europese Economische Ruimte
EHRM	Europees Hof voor de Rechten van de Mens
EPD's	Elektronische patiëntendossiers
EU	Europese Unie
EU-Grondrechtenhandvest	Handvest van de grondrechten van de Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
FAIR	Findable, Accessible, Interoperable, Reusable
FG	Functionaris Gegevensbescherming
GGZ	Geestelijke gezondheidszorg
GTS	Gespecificeerde Toestemming Structureel
HvJ EU	Hof van Justitie van de Europese Unie
IGJ	Inspectie Gezondheidszorg en Jeugd
LSP	Landelijk Schakelpunt

METC's	Medisch-ethische toetsingscommissies
NHS	National Health Service
nWMO-onderzoek	Onderzoek dat buiten de reikwijdte valt van de WMO
PGO	Persoonlijke gezondheidsomgeving
PHT	Personal Health Train
RIVM	Rijksinstituut voor Volksgezondheid en Milieu
SCC's	Standard Contractual Clauses
Tw	Telecommunicatiewet
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming
VWS	Volksgezondheid, Welzijn en Sport
Wabvpz	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
Wbp	Wet bescherming persoonsgegevens
Wet BIG	Wet op de Beroepen in de Individuele Gezondheidszorg
WGBO	Wet op de geneeskundige behandelingsovereenkomst (Burgerlijk Wetboek, boek 7, titel 7, afdeling 5)
WMO	Wet medisch-wetenschappelijk onderzoek met mensen
WP	Article 29 Data Protection Working Party
Wpr	Wet persoonsregistraties

Bijlage 1: Verwerking van gezondheidsgegevens en genetische gegevens

Tabel 5 Mogelijkheden om het verbod verwerking bijzondere persoonsgegevens op te heffen

Opheffingsmogelijkheid	Toelichting
Wettelijke plicht	Toestemming is niet aan de orde, als voor een bepaalde gegevensverwerking een wettelijke verplichting nageleefd dient te worden, zoals wettelijk geregelde declaratieverplichtingen. Het naleven van een wettelijke plicht is een rechtsgrond.
Handelingen door hulpverleners en het beheer van hun praktijk ¹⁴⁵ en uitvoering van behandelingsovereenkomst ¹⁴⁶	<p>De AVG-toestemming speelt ook geen rol, zodra hulpverleners de gezondheidsgegevens nodig hebben met het oog op een goede behandeling of verzorging van de betrokkene (lees: de patiënt).</p> <p>Hulpverleners mogen gezondheidsgegevens ook gebruiken als dit nodig is voor het beheer van hun instelling, zoals een ziekenhuis of hun beroepspraktijk. Hieronder valt ook het waarborgen van de kwaliteit van de verleende zorg. Denk aan intercollegiale toetsing door hulpverleners onderling. Ook mag een hulpverlener gegevens gebruiken voor eigen statistisch onderzoek, dus zonder dat hier anderen bij betrokken zijn (WP131, 2007).</p> <p>Voor bovengenoemde gegevensverwerkingen is dus geen AVG-toestemming nodig, omdat dit uit de wet¹⁴⁷ blijkt en omdat deze gegevensverwerking meestal plaatsvindt vanwege de uitvoering van de behandelingsovereenkomst en nodig is voor de zorgpraktijk.</p>
De verwerking is noodzakelijk voor de bescherming van de vitale belangen van de betrokkene of een ander ¹⁴⁸	Dit gaat over de situatie waarin de betrokkene (fysiek of juridisch) niet in staat is zijn toestemming te geven. Deze mogelijkheid is dus niet van toepassing op al het handelen van hulpverleners, maar doet zich slechts voor in 'leven of dood'-kwesties of als er vrees is voor ernstige gezondheidsschade als de gegevens niet worden verwerkt. Bijvoorbeeld als de patiënt in coma ligt of als direct na een verkeersongeluk nagegaan dient te worden welke bloedgroep een bewusteloos slachtoffer heeft.

145 Artikel 30 lid 3 sub a Uitvoeringswet AVG.

146 Artikel 9 lid 2 sub h AVG.

147 Artikel 30 lid 3 sub a Uitvoeringswet AVG.

148 Artikel 9 lid 2 sub c AVG.

<p>Genetische gegevens: verbod op bovenpersoonlijk gebruik, behalve als zwaarwegend geneeskundig belang prevaleert, of er sprake is van medisch data-onderzoek</p>	<p>De verwerking is niet toegestaan als de verwerking zou plaatsvinden met betrekking tot anderen in dezelfde genetische lijn. Het is niet relevant of de betrokkene of enig familielid in dezelfde genetische lijn daarvoor uitdrukkelijke toestemming zou geven.</p> <p>Bovenpersoonlijk gebruik van genetische gegevens is alleen toegestaan, wanneer een zwaarwegend geneeskundig belang prevaleert. Bijvoorbeeld wanneer uit erfelijkheidsonderzoek blijkt dat behandeling van anderen dan de betrokkene (namelijk familieleden) wellicht noodzakelijk is. In dat geval moet het in het belang van die anderen, niet zonder meer verboden zijn om hen daaromtrent te benaderen, mits het medische beroepsgeheim de gegevensverwerking niet in de weg staat.¹⁴⁹</p> <p>Onderzoek met genetische gegevens zonder toestemming is toegestaan, als de verwerking noodzakelijk is voor wetenschappelijk onderzoek in het algemeen belang of statistiek.¹⁵⁰</p>
--	---

Tabel 6 Erkende gronden voor doorbreking van het beroepsgeheim, naast toestemming

Uitzondering	Omschrijving
<p>Op grond van een wettelijke bepaling</p>	<p>De wet kan bepalen dat het beroepsgeheim doorbroken mag worden.¹⁵¹ In zo'n geval moet een hulpverlener de afweging maken of hij van deze mogelijkheid gebruik maakt. In sommige gevallen bepaalt de wet dat de hulpverlener verplicht is informatie aan derden te verstrekken. Denk aan de Wet Publieke Gezondheid op basis waarvan artsen verplicht geconstateerde bepaalde infectieziekten als COVID-19 onverwijld aan de GGD moeten melden.¹⁵² De WGBO zelf bevat ook wettelijke gronden op basis waarvan gegevens mogen worden ingezien omwille van een geoorloofde doorbreking van het beroepsgeheim.</p> <p>Ook voorziet de WGBO in de situatie waarin het verstrekken van informatie aan de vertegenwoordigers van een patiënt mogelijk is, als de patiënt niet goed zelf zijn eigen belangen kan behartigen.¹⁵³ Daarnaast moet een hulpverlener volgens de WGBO een andere hulpverlener consulteren als hij twijfel of hij gegevens aan de patiënt mag onthouden.¹⁵⁴</p>

149 Memorie van Toelichting Uitvoeringswet AVG bij artikel 28 lid 2 sub a, p. 93.

150 Art. 28 lid 2 sub b j.o. lid 3 Uitvoeringswet AVG.

151 art. 7:457 lid 1, laatste volzin BW.

152 Artikel 22 Wet Publieke Gezondheid.

153 art. 7:457 lid 3 BW.

154 art. 7:448 lid 3 BW

<p>De aanwezigheid van een noodtoestand, in de zin van een conflict van plichten</p>	<p>Dit betreft de situatie waarin de hulpverlener in een 'conflict van plichten' komt te verkeren, als hij zich aan zijn medisch beroepsgeheim houdt. Voorbeelden van deze 'noodtoestand' zijn de hulpverlener die kennis heeft over een door de patiënt beraamde moord of kindermishandeling. De hulpverlener dient zelf de afweging te maken op basis van professionele criteria.</p>
<p>Doorbreking van het beroepsgeheim in het geval van zwaarwegende belangen (in het strafrecht: 'zeer uitzonderlijke omstandigheden')</p>	<p>Deze uitzondering is in de rechtspraak van de Hoge Raad ontwikkeld. Een geval waarin zwaarwegende belangen een doorbreking van het beroepsgeheim rechtvaardigt, is als er sprake is van een testament waarvan vermoed wordt dat de erfflater wilsonbekwaam was tijdens het opstellen ervan.¹⁵⁵</p> <p>In het strafrecht wordt er gesproken van 'zeer uitzonderlijke omstandigheden' die een afweging rechtvaardigen tussen het belang van geheimhouding en het belang dat de waarheid aan het licht komt.¹⁵⁶ Ten behoeve van die afweging heeft de Hoge Raad hiervoor relevante factoren uiteengezet.¹⁵⁷</p>
<p>Veronderstelde toestemming</p>	<p>In de zorgpraktijk hanteert men de term 'veronderstelde toestemming'.¹⁵⁸ Hiermee wordt tot uitdrukking gebracht dat voor sommige gegevensverstrekkingen van de hulpverlener aan een ander niet expliciet de toestemming van de patiënt hoeft te worden gevraagd, omdat 'verondersteld' wordt dat de patiënt de toestemming heeft gegeven of zal geven. Denk aan de situatie waarin de patiënt instemt met de doorverwijzing van de huisarts naar medisch specialist en vice versa (RIVM 2017) en de huisarts c.q. specialist medische gegevens opneemt in de verwijsbrief (Buijsen et al. 2012). Ook kan worden gedacht aan spoedeisende situaties, waarin de patiënt niet in staat is om toestemming te geven. Veronderstelde toestemming wordt ook wel in verband gebracht met gegevensdeling tussen hulpverleners die betrokken zijn bij één behandelingsovereenkomst. Deze betrokkenen mogen dan veronderstellen dat de patiënt hiervoor toestemming heeft gegeven, zo luidt de gedachte (Struijs 2017). Hetzelfde geldt voor het gebruik van medische gegevens voor kwaliteitsdoeleinden, zoals bij incidentmeldingen en kwaliteitsvisaties, omdat dit in het verlengde ligt van goede zorgverlening (RIVM 2017). In al deze gevallen kan volgens de KNMG toestemming <i>niet</i> worden verondersteld als de patiënt zijn <i>bezwaar</i> heeft geuit.</p>

155 Hoge Raad 20 april 2001, ECLI:NL:HR2001:AB1201.

156 Hoge Raad, 21 oktober 2008, NJ 2008, 630, HR 27 mei 2008, LJN BC1370, NJ 2008, 407, Hoge Raad, 5 juli 2011, NJ 2011, 416 en Hoge Raad ECLI:NL:HR:2013:BZ9943.

157 Hoge Raad, 28 februari 2012, NJ 2012, 537.

158 KNMG, Richtlijn Omgaan met medische gegevens, par. 7.4.2, <https://www.knmg.nl/richtlijn-omgaan-met-medische-gegevens/>.

Toelichting: De constructie “veronderstelde toestemming” leidt in de praktijk tot allerlei uitvoerings- en interpretatievragen. Het is geen wettelijk begrip en pogingen om de ‘veronderstelde toestemming’ in de wet op te nemen, zijn niet succesvol geweest.¹⁵⁹ Als een hulpverlener spreekt van ‘veronderstelde toestemming’, wordt meestal bedoeld op een situatie die reeds is ondervangen door de AVG, Uitvoeringswet AVG of de WGBO. Voor een verstrekking vanwege wetenschappelijk onderzoek is in ieder geval veronderstelde toestemming niet aan de orde (CBP 2005).

159 Tweede Kamer, vergaderjaar 2017–2018, 34 994, nr. 3, *Memorie van Toelichting Wijziging van Boek 7 van het Burgerlijk Wetboek, de Jeugdwet en enkele andere wetten ter verbetering van patiëntgerichte zorg en het opnemen van een wettelijke regeling voor het inzage-recht in het medisch dossier van een overleden patiënt*, p. 21.

Bijlage 2: Verhouding tussen de (U)AVG en de WGBO

Tabel 7 Verhouding tussen de (U)AVG en de WGBO

Begrip	(U)AVG	WGBO
Beschermde doelgroep	Levende, natuurlijke, personen	Zowel levende als overleden patiënten
Type informatie	Persoonsgegevens, zoals gegevens over gezondheid	Inlichtingen over de patiënt en gegevens uit het dossier
Context relatie	Personen ten opzichte van overheden, bedrijven en andere partijen zoals onderzoeksinstellingen of personen (binnen de reikwijdte van de AVG), ongeacht het bestaan van een contract	Contractuele behandelrelatie tussen hulpverlener en patiënt
Bewaartermijn	Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is	De hulpverlener bewaart het dossier gedurende twintig jaren, te rekenen vanaf het tijdstip waarop de laatste wijziging in het dossier heeft plaatsgevonden, of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit
Recht op wissing	De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de verwerkingsverantwoordelijke moet dit onder meer doen als de betrokkene zijn toestemming heeft ingetrokken en een andere rechtsgrond voor de verwerking ontbreekt.	De hulpverlener vernietigt de gegevens uit het dossier na een daartoe strekkend schriftelijk of elektronisch verzoek van de patiënt, maar dit geldt bijvoorbeeld niet, als het verzoek gegevens betreft waarvan redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de patiënt.

<p>Recht op inzage</p>	<p>De betrokkene heeft het recht om van de verwerkings-verantwoordelijke uitsluitel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens. De verwerkingsverantwoordelijke verstrekt de betrokkene een kopie van de persoonsgegevens die worden verwerkt. Dit recht om een kopie te verkrijgen, doet geen afbreuk aan de rechten en vrijheden van anderen.</p>	<p>De hulpverlener verstrekt aan de patiënt desgevraagd inzage in en/of afschrift van de gegevens uit het dossier. De verstrekking blijft achterwege voor zover dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander.</p> <p>Indien de hulpverlener door inlichtingen over de patiënt dan wel inzage in of afschrift van de gegevens uit het dossier te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij zulks achterwege.</p>
<p>Statistiek of wetenschappelijk onderzoek met gezondheidsgegevens</p>	<p>Het verbod om gezondheidsgegevens te verwerken, is niet van toepassing, indien:</p> <ul style="list-style-type: none"> a. de verwerking noodzakelijk is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden; b. het onderzoek een algemeen belang dient; c. het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost; en d. bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. 	<p>Zonder toestemming van de patiënt, ten behoeve van statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid, kunnen aan een ander desgevraagd inlichtingen over de patiënt of inzage in de gegevens uit het dossier worden verstrekt, indien het vragen van toestemming in redelijkheid niet mogelijk is of het vragen van toestemming in redelijkheid niet kan worden verlangd. Deze verstrekking is slechts mogelijk indien: (a) het onderzoek een algemeen belang dient, (b) het onderzoek niet zonder de desbetreffende gegevens kan worden uitgevoerd, en (c) voor zover de betrokken patiënt tegen een verstrekking niet uitdrukkelijk bezwaar heeft gemaakt.</p>
<p>Anonieme gegevens</p>	<p>De beginselen van de AVG zijn niet van toepassing op anonieme gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon, of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is. De AVG heeft derhalve geen betrekking op de verwerking van dergelijke anonieme gegevens, onder meer voor statistische of onderzoeksdoeleinden.</p>	<p>Van het lichaam afgescheiden anonieme stoffen en delen kunnen worden gebruikt voor medisch statistisch of ander medisch wetenschappelijk onderzoek, voor zover de patiënt van wie het lichaamsmateriaal afkomstig is, geen bezwaar heeft gemaakt tegen zodanig onderzoek en het onderzoek met de vereiste zorgvuldigheid wordt verricht.</p> <p>Onder onderzoek met van het lichaam afgescheiden anonieme stoffen en delen wordt verstaan: onderzoek waarbij is gewaarborgd dat het bij het onderzoek te gebruiken lichaamsmateriaal en de daaruit te verkrijgen gegevens niet tot de persoon herleidbaar zijn.</p>

Minder-jarigen	Als hoofdregel geldt dat, als de betrokkene de leeftijd van zestien jaren nog niet heeft bereikt, in zijn plaats de toestemming van zijn wettelijk vertegenwoordiger (zoals ouders) is vereist. ¹⁶⁰ Een wetsvoorstel beoogt de UAVG-regeling meer in lijn te brengen met de WGBO. ¹⁶¹	Als hoofdregel geldt dat patiënten vanaf twaalf jaar oud hun (privacy)rechten kunnen uitoefenen, zodat zij toestemming dienen te geven naast hun wettelijk vertegenwoordigers. ¹⁶²
Handelings-onbekwamen	<p>Indien de betrokkene onder curatele is gesteld, c.q. ten behoeve van de betrokkene een bewind of mentorschap is ingesteld, is, voor zover het een aangelegenheid betreft waarvoor de betrokkene onbekwaam dan wel onbevoegd is, in de plaats van de toestemming van de betrokkene die van zijn wettelijk vertegenwoordiger vereist (artikel 5 lid 2 UAVG).</p> <p>Het voorgaande betekent dat in het geval van bewindvoering, de betrokkene in staat is om toestemming te geven voor secundair gebruik van gegevens voor onderzoek.¹⁶³</p>	Het gaat hier om de patiënt die niet 'in staat kan worden geacht tot een redelijke waardering van zijn belangen ter zake.' In zulke gevallen wordt de patiënt wettelijk vertegenwoordigd, behalve in nood-situaties waarin de hulpverlener de beslissingen mag nemen ten behoeve van de patiënt. De vertegenwoordiger kan in voorkomende gevallen bestaan uit een familielid. ¹⁶⁴

160 Artikel 5 lid 1 UAVG. Zie ook lid 3 met betrekking tot de uitoefening van de rechten van betrokkenen.

161 <https://www.internetconsultatie.nl/verzamelwetgegevensbescherming>.

162 Research Protocol by at MedLawconsult, Evert-Ben van Veen in The Hague, *The Netherlands, 'Big data analytics' and processing of health data for scientific research purposes : the Dutch legal framework*, <https://www.timelex.eu/sites/default/files/2019-01/31.%20Dutch%20legal%20framework.pdf>.

163 *Idem*.

164 *Idem*.

Bijlage 3: Toestemming volgens de AVG

De AVG-toestemming is elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de patiënt de hem betreffende verwerking van persoonsgegevens aanvaardt.

Actieve handeling

Een wilsuiting is hier een ondubbelzinnige actieve handeling, of een verklaring van de patiënt. Een actieve handeling is bijvoorbeeld het aanvinken van een vakje en daarna klikken op een 'ik ga toestemming'-knop. Of denk aan een elektronische handtekening waarmee een patiënt akkoord geeft aan een hulpverlener om het dossier door te sturen voor een second opinion (EDPB Guidelines 05/2020). De patiënt moet zich ervan bewust zijn dat hij/zij toestemming geeft en tot hoever de toestemming reikt. Een verklaring mag schriftelijk zijn, maar ook mondeling, zolang uit die verklaring blijkt dat de patiënt vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt (EDPB Guidelines 05/2020).

Passieve gedragingen leiden niet tot rechtsgeldige AVG-toestemming. Dus: stilzwijgen, het gebruik van vooraf aangevinkte vakjes of inactiviteit mag niet als toestemming gelden. Ook een situatie waarin een patiënt actief *bezwaar* moet maken als hij/zij het niet eens is met het gegevensgebruik, geldt niet als een rechtsgeldige AVG-toestemming. Voor een geldige AVG-toestemming dient een actieve handeling te worden gefaciliteerd.

Toestemming moet 'vrijelijk' worden verleend

De AVG-toestemming moet vrijelijk worden verleend. Situaties waarin de toestemming wordt geacht *niet* vrijelijk te zijn verleend, zijn:

- als geen afzonderlijke toestemming kan worden gegeven voor verschillende persoonsgegevensverwerkingen, ondanks het feit dat dit in het individuele geval passend is;
- als de uitvoering van een overeenkomst (waaronder dienstverlening) afhankelijk is van de toestemming, ondanks het feit dat zulke toestemming niet noodzakelijk is voor de uitvoering van de overeenkomst en/of de dienstverlening;
- als de patiënt zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen.

De context waarin toestemming wordt gevraagd is belangrijk. De (online) dienstverlening van een hulpverlener, mag bijvoorbeeld niet afhankelijk worden gesteld van de toestemming van een patiënt, als het weigeren van de toestemming ertoe leidt dat de patiënt niet (of niet goed) geholpen kan worden (WP131, 2007).

Wie moet toestemming vragen en wat moet diegene doen?

De AVG-toestemming wordt gevraagd door de verwerkingsverantwoordelijke. Dat is de persoon of de partij die het doel (of de doelen) vaststelt van het gegevensgebruik. De AVG-toestemming die wordt gevraagd, heeft betrekking op de gegevensverwerkingen waarvoor de betreffende partij zelf (of samen met anderen) als verwerkingsverantwoordelijke(n) geldt. De verwerkingsverantwoordelijke partij is meestal de onderzoeker, al dan niet tezamen met de hulpverlener (zoals een ziekenhuis).

Als er meerdere verwerkingsverantwoordelijken zijn, dan verwacht de AVG dat de partijen onderling in een 'regeling' afspraken maken over wie verantwoordelijk is voor de uitvoering van de AVG-verplichtingen in de praktijk. Bijvoorbeeld wie de AVG-verzoeken van patiënten, zoals patiënten, zal beantwoorden.¹⁶⁵

Als toestemming is gevraagd voor het gegevensgebruik, dan gelden de hieronder uiteengezette eisen (zie Tabel 8).

Afzonderlijke toestemming

Daarnaast moet de verwerkingsverantwoordelijke soms rekening houden met afzonderlijke toestemming. De gevraagde toestemming moet gelden voor alle gegevensgebruik die hetzelfde doel (of dezelfde doeleinden) dient. Als het gegevensgebruik meerdere doeleinden heeft, dan moet de toestemming voor elkaar daarvan – afzonderlijk – worden verleend.

Gebundelde toestemmingen, zodat de patiënt maar één akkoord hoeft te geven op verschillende activiteiten, voldoen waarschijnlijk *niet* aan de AVG. Dus: als voor verschillende doelen om toestemming wordt gevraagd, is het van belang om per doel de persoon zijn/haar toestemming te laten geven. Bijvoorbeeld door het aankruisen van een invulvakje. In de praktijk gebeurt dit nog steeds veel op papier.

Tabel 8 Eisen wanneer toestemming is gevraagd voor gegevensverbruik

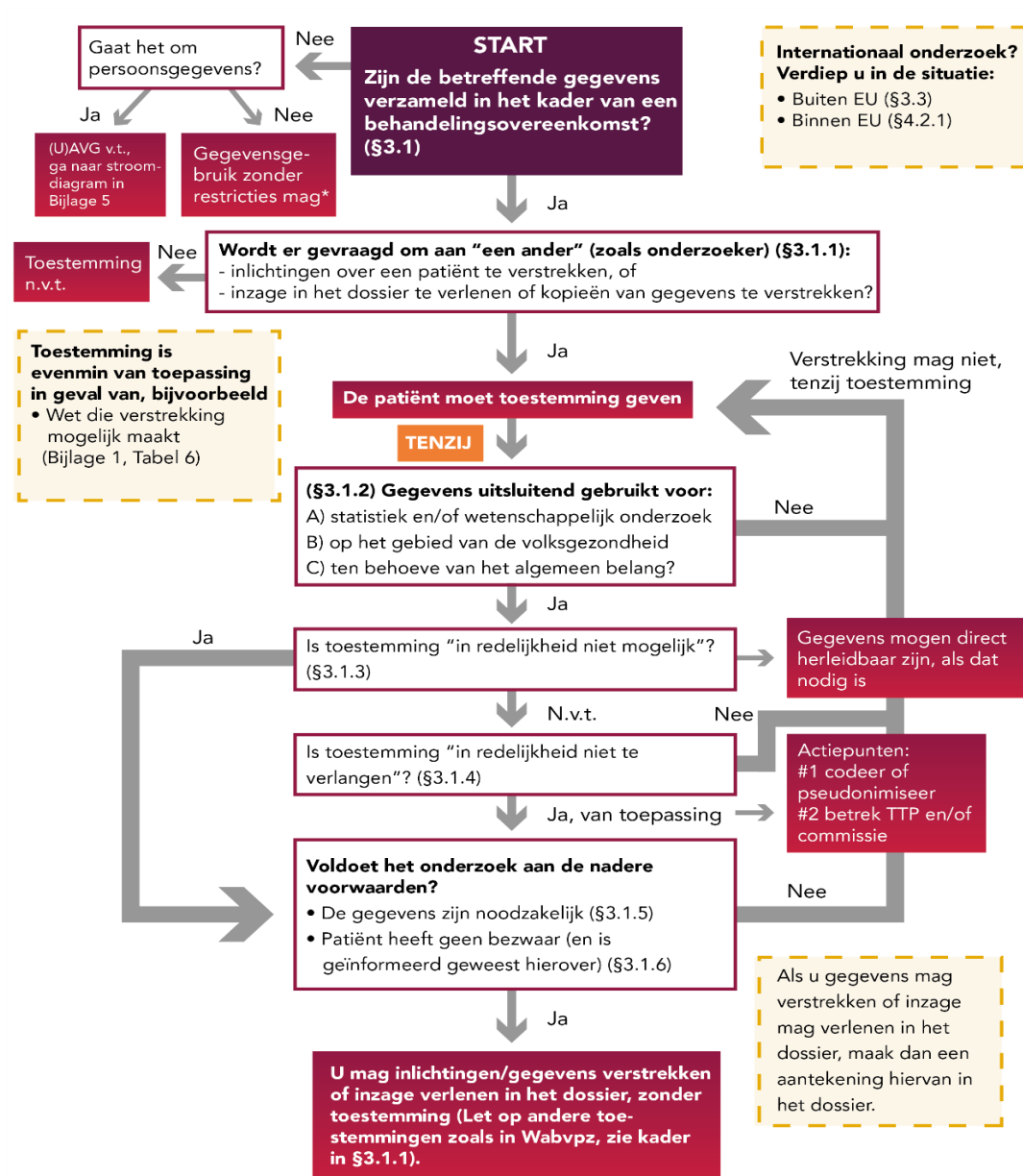
Onderwerp	Eis
Bewijslast	De verwerkingsverantwoordelijke moet kunnen aantonen dat de patiënt toestemming heeft voor de verwerking van zijn persoonsgegevens. Bijvoorbeeld met behulp van een logbestand waarin de handelingen van de patiënt t.b.v. de toestemming met een <i>timestamp</i> zijn vastgelegd.
Volledig informeren	De verwerkingsverantwoordelijke moet het voor een persoon glashelder maken, of de activiteit die hij/zij ontplooit, verbonden is met het geven van toestemming. Die persoon moet in staat zijn te beoordelen in hoeverre hij bereid is zijn gegevens te verstrekken om zijn activiteit te ontplooiën. Er mag geen enkele marge zijn voor dubbelzinnigheid. Het moet voor de patiënt duidelijk zijn wie (als verwerkingsverantwoordelijke(n)) de toestemming vraagt en wat de doeleinden van het gegevensgebruik zijn. Ook moet de patiënt worden geïnformeerd dat hij/zij altijd het recht heeft om zijn toestemming in te trekken.
Begrijpelijk en eenvoudig	De verwerkingsverantwoordelijke moet het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm, en in duidelijke en eenvoudige taal presenteren. Hierbij moet een duidelijk onderscheid worden gemaakt tussen de tekst waarop de toestemming betrekking heeft en andere zaken.
Intrekking faciliteren	De verwerkingsverantwoordelijke moet faciliteren dat de patiënt zijn/haar toestemming kan intrekken op een manier die even eenvoudig is als het geven van de toestemming. De gegevens die zijn verzameld vóór de intrekking moeten dan verwijderd worden als deze niet meer nodig zijn om het doel – waarvoor de toestemming destijds is gevraagd – te behalen en er geen andere rechtsgrond van toepassing is (EDPB Guidelines 05/2020). Na intrekking mogen er geen gegevens meer worden verzameld, behalve als er een andere rechtsgrond is dan toestemming.
Recht op gegevens-overdracht	De patiënt heeft het recht op overdraagbaarheid van gegevens. D.w.z. dat de patiënt de gegevens die hij/zij heeft verstrekt, dient te ontvangen in een gestructureerde, gangbare en voor een machine leesbare vorm, zodat hij deze gegevens aan een andere partij kan overdragen.
Kinderen en toestemming	Patiënten onder de zestien jaar oud kunnen niet zelf AVG-toestemming geven. Hun wettelijk vertegenwoordigers als ouders/voogden moeten dit doen. ¹⁶⁶ Een uitzondering hierop is, als het gaat om preventieve dienstverlening of begeleidingsdiensten die rechtstreeks aan het kind worden aangeboden. Bijvoorbeeld een online chat van de kindbescherming. Hiervoor is geen voorafgaande ouderlijke toestemming vereist.

166 De Verzamelwet gegevensbescherming beoogt de verhouding tussen de UAVG en de WGBO over toestemming van o.a. minderjarigen te verhelderen. Zie: <https://www.internetconsultatie.nl/verzamelwetgegevensbescherming>.

Tijdstip en ‘houdbaarheid’ toestemming?

De AVG-toestemming moet worden verleend vóórdat de gegevens van de patiënt worden ‘verwerkt’. Dit betekent dus dat de toestemming moet worden gevraagd (en verkregen) vóórdat de gegevens automatisch worden verwerkt, bijvoorbeeld met behulp van *machine learning* of, als dit aan de orde is, als de gegevens worden doorgezonden naar een andere partij. De AVG verschaft geen specifieke termijn voor de geldigheid van de toestemming. Hoe lang toestemming geldig blijft, hangt af van de context, de werkingssfeer van de oorspronkelijke toestemming en de verwachtingen van de patiënt.

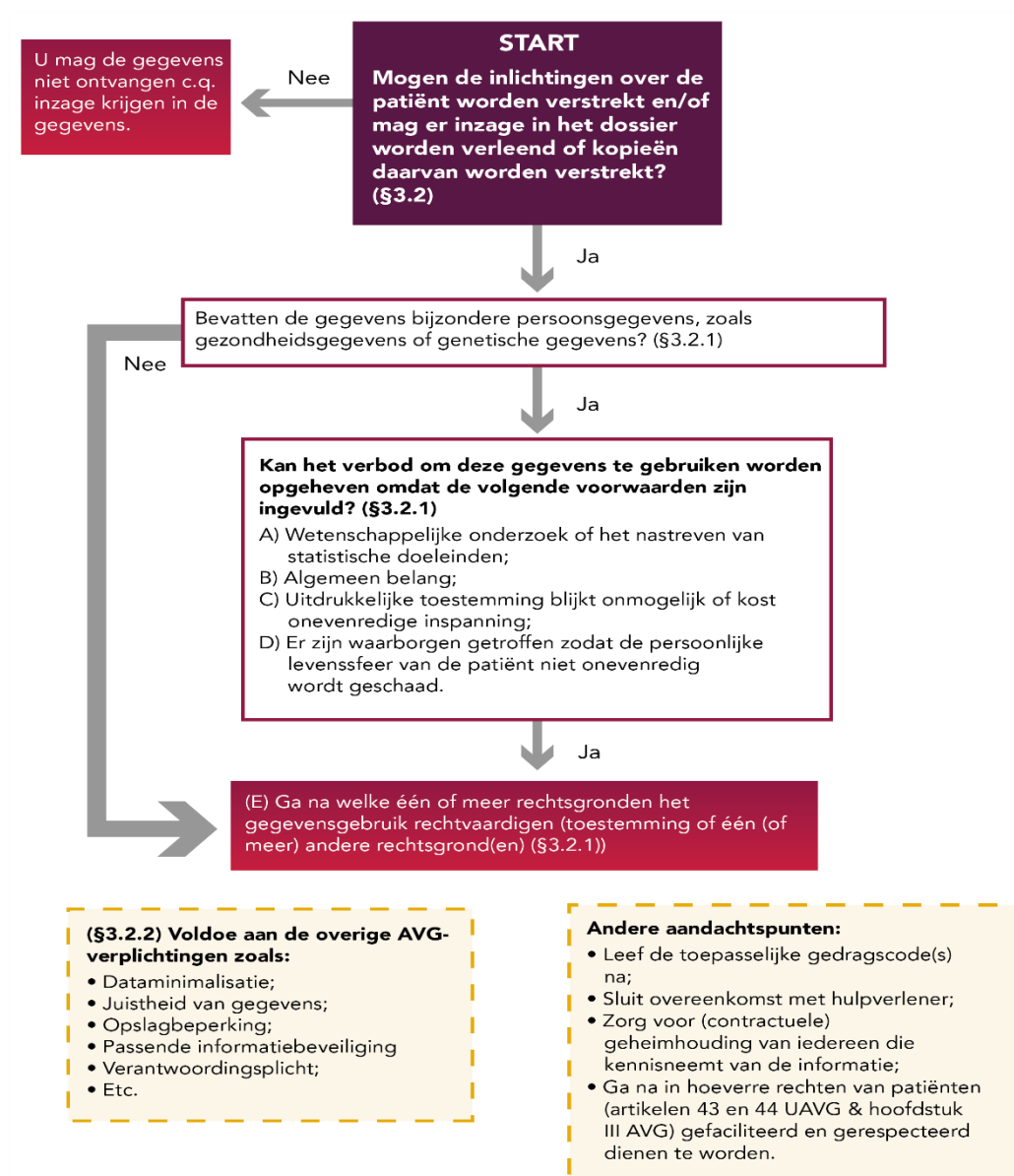
Bijlage 4: Stroomdiagram ‘Data-inzage of -verstrekking voor nWMO-onderzoek door hulpverlener’



*Let op: door acties als koppeling en analyse kunnen niet-privacygevoelige gegevens 'verkleuren' naar persoonsgegevens. De (U)AVG is daarop van toepassing.

Bron: Rathenau Instituut (2020). Datasolidariteit voor gezondheid – Verbeterpunten met oog voor ieders belang. Den Haag (auteurs: Gerritsen, J. & P. Verhoef).

Bijlage 5: Stroomdiagram 'Gebruik data voor nWMO-onderzoek door onderzoeker'



Bron: Rathenau Instituut (2020). Datasolidariteit voor gezondheid – Verbeterpunten met oog voor ieders belang. Den Haag (auteurs: Gerritsen, J. & P. Verhoef).

© Rathenau Instituut 2020

Verveelvoudigen en/of openbaarmaking van (delen van) dit werk voor creatieve, persoonlijke of educatieve doeleinden is toegestaan, mits kopieën niet gemaakt of gebruikt worden voor commerciële doeleinden en onder voorwaarde dat de kopieën de volledige bovenstaande referentie bevatten. In alle andere gevallen mag niets uit deze uitgave worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie of op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming.

Open Access

Het Rathenau Instituut heeft een Open Access beleid. Rapporten, achtergrondstudies, wetenschappelijke artikelen, software worden vrij beschikbaar gepubliceerd. Onderzoeksgegevens komen beschikbaar met inachtneming van wettelijke bepalingen en ethische normen voor onderzoek over rechten van derden, privacy, en auteursrecht.

Contactgegevens

Anna van Saksenlaan 51
Postbus 95366
2509 CJ Den Haag
070-342 15 42
info@rathenau.nl
www.rathenau.nl

Bestuur van het Rathenau Instituut

Mw. Gerdi Verbeet
Prof. dr. Noelle Aarts
Drs. Felix Cohen
Dr. Hans Dröge
Dr. Laurence Guérin
Dr. Janneke Hoekstra, MSc
Prof. mr. dr. Erwin Muller
Drs. Rajash Rawal
Prof. dr. ir. Peter-Paul Verbeek
Dr. ir. Melanie Peters (secretaris)

Het Rathenau Instituut stimuleert de publieke en politieke meningsvorming over de maatschappelijke aspecten van wetenschap en technologie. We doen onderzoek en organiseren het debat over wetenschap, innovatie en nieuwe technologieën.

Rathenau Instituut